Регламент N 2016/679 Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)" [рус., англ.] (Принят в г. Брюсселе 27.04.2016)

[неофициальный перевод] <*>

РЕГЛАМЕНТ (ЕС) N 2016/679
ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА ЕС
О ЗАЩИТЕ ФИЗИЧЕСКИХ ЛИЦ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
И О СВОБОДНОМ ОБРАЩЕНИИ ТАКИХ ДАННЫХ, А ТАКЖЕ ОБ ОТМЕНЕ
ДИРЕКТИВЫ 95/46/ЕС (ОБЩИЙ РЕГЛАМЕНТ О ЗАЩИТЕ
ПЕРСОНАЛЬНЫХ ДАННЫХ) <>**

(Брюссель, 27 апреля 2016 года)

(Действие Регламента распространяется
на Европейское экономическое пространство)

<*> Перевод Новиковой Е.В.

<**> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) Опубликован в Официальном Журнале (далее - ОЖ) N L 119, 04.05.2016, стр. 1 - 88.

Европейский Парламент и Совет Европейского Союза,

руководствуясь Договором о функционировании Европейского Союза, и, в частности, Статьей 16 Договора,

на основании предложения Европейской Комиссии,

после передачи проекта законодательного акта национальным парламентам,

на основании заключения Европейского комитета по экономическим и социальным вопросам <*>,

---

<*> ОЖ N C 229, 31.07.2012, стр. 90.

на основании заключения Комитета регионов <*>,

<*> ОЖ N C 391, 18.12.2012, стр. 127.

действуя в соответствии с обычной законодательной процедурой <*>,

---

<*> Позиция Европейского Парламента от 12 марта 2014 г. (еще не опубликована в ОЖ) и позиция Совета ЕС при первом чтении от 8 апреля 2016 г. (еще не опубликована в ОЖ). Позиция Европейского Парламента от 14 апреля 2016 г.

принимая во внимание следующие обстоятельства:

(1) Защита физических лиц при обработке персональных данных является основным правом. Статья 8(1) Хартии Европейского Союза об основных правах ("Хартия") и Статья 16(1) Договора о функционировании Европейского Союза (TFEU) предусматривают, что каждый человек имеет право на защиту относящихся к нему персональных данных.

(2) Принципы и правила защиты физических лиц при обработке их персональных данных вне зависимости от гражданства или места жительства лица должны соответствовать основным правам и свободам, в частности, праву на защиту персональных данных. Целью настоящего Регламента является содействие формированию пространства свободы, безопасности и правосудия и экономического союза, содействие экономическому и социальному прогрессу, укреплению и сближению экономик в рамках внутреннего рынка, а также содействие благосостоянию физических лиц.

(3) Целью Директивы 95/46/ЕС Европейского Парламента и Совета ЕС <*> является гармонизация положений о защите основных прав и свобод физических лиц при обработке данных, а также гарантия свободного движения персональных данных между государствами-членами ЕС.

<*> Директива 95/46/ЕС Европейского Парламента и Совета ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (ОЖ N L 281, 23.11.1995, стр. 31).

(4) Целью обработки персональных данных является служба человечеству. Право на защиту персональных данных не является абсолютным правом; его необходимо рассматривать относительно его функции в обществе, оно должно быть уравнено с другими основными правами в соответствии с принципом пропорциональности. Настоящий Регламент соблюдает все основные права, свободы и принципы, признанные в Хартии и закрепленные в Договорах, в частности, уважение частной и семейной жизни, жилища и переписки, защиту персональных данных, свободу мысли, совести и вероисповедания, свободу выражения мнения и распространения информации, право ведения хозяйственной деятельности, право на эффективное средство правовой защиты и на справедливое судебное разбирательство, культурное, религиозное и языковое разнообразие.

(5) Экономическая и социальная интеграция, явившаяся следствием функционирования внутреннего рынка, привела к существенному увеличению трансграничного потока персональных данных. Обмен персональными данными между государственными и негосударственными субъектами, в том числе физическими лицами, объединениями и предприятиями на территории Союза, увеличился. Национальные органы в государствах-членах ЕС призваны в соответствии с законодательством Союза сотрудничать и обмениваться персональными данными в целях выполнения своих обязанностей или осуществления задач от имени органа власти другого государства-члена ЕС.

(6) В связи с быстрым развитием технологий и глобализацией появились новые проблемы, связанные с защитой персональных данных. Масштаб сбора и обмена персональными данными существенно увеличился. Технологии позволяют частным компаниям и органам государственной власти в рамках осуществления своей деятельности использовать персональные данные в беспрецедентном масштабе. В последнее время физические лица все чаще делают доступной личную информацию. Технологии изменили экономическую и социальную жизнь, они должны и далее облегчать свободное движение персональных данных в Союзе, а также их передачу третьим странам и международным организациям, при этом необходимо обеспечить высокий уровень защиты персональных данных.

(7) Указанные достижения требуют наличия надежной, более согласованной правовой базы в области защиты данных в Союзе, опирающейся на строгое исполнение, так как это имеет существенное значение для создания атмосферы доверия, которая позволит цифровой экономике развиваться в рамках внутреннего рынка. Физические лица должны иметь право распоряжаться своими собственными персональными данными. Необходимо повысить уровень правовой определенности и практической достоверности для физических лиц, субъектов экономической деятельности и органов государственной власти.

(8) Если в настоящем Регламенте предусмотрены спецификации или ограничения его положений законодательством государства-члена ЕС, государства-члены ЕС могут по мере необходимости инкорпорировать элементы настоящего Регламента в свое национальное законодательство для обеспечения согласованности, а также для того, чтобы сделать национальные положения более доступными для лиц, в отношении которых они применяются.

(9) Цели и принципы Директивы 95/46/ЕС по-прежнему сохраняют юридическую силу, но она не препятствует фрагментации при имплементации защиты данных в Союзе, правовой неопределенности или распространенному общественному мнению относительно того, что имеются существенные риски для защиты физических лиц, в частности, относительно сетевой активности. Различия в уровне защиты прав и свобод физических лиц, в особенности права на защиту персональных данных при обработке персональных данных в государствах-членах ЕС, могут препятствовать свободному движению персональных данных на территории Союза. В связи с этим указанные различия представляют собой препятствие для осуществления экономической деятельности на уровне Союза, нарушают свободу конкуренции и затрудняют органам власти исполнение их обязанностей согласно законодательству Союза. Указанное различие в уровнях защиты является результатом существования различий в имплементации и применении Директивы 95/46/ЕС.

(10) Для обеспечения согласованного и высокого уровня защиты физических лиц и для устранения препятствий движению персональных данных в Союзе уровень защиты прав и свобод физических лиц при обработке указанных данных должен быть эквивалентным во всех государствах-членах ЕС. На всей территории Союза необходимо гарантировать согласованное и однородное применение положений о защите основных прав и свобод физических лиц при обработке персональных данных. В том, что касается обработки персональных данных для соблюдения правовых обязательств, для выполнения задачи в защиту общественных интересов или при осуществлении полномочий, закрепленных за контролером, государствам-членам ЕС необходимо разрешить сохранять или вводить национальные положения для дальнейшего применения положений настоящего Регламента. В совокупности с общим и горизонтальным законодательством относительно защиты данных, имплементирующим Директиву 95/46/ЕС, государства-члены ЕС располагают несколькими специфическими нормами в областях, которые требуют более специфических положений. Настоящий Регламент также предлагает государствам-членам ЕС свободу действия в целях определения предписаний, в том числе для обработки особых категорий персональных данных ("конфиденциальные сведения"). В связи с этим настоящий Регламент не исключает законодательство государства-члена ЕС, которое устанавливает обстоятельства для особых ситуаций обработки, в том числе более точное определение условий, при которых обработка персональных данных будет основываться на принципе законности.

(11) Эффективная защита персональных данных на территории Союза требует усиления и точного установления прав субъектов персональных данных и обязанностей тех, кто обрабатывает и определяет обработку персональных данных, а также эквивалентные полномочия по контролю и обеспечению соблюдения положений для защиты персональных данных и равнозначных санкций за нарушение в государствах-членах ЕС.

(12) Статья 16(2) TFEU предписывает Европейскому Парламенту и Совету ЕС установить правила в отношении защиты физических лиц при обработке персональных данных и правила в отношении свободного обращения персональных данных.

(13) Для того чтобы гарантировать соответствующий уровень защиты физических лиц на территории Союза и предупредить возникновение отклонений, мешающих свободному обращению персональных данный в рамках внутреннего рынка, Регламент необходим для обеспечения правовой определенности и прозрачности для субъектов экономической деятельности, включая микропредприятия, малые и средние предприятия, а также для обеспечения физических лиц во всех государствах-членах ЕС таким же уровнем юридически действительных прав, обязанностей и ответственности для контролеров и лиц, осуществляющих обработку, для того, чтобы гарантировать соответствующий мониторинг процесса обработки персональных данных, и равнозначных санкций во всех государствах-членах ЕС, а также плодотворное сотрудничество между надзорными органами различных государств-членов ЕС. Надлежащее функционирование внутреннего рынка требует того, чтобы свободное обращение персональных данных в Союзе не было ограничено или запрещено по причинам, связанным с защитой физических лиц при обработке персональных данных. Для того чтобы принять во внимание специфическую ситуацию микропредприятий, малых и средних предприятий, настоящий Регламент включает в себя частичное отступление в отношении ведения учета для организаций, на которых занято менее 250 работников. В дополнение к этому институты и органы Союза, государства-члены ЕС и их надзорные органы могут учитывать специфические нужды микропредприятий, малых и средних предприятий при применении настоящего Регламента. Понятие "микропредприятия, малые и средние предприятия" указано в Статье 2

Приложения к Рекомендации 2003/361/ЕС Европейской Комиссии <*>.

<*> Рекомендация Европейской Комиссии от 6 мая 2003 г. относительно определения микропредприятий, малых и средних предприятий (C(2003) 1422) (ОЖ N L 124, 20.05.2003, стр. 36).

(14) Защита, предусмотренная настоящим Регламентом, должна применяться в отношении физических лиц вне зависимости от их гражданства или места жительства при обработке их персональных данных. Настоящий Регламент не охватывает обработку персональных данных юридических лиц и, в частности, предприятий, учрежденных в качестве юридических лиц, включая наименование и форму юридического лица, а также контактную информацию юридического лица.

(15) Для предотвращения серьезного риска обхода положений защита физических лиц должна быть технически нейтральной и не должна зависеть от используемых технических средств. Защита физических лиц должна применяться в отношении обработки персональных данных при помощи автоматизированных средств, а также в отношении ручной обработки, если персональные данные содержатся или должны будут содержаться в файловой системе. Файлы или группы файлов, а также их титульные страницы, которые не структурированы в соответствии со специальными критериями, не должны подпадать под сферу применения настоящего Регламента.

(16) Настоящий Регламент не распространяется на вопросы, связанные с защитой фундаментальных прав и свобод или со свободным движением персональных данных в отношении деятельности, которая не подпадает под действие законодательства Союза, например деятельности, связанной с национальной безопасностью. Настоящий Регламент не распространяется на обработку персональных данных государствами-членами ЕС при осуществлении деятельности, касающейся общей внешней политики и политики безопасности Союза.

(17) Регламент (ЕС) 45/2001 Европейского Парламента и Совета ЕС <*> применяется в отношении обработки персональных данных институтами, органами, учреждениями и агентствами Союза. Регламент (ЕС) 45/2001 и другие законодательные акты Союза в области обработки персональных данных должны быть изменены в соответствии с принципами и нормами, установленными в настоящем Регламента, и должны применяться в контексте настоящего Регламента. В целях обеспечения четкой и согласованной базы по защите данных в Союзе после принятия настоящего Регламента следует внести необходимые изменения в Регламент (ЕС) 45/2001 для того, чтобы обеспечить возможность его применения одновременно с применением настоящего Регламента.

<*> Регламент (ЕС) 45/2001 Европейского Парламента и Совета ЕС от 18 декабря 2000 г. о защите физических лиц при обработке персональных данных, осуществляемой институтами и органами Сообщества и о свободном обращении таких данных (ОЖ N L 8, 12.01.2001, стр. 1).

(18) Настоящий Регламент не применяется в отношении обработки персональных данных физическими лицами в ходе осуществления исключительно личной или бытовой деятельности, не связанной с профессиональной или коммерческой деятельностью. Личная или бытовая деятельность может включать в себя переписку и сохранение адресов или взаимодействие через социальные сети и сетевую активность, осуществляемые в контексте такой деятельности. Однако настоящий Регламент применяется в отношении контролеров или лиц, осуществляющих обработку, которые обеспечивают средства для обработки персональных данных для такой личной или бытовой деятельности.

(19) Защита физических лиц при обработке персональных данных компетентными органами в целях предупреждения, расследования, выявления уголовных преступлений или привлечения к ответственности, или приведения в исполнение уголовных наказаний, включая защиту и предотвращение угроз общественной безопасности, а также свободное обращение таких данных являются предметом отдельного законодательного акта Союза. Вследствие этого настоящий Регламент не применяется в отношении обработки данных для указанных целей. Однако обрабатываемые органами государственной власти в рамках настоящего Регламента персональные данные, если они используются для указанных целей,

должны регулироваться более конкретным законодательным актом Союза, а именно Директивой (ЕС) 2016/680 Европейского Парламента и Совета ЕС <*>. Государства-члены ЕС могут поручить компетентным органам в значении Директивы (ЕС) 2016/680 выполнение задач, которые необязательно осуществляются в целях предупреждения, расследования, выявления уголовных преступлений или привлечения к ответственности или приведения в исполнение уголовных наказаний, включая защиту и предотвращение угроз общественной безопасности, для того чтобы обработка персональных данных для указанных иных целей, постольку, поскольку она находится в рамках законодательства Союза, подпадала под действие настоящего Регламента.

<*> Директива (ЕС) 2016/680 Европейского Парламента и Совета ЕС от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных компетентными органами в целях предупреждения, расследования, выявления уголовных преступлений или привлечения к ответственности, или приведения в исполнение уголовных наказаний, и о свободном движении таких данных и отмене Рамочного Решения 2008/977/ПВД Совета ЕС (см. стр. 89 настоящего ОЖ).

При обработке персональных данных компетентными органами в целях, подпадающих под действие настоящего Регламента, государства-члены ЕС должны иметь возможность сохранять или вводить более конкретные положения для адаптации к применению норм настоящего Регламента. Такие положения могут определять более точные требования для обработки персональных данных указанными компетентными органами для указанных иных целей, с учетом конституционной, организационной и административной структуры соответствующего государства-члена ЕС. Если обработка персональных данных частными организациями попадает под действие настоящего Регламента, настоящий Регламент должен обеспечивать возможность государствам-членам ЕС при наличии определенных оснований законодательно ограничивать определенные обязанности и права, если такое ограничение представляет собой необходимую и пропорциональную меру в демократическом обществе для защиты специфических важных интересов, включая общественную безопасность и предупреждение, расследование, выявление уголовных преступлений или привлечение к ответственности или приведение в исполнение уголовных наказаний, в том числе защиту и предотвращение угроз общественной безопасности. Например, это имеет существенное значение в рамках противодействия отмыванию доходов, полученных преступным путем, или в рамках деятельности лабораторий судебной экспертизы.

(20) Поскольку настоящий Регламент применяется inter alia в отношении деятельности судов и других судебных органов, законодательство Союза или государства-члена ЕС могло бы определить процесс и процедуры обработки данных в отношении обработки персональных данных судами и другими судебными органами. Для того чтобы обеспечить независимость судебной системы при осуществлении судебных задач, включая процесс принятия решения, компетенция надзорных органов не должна охватывать обработку персональных данных, если суды действуют в пределах своей судейской дееспособности. Необходимо обеспечить возможность передачи контроля над процессом обработки данных особым органам в рамках судебной системы государства-члена ЕС, которые должны, в частности, гарантировать соблюдение норм настоящего Регламента, повысить осведомленность среди представителей судебно-прокурорской системы относительно их обязанностей согласно настоящему Регламенту и рассматривать жалобы в отношении указанного процесса обработки данных.

(21) Настоящий Регламент действует без ущерба применению Директивы 2000/31/ЕС Европейского Парламента и Совета ЕС <*>, и, в частности, применению норм Статей 12 - 15 указанной Директивы об ответственности поставщиков посреднических услуг. Указанная Директива ориентирована на содействие нормальному функционированию внутреннего рынка и обеспечивает свободное обращение услуг информационного общества среди государств-членов ЕС.

<*> Директива 2000/31/ЕС Европейского Парламента и Совета ЕС от 8 июня 2000 г. о некоторых правовых аспектах информационных услуг на внутреннем рынке, в частности, об электронной коммерции (Директива об электронной коммерции) (ОЖ N L 178, 17.07.2000, стр. 1).

(22) Любая обработка персональных данных в контексте деятельности об учреждении контролера или лица, обрабатывающего данные, в Союзе должна осуществляться в соответствии с настоящим Регламентом, вне зависимости от того, проводится ли обработка данных на территории Союза. Учреждение подразумевает эффективное и реальной осуществление деятельности посредством установившихся договоренностей. В этой связи юридическая форма таких договоренностей, вне зависимости от того, идет ли речь об отделении или дочернем предприятии с правосубъектностью, не является определяющим фактором.

(23) В целях гарантии того, что физические лица не лишены предоставляемой согласно настоящему Регламенту защиты, обработка персональных данных субъектов данных, находящихся в Союзе, не учрежденными в Союзе контролером или обрабатывающим данные лицом должна подпадать под действие настоящего Регламента, если обработка данных имеет отношение к предложению товаров или услуг таким субъектам данным, вне зависимости от внесения платы. Для того чтобы определить, предлагает ли такой контролер или обрабатывающее данное лицо товары или услуги субъектам данным, которые находятся в Союзе, необходимо установить очевидность того, что контролер или обрабатывающее данное лицо намеревается предложить услуги субъектам данным в одном или нескольких государствах-членах ЕС в Союзе. В свою очередь явная доступность интернет-сайта контролера, обрабатывающего данные лица или посредника в Союзе, адреса электронной почты или иных контактных данных, или использование языка, принятого в третьей стране, в которой учрежден контролер, недостаточны для установления такого намерения, такие факторы как использование языка или валюты, распространенной в одном или нескольких государствах-членах ЕС, в совокупности с возможностью заказа товаров или услуг на данном языке, или упоминание покупателей или пользователей, находящихся в Союзе, указывают на то, что контролер намерен предложить товары или услуги субъектам данных в Союзе.

(24) Обработка персональных данных субъектов данных, находящихся в Союзе, не учрежденными в Союзе контролером или обрабатывающим данные лицом также подпадает под действие настоящего Регламента, если она связана с мониторингом поведенческой активности указанных субъектов данных постольку, поскольку их поведенческая активность имеет место в Союзе. Для того чтобы определить, может ли обработка данных рассматриваться в целях мониторинга поведенческой активности субъектов данных, необходимо установить, прослеживается ли деятельность физических лиц в сети интернет, включая возможное последующее использование способов обработки персональных данных, посредством которых составляется профиль физического лица, особенно для принятия относящихся к нему решений или для анализа или прогнозирования его/ее личных предпочтений, форм поведения и жизненных позиций.

(25) Если законодательство государства-члена ЕС применяется в силу действия международного публичного права, как например, в дипломатическом представительстве или консульском учреждении государства-члена ЕС, настоящий Регламент должен также применяться в отношении контролера, не учрежденного в Союзе.

(26) Принципы защиты данных должны применяться в отношении любой информации, касающейся идентифицированного или идентифицируемого физического лица. Подвергнутые псевдонимизации персональные данные, которые могут быть соотнесены с физическим лицом посредством использования дополнительной информации, должны рассматриваться в качестве информации об идентифицируемом физическом лице. В целях установления того, является ли физическое лицо идентифицируемым, следует принять во внимание все средства, с высокой степенью вероятности используемые контролером или иным лицом, для того чтобы прямо или косвенно идентифицировать физическое лицо, например, выявление. При определении того, используются ли средства с достаточной степенью вероятности для идентификации физического лица, следует обратить внимание на все объективные факторы, такие как расходы на идентификацию и количество времени, необходимого для идентификации, с учетом имеющихся на момент обработки технологий и технологических разработок. Вследствие этого принципы защиты данных не применяются в отношении анонимной информации, а именно информации, которая не относится к идентифицированному или идентифицируемому физическому лицу, или в отношении персональных данных, предоставленных анонимно таким образом, что субъект данных не идентифицируется. Настоящий Регламент не касается обработки указанной анонимной информации, в том числе в статистических или исследовательских целях.

(27) Настоящий Регламент не применяется в отношении персональных данных умерших лиц.

Государства-члены ЕС могут предусмотреть положения в области обработки персональных данных умерших лиц.

(28) Применение псевдонимизации в отношении персональных данных может снизить риски для субъектов данных и помочь контролерам и лицам, обрабатывающим данные, при выполнении ими своих обязанностей по защите данных. Прямое введение "псевдонимизации" в настоящем Регламенте не исключает использование любых других мер по защите данных.

(29) В целях создания стимулов для применения псевдонимизации при обработке персональных данных меры псевдонимизации, допускающие проведение общего анализа, должны быть возможны у того же контролера, если указанный контролер принял технические и организационные меры, необходимые в целях обеспечения, для соответствующей обработки, имплементации настоящего Регламента и гарантии того, что дополнительная информация для соотнесения персональных данных с определенным субъектом данных хранится отдельно. Контролер, обрабатывающий персональные данные, должен указать уполномоченных лиц у того же самого контролера.

(30) Физические лица могут быть связаны с сетевыми идентификаторами, предусмотренными их устройствами, приложениями, программными средствами и протоколами, как например, IP-адреса, идентификаторы типа куки-файлы или иные идентификаторы, например метки радиочастотной идентификации. Это может оставлять следы, которые, особенно в сочетании с уникальными идентификаторами и другой полученной серверами информацией, могут быть использованы для создания профилей физических лиц и для их идентификации.

(31) Органы государственной власти, которым раскрываются персональные данные в соответствии с юридической обязанностью по осуществлению официального представительства, например, налоговые органы и органы таможенного контроля, отделы финансовых расследований, независимые административные органы или службы по надзору за финансовым рынком, ответственные за регулирование и надзор за фондовыми рынками, не должны считаться получателями, если они получают персональные данные, которые в соответствии с законодательством Союза или государства-члена ЕС необходимы для осуществления конкретного исследования в интересах общества. Запрос на раскрытие данных, направленный органами государственной власти, всегда должен осуществляться в письменной форме, быть обоснованным и носить случайный характер, он не должен касаться целостности файловой системы или вести к объединению файловых систем. Обработка персональных данных указанными органами государственной власти должна соответствовать применимым нормам по защите данных согласно целям обработки.

(32) Согласие должно быть дано посредством четкого утвердительного действия, при помощи которого субъект данных демонстрирует добровольное, определенное и однозначное согласие на обработку относящихся к нему персональных данных, например, посредством письменного заявления, в том числе поданного электронным способом, или устного заявления. Сюда может относиться простановка галочки/крестика при посещении интернет-сайта, выбор технических настроек для услуг информационного общества или иное заявление или способ поведения, который четко указывает на то, что субъект данных в указанном контексте согласен на запланированную обработку своих персональных данных. Молчание, уже проставленная галочка/крестик или бездействие лица не является согласием. Согласие должно охватывать всю обработку, осуществляемую для той же самой цели или целей. Если обработка служит нескольким целям, согласие должно быть дано для каждой из них. Если согласие субъекта данных должно быть дано электронным способом, запрос должен быть сделан в четкой и лаконичной форме, без ненужного прекращения услуги, для которой предоставляется согласие.

(33) Не всегда имеется возможность полностью идентифицировать цель обработки персональных данных для целей научного исследования во время сбора персональных данных. Вследствие этого, субъектам данных необходимо разрешить давать свое согласие в отношении определенных областей научного исследования в соответствии с признанными этическими стандартами научных исследований. Субъекты данных должны иметь возможность давать свое согласие только в отношении определенных областей исследования или частей исследовательских проектов в той мере, в какой это допустимо в рамках запланированной цели.

(34) Генетические данные должны определяться как персональные данные в отношении

унаследованных или приобретенных характеристик физического лица, которые были получены в результате анализа биологического образца соответствующего лица, в частности, в результате хромосомного анализа, анализа ДНК или РНК, или анализа иных элементов, позволяющего получить эквивалентную информацию.

(35) Связанные со здоровьем персональные данные должны включать в себя все данные, которые относятся к состоянию здоровья субъекта данных и раскрывают информацию о прошлом, текущем и будущем физическом или психологическом состоянии здоровья субъекта данных. Сюда относится информация о физическом лице, собранная в ходе регистрации или предоставления медицинских услуг согласно Директиве 2011/24/ЕС Европейского Парламента и Совета ЕС <*> указанному физическому лицу; номер, символ или знак, присвоенные физическому лицу для однозначной идентификации указанного лица в целях здоровья; информация, полученная в результате исследования или обследования части тела или телесного материала, включая генетические данные и биологические образцы; а также любая информация, например, о заболевании, инвалидности, риске заболевания, медицинском анамнезе, клиническом лечении или о физиологическом или медико-биологическом состоянии субъекта данных, независимо от источника данных, например, они могут быть получены от врача или другого медицинского работника, больницы, медицинского оборудования или в результате диагностики в лабораторных условиях.

<*> Директива 2011/24/ЕС Европейского Парламента и Совета ЕС от 9 марта 2011 г. о правах пациентов в трансграничном медицинском обслуживании (ОЖ N L 88, 04.04.2011, стр. 45).

(36) Основное учреждение контролера в Союзе должно являться местом его центральной администрации в Союзе за исключением случаев, когда решения о целях и средствах обработки персональных данных принимаются в ином учреждении контролера в Союзе, в таком случае указанное другое учреждение должно считаться основным учреждением. Для определения основного учреждения контролера в Союзе необходимо использовать объективные критерии, при этом предполагается эффективное и реальное осуществление управленческой деятельности, в рамках которой принимаются основные решения относительно целей и средств обработки посредством четких договоренностей. Указанный критерий не должен зависеть от того, осуществляется ли обработка персональных данных в указанном месте. Наличие и использование технических средств и методов для обработки персональных данных или деятельности, связанной с обработкой, само по себе не образует основное учреждение и вследствие этого не является определяющим критерием для основного учреждения. Основное учреждение обрабатывающего данные лица должно являться местом его центральной администрации в Союзе или, если в Союзе у него нет центральной администрации, местом, где в Союзе осуществляется связанная с обработкой основная деятельность. Если в обработке участвует контролер и обрабатывающее данные лицо, компетентным главным надзорным органом должен оставаться надзорный орган государства-члена ЕС, в котором находится основное учреждение контролера, а надзорный орган обрабатывающего данные лица должен считаться соответствующим надзорным органом, и указанный надзорный орган должен участвовать в предусмотренной настоящим Регламентом процедуре сотрудничества. В любом случае, надзорные органы государства-члена ЕС или государств-членов ЕС, в которых обрабатывающее данные лицо имеет один или несколько учреждений, не должны считаться соответствующими надзорными органами, если проект решения касается только контролера. Если обработка осуществляется группой предприятий, основное учреждение контролирующего предприятия должно считаться основным учреждением группы предприятий, за исключением случаев, когда цели и средства обработки определяются другим предприятием.

(37) Группа предприятий должна включать в себя контролирующее предприятие и подконтрольные ему предприятия; при этом контролирующее предприятие должно являться предприятием, которое может оказывать решающее воздействие на другие предприятия в силу, например, имущественных отношений, финансового участия или предписаний, которые его регулируют, или полномочия на имплементацию норм о защите персональных данных. Предприятие, которое контролирует обработку персональных данных на предприятиях, входящих в его состав, совместно с указанными предприятиями должны рассматриваться в качестве группы предприятий.

(38) Дети нуждаются в особой защите своих персональных данных, так как они в меньшей степени

осознают риски, последствия, соответствующие гарантии и права при обработке персональных данных. Указанная особая защита должна, в частности, применяться в отношении использования персональных данных детей в целях маркетинга или создания личностного профиля или профиля пользователя и сбора персональных данных детей при использовании услуг, предлагаемых непосредственно детям. Согласие лиц, обладающих родительской ответственностью, не является необходимым в контексте профилактических мероприятий и консультационных услуг, предлагаемых непосредственно ребенку.

(39) Любая обработка персональных данных должна быть законной и справедливой. Для физических лиц прозрачность обработки состоит в том, что относящиеся к ним персональные данные собираются, используются, просматриваются или иным образом обрабатываются, а также в том, в какой степени персональные данные обрабатываются или будут обрабатываться. Принцип прозрачности требует, чтобы любая информация или сообщения в отношении обработки указанных персональных данных были легкодоступны и понятны и составлены на ясном и простом языке. Указанный принцип касается, в частности, информации относительно личности контролера и целей обработки, а также иной информации, которая гарантирует справедливую и прозрачную обработку в отношении соответствующих физических лиц и их права на получение подтверждения и сообщения относительно того, какие относящиеся к ним персональные данные обрабатываются. Физические лица должны быть осведомлены о рисках, нормах, гарантиях и правах в отношении обработки персональных данных и о том, как осуществлять свои права в отношении указанной обработки. В частности, определенные цели, для которых обрабатываются персональные данные, должны быть ясными и законными, они должны определяться в ходе сбора персональных данных. Персональные данные должны быть соответствующими, уместными и ограниченными тем, что необходимо для целей, относительно которых они обрабатываются. В частности, это требует гарантии того, что срок, в течение которого хранятся персональные данные, был ограничен строгим минимумом. Персональные данные должны обрабатываться только, если цель обработки не могла быть достигнута иным способом. Для того чтобы гарантировать, что персональные данные не хранятся дольше положенного, контролер должен установить сроки для их уничтожения или для периодического пересмотра. Необходимо принять обоснованные меры, чтобы гарантировать, что неточные персональные данные были исправлены или удалены. Персональные данные должны обрабатываться таким образом, чтобы гарантировать их соответствующую защиту и конфиденциальность, включая предотвращение несанкционированного доступа или использования персональных данных и оборудования, используемого для обработки.

(40) Для того чтобы обработка была законной, персональные данные должны обрабатываться на основании согласия соответствующего субъекта данных или на ином законном основании, установленном или в настоящем Регламенте, или в другом законодательстве Союза или государства-члена ЕС, указанном в настоящем Регламенте, включая необходимость соблюдать законное обязательство, под действие которого подпадает контролер, или необходимость исполнять договор, одной из сторон которого является субъект данных, или для принятия мер по запросу субъекта данных до заключения договора.

(41) В случае если в настоящем Регламенте делается ссылка на законное основание или законодательную меру, это не обязательно требует принятия парламентом законодательного акта, без ущерба требованиям согласно конституционному строю соответствующего государства-члена ЕС. Однако указанное законное основание или законодательная мера должны быть ясными и точными, их применение должно быть заранее предсказуемо для лиц, которых они касаются, в соответствии с судебной практикой Суда Европейского Союза ("Суд") и Европейского суда по правам человека.

(42) В случае если обработка основывается на согласии субъекта данных, контролер должен быть в состоянии подтвердить, что субъект данных дал свое согласие на обработку. В частности, в рамках письменного заявления по другому вопросу гарантии должны обеспечивать, что субъект данных осознает факт того, что он дает свое согласие и в каком объеме указанное согласие дается. В соответствии с Директивой 93/13/ЕЭС Совета ЕС <*> заявление о согласии, предварительно сформулированное контролером, должно предоставляться в понятной и легкодоступной форме, с использованием ясного и простого языка, оно не должно содержать несправедливых условий. Для того чтобы проинформировать о согласии, субъект данных должен знать, как минимум, идентификационные данные контролера и цели обработки персональных данных. Согласие не считается данным добровольно, если у субъекта данных нет подлинного и свободного выбора или он не в состоянии без ущерба отказаться или аннулировать свое согласие.

<*> Директива 93/13/ЕЭС Совета ЕС от 5 апреля 1993 г. о несправедливых условиях в договорах с потребителями (ОЖ N L 95, 21.04.1993, стр. 29).

(43) Для того чтобы гарантировать, что согласие дается добровольно, оно не должно создавать юридическое основание для обработки персональных данных в особых случаях, когда между субъектом данных и контролером существует явный дисбаланс, в частности, если контролер является органом государственной власти и вследствие этого с учетом всех обстоятельств указанной особой ситуации маловероятно, что согласие было дано добровольно. Предполагается, что согласие не дано добровольно, если отдельное согласие не может быть дано в отношении разных видов обработки персональных данных, несмотря на то, что в отдельном случае это является оправданным, или если исполнение договора, включая предоставление услуги, зависит от согласия, несмотря на то, что указанное согласие не является необходимым для исполнения договора.

(44) Обработка данных должна основываться на принципах законности, если она необходима для исполнения договора или для запланированного заключения договора.

(45) В случае если обработка осуществляется в соответствии с законной обязанностью, под действие которой подпадает контролер, или если обработка необходима для выполнения задачи в интересах общества или при осуществлении должностных полномочий, она должна основываться на законодательстве Союза или государства-члена ЕС. Настоящий Регламент не требует специального законодательства в отношении каждого отдельного вида обработки. Законодательства в качестве основания для нескольких видов обработки может быть достаточно, если обработка данных основана на законной обязанности, под действие которой подпадает контролер, или если обработка необходима для выполнения задачи в интересах общества или при осуществлении должностных полномочий. В законодательстве Союза или государства-члена ЕС также должна быть определена цель обработки. Кроме этого, указанное законодательство может уточнять общие условия настоящего Регламента, регулирующие законность обработки персональных данных, может устанавливать спецификации для определения контролера, типы подлежащих обработке персональных данных, соответствующие субъекты данных, организации, которым персональные данные могут раскрываться, целевые ограничения, срок хранения и другие меры для гарантии законной и справедливой обработки. Также в законодательстве Союза или государства-члена ЕС необходимо определить, должен ли контролер, выполняющий задачу в интересах общества или при исполнении должностных полномочий, являться органом государственной власти или другим физическим или юридическим лицом, подпадающим под действие публичного права или при условии, что это оправдано с точки зрения интересов общества, в том числе в целях здоровья, например, общественного здравоохранения, социальной защиты и управления медицинскими услугами, под действие частного права, например, в качестве профессионального объединения.

(46) Обработка персональных данных также считается законной, если она необходима для защиты жизненно важных интересов субъекта данных или другого физического лица. Обработка персональных данных, основанная на жизненном интересе другого физического лица, должна в принципе осуществляться только, если она не может быть проведена на ином законном основании. Некоторые типы обработки могут служить как важным основаниям общественного интереса, так и жизненно важным интересам субъекта данных, например, если обработка необходима в гуманитарных целях, в том числе для контроля эпидемий и их распространения или в чрезвычайных ситуациях гуманитарного характера, в частности, во время техногенных или природных катастроф.

(47) Законные интересы контролера, включая контролера, которому могут быть раскрыты персональные данные, или третьей стороны могут создать законное основание для обработки, при условии, что они не превалируют над интересами или основными правами и свободами субъекта данных, с учетом разумных ожиданий субъектов данных, основанных на взаимоотношении с контролером. Указанный законный интерес может иметь место, например, если между субъектом данных и контролером существуют соответствующие отношения в ситуациях, когда субъект данных является клиентом или состоит на службе контролера. В любом случае наличие законного интереса нуждается в тщательной оценке, в том числе относительно того, может ли субъект данных при сборе персональных данных разумно ожидать, что обработка будет осуществляться для указанной цели. Интересы и основные права субъекта данных могут,

в частности, превалировать над интересом контролера данных, если персональные данные обрабатываются в условиях, когда субъекты данных обоснованно не ожидают проведения дальнейшей обработки. Так как законодатель обязан на уровне законодательного акта предусмотреть законное основание для обработки персональных данных органами государственной власти, указанное законное основание не должно применяться в отношении обработки органами государственной власти при выполнении ими своих задач. Обработка персональных данных, необходимая в целях предотвращения мошенничества, также является законным интересом соответствующего контролера данных. Обработка персональных данных в целях адресного маркетинга может рассматриваться в качестве обработки, служащей законному интересу.

(48) Контролеры, являющиеся частью группы предприятий или институтов, относящихся к центральному органу, могут иметь законный интерес, связанный с передачей персональных данных в рамках группы предприятий для внутренних административных целей, включая обработку персональных данных клиентов и работников. Общие принципы передачи персональных данных в рамках группы предприятий расположенному в третьей стране предприятию остаются в силе.

(49) Обработка персональных данных органами государственной власти, группой реагирования на компьютерные чрезвычайные происшествия (CERTs), группой реагирования на инциденты, связанные с компьютерной безопасностью (CSIRTs), поставщиками сетей электронных коммуникаций и услуг, а также поставщиками технологий и услуг по обеспечению безопасности является законным интересом соответствующего контролера данных в той мере, в какой она необходима и пропорциональна целям обеспечения сетевой и информационной безопасности, то есть способности сети или информационной системы противостоять, на заданном уровне достоверности, случайным событиям, незаконным или преднамеренным действиям, которые компрометируют доступность, подлинность, целостность и конфиденциальность сохраненных или переданных персональных данных, а также безопасность соответствующих услуг, переданных через указанные сети или системы. Указанный законный интерес может включать в себя, например, предотвращение несанкционированного доступа к сетям электронных коммуникаций и распространения вредоносного кода, а также пресечение сетевых атак и угроз для компьютерных и электронных систем связи.

(50) Обработка персональных данных в целях, отличных от тех, для которых персональные данные первоначально собирались, должна быть разрешена только, если она соответствует целям, для которых персональные данные были изначально получены. В указанном случае не требуется иное законное основание, отдельное от того, посредством которого был разрешен сбор персональных данных. Если обработка необходима для выполнения задачи в интересах общества или при осуществлении должностных полномочий, предоставленных контролеру, законодательство Союза или государства-члена ЕС может определить и установить задачи и цели, для которых дальнейшая обработка считается соответствующей и законной. Дальнейшая обработка для целей архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях рассматривается в качестве соответствующей законной обработки. Законное основание, предусмотренное законодательством Союза или государства-члена ЕС для обработки персональных данных, может также предусматривать законное основание для дальнейшей обработки. Для того чтобы убедиться в том, соответствует ли цель дальнейшей обработки цели, для которой персональные данные были первоначально получены, контролер, после выполнения всех требований относительно законности первоначальной обработки, должен принять во внимание, inter alia, следующее: любую связь между указанными целями и целями запланированной дальнейшей обработки; контекст, в котором были получены персональные данные, в частности, разумные ожидания субъектов данных, основанные на отношении с контролером, относительно их дальнейшего использования; характер персональных данных; последствия запланированной дальнейшей обработки для субъектов данных, и наличие соответствующих гарантий первоначальной и запланированной дальнейшей обработки.

В случае если субъект данных дал свое согласие или если обработка основана на законодательстве Союза или государства-члена ЕС, которое в демократическом обществе является необходимой и пропорциональной мерой для защиты, в частности, важных целей общего интереса общества, необходимо разрешить контролеру дальнейшую обработку персональных данных независимо от сопоставимости целей. В любом случае необходимо гарантировать применение принципов, установленных в настоящем Регламенте и, в частности, информирование субъекта данных об указанных других целях и о его правах, в

том числе праве на возражение. Указания контролера на возможные уголовно-наказуемые деяния или угрозы общественной безопасности и передача соответствующих персональных данных в отдельных случаях или в нескольких случаях, связанных с одним и тем же уголовно-наказуемым деянием или угрозами общественной безопасности, компетентному органу должны рассматриваться в качестве законного интереса контролера. Однако указанная передача в рамках законного интереса контролера или дальнейшая обработка персональных данных должны быть запрещены, если обработка не соответствует законной, профессиональной или иной обязанности по соблюдению конфиденциальности.

(51) Персональные данные, которые по своей природе носят конфиденциальный характер в отношении основных прав и свобод, нуждаются в особой защите, так как контекст их обработки может привести к существенному риску для основных прав и свобод. Указанные персональные данные должны включать в себя персональные данные, раскрывающие расовое и этническое происхождение, при этом использование термина "расовое происхождение" в настоящем Регламенте не означает, что Союз одобряет теории, которые пытаются установить существование отдельных человеческих рас. Обработка фотографий не должна систематически считаться обработкой особых категорий персональных данных, так как они охвачены определением понятия "биометрические данные" только, когда они обрабатываются посредством особых технических средств, позволяющих провести уникальную идентификацию или аутентичность физического лица. Указанные персональные данные не должны обрабатываться за исключением случаев, когда обработка разрешена в особых установленных в настоящем Регламенте случаях, с учетом того, что законодательство государств-членов ЕС может установить особые положения о защите данных, для того чтобы адаптировать применение положений настоящего Регламента в целях соблюдения законного обязательства или в целях выполнения задачи в интересах общества или при осуществлении должностных полномочий контролера. В дополнение к особым требованиям для указанной обработки должны применяться общие принципы и другие положения настоящего Регламента, в частности, относительно условий законной обработки. Необходимо прямо предусмотреть частичные отступления от общего запрета на обработку указанных особых категорий персональных данных, inter alia, если субъект данных дает прямое согласие или если имеются особые потребности, в частности, если обработка осуществляется в рамках законной деятельности определенных объединений или фондов, целью которых является разрешение на реализацию основных свобод.

(52) Также частичные отступления от запрета на обработку особых категорий персональных данных необходимо разрешить, если они предусмотрены в законодательстве Союза или государства-члена ЕС и имеются соответствующие гарантии для защиты персональных данных и других основных прав, если это оправдано с точки зрения общественного интереса, в частности, в отношении обработки персональных данных в области трудового законодательства, законодательства о социальной защите, включая пенсии, и в целях обеспечения безопасности, мониторинга здоровья и предупреждения заболеваний, предотвращения или контроля инфекционных заболеваний и других серьезных угроз здоровью. Указанные частичные отступления могут быть сделаны в целях здоровья, включая здоровье населения и управление медицинскими услугами, особенно для гарантии качества и экономической эффективности методов, используемых для урегулирования претензий в системе медицинского страхования, или в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях. Частичное отступление также может быть сделано для обработки персональных данных, необходимой для обоснования, исполнения или оспаривания исковых требований, в рамках судебной процедуры или в рамках административной или внесудебной процедуры.

(53) Особые категории персональных данных, которые требуют более высокой степени защиты, должны обрабатываться в целях, связанных со здоровьем, только если это необходимо для достижения целей в интересах физических лиц или общества в целом, в частности, в контексте управления медицинскими или социальными услугами и системами, включая обработку таких данных центральными национальными органами здравоохранения в целях контроля качества, информации управления и общего национального и местного надзора за системой медицинского и социального обслуживания и в целях обеспечения непрерывности медицинского обслуживания или социального обеспечения и трансграничного медицинского обслуживания или в целях обеспечения безопасности, мониторинга здоровья и предупреждения заболеваний, или в целях архивирования в интересах общества, в целях научного или исторического исследования, или в статистических целях, на основании законодательства Союза или государства-члена ЕС, которое должно соответствовать цели общественного интереса, а также в отношении исследований, проводимых в области общественного здравоохранения в интересах общества.

Вследствие этого, настоящий Регламент должен предусмотреть гармонизированные условия для обработки особых категорий персональных данных, связанных со здоровьем, в отношении особых потребностей, в частности, если обработка данных осуществляется в определенных, связанных со здоровьем, целях лицами, которые несут законную обязанность о соблюдении профессиональной тайны. Законодательство Союза или государства-члена ЕС должно предусматривать особые и приемлемые меры для защиты основных прав и персональных данных физических лиц. Государства-члены ЕС могут сохранять или вносить дополнительные условия, в том числе ограничения, в отношении обработки генетических данных, биометрических данных или данных, касающихся здоровья. Однако это не должно препятствовать свободному обращению персональных данных в Союзе, если указанные условия применяются в отношении трансграничной обработки указанных данных.

(54) По причинам общественного интереса в областях общественного здравоохранения может быть необходимо проведение обработки особых категорий персональных данных без согласия субъекта данных. Указанная обработка должна осуществляться в соответствии с приемлемыми и особыми мерами для защиты прав и свобод физических лиц. В указанном контексте понятие "общественное здравоохранение" должно пониматься в значении Регламента (ЕС) 1338/2008 Европейского Парламента и Совета ЕС <*> и включать в себя все элементы, связанные со здоровьем, а именно, состояние здоровья, в том числе заболеваемость и нетрудоспособность, факторы, влияющие на состояние здоровья, потребности в медицинском обслуживании, ресурсы, отнесенные к медицинскому обслуживанию, предоставление и универсальный доступ к медицинскому обслуживанию, а также соответствующие расходы и финансирование и причины смертности. Указанная обработка касающихся здоровья данных по причинам общественного интереса не должна приводить к тому, что персональные данные будут обрабатываться в других целях третьей стороной, например работодателями или страховыми и банковскими компаниями.

<*> Регламент (ЕС) 1338/2008 Европейского Парламента и Совета ЕС от 16 декабря 2008 г. о статистике Сообщества в отношении общественного здравоохранения и безопасности на рабочих местах (ОЖ N L 354, 31.12.2008, стр. 70).

(55) Кроме того, обработка персональных данных официальными органами для достижения установленной конституционным правом или международным публичным правом цели официально признанных религиозных организаций осуществляется по причинам общественного интереса.

(56) В случае если в ходе предвыборной деятельности функционирование демократической системы в государстве-члене ЕС требует того, чтобы политические партии собирали персональные данные о политических взглядах лиц, обработка указанных данных может быть разрешена по причинам общественного интереса, при условии наличия соответствующих гарантий.

(57) Если персональные данные, обрабатываемые контролером, не позволяют ему идентифицировать физическое лицо, контролер данных не обязан получать дополнительную информацию для идентификации субъекта данных только в целях соблюдения положения настоящего Регламента. Однако контролер не должен отказываться принимать дополнительную информацию, предоставляемую субъектом данных в целях содействия осуществлению своих прав. Идентификация должна включать в себя цифровую идентификацию субъекта данных, например, посредством механизма аутентификации, например, тех же самых удостоверяющих документов, используемых субъектом данных для того, чтобы войти под своим логином в онлайновую службу, предоставляемую контролером данных.

(58) Принцип прозрачности требует, чтобы любая информация, предоставляемая общественности или субъекту данных, была лаконичной, легкодоступной и понятной, и чтобы использовался ясный и простой язык, и дополнительно, при необходимости, использовались визуальные элементы. Указанная информация может предоставляться в электронной форме, например, если она адресована общественности, на интернет-сайте. Это имеет существенное значение в ситуациях, когда вследствие большого количества участников и сложности необходимой техники субъекты данных не могут узнать и понять, кем и для каких целей относящиеся к ним персональные данные собираются, например, в случае рекламы в интернете. Исходя из того, что дети требуют особой защиты, любая информация и сообщения, если обработка адресована ребенку, должны быть составлены на ясном, простом и понятном ребенку

языке.

(59) Необходимо предусмотреть условия для содействия осуществлению прав субъекта данных согласно настоящему Регламенту, включая механизмы для запроса и, при необходимости, бесплатного получения, в частности, доступа к персональным данным, их исправления или удаления и осуществления права на возражение. Контролер также должен предусмотреть средства для электронного запроса, особенно, если персональные данные обрабатываются электронным способом. Контролер обязан незамедлительно и как минимум в течение одного месяца ответить на запросы субъекта данных и, если он не намерен удовлетворять просьбу, указать причины.

(60) Принципы справедливой и прозрачной обработки требуют, чтобы субъект данных был проинформирован о наличии процесса обработки и ее целях. Контролер должен предоставить субъекту данных всю дополнительную информацию, необходимую для обеспечения справедливой и прозрачной обработки, с учетом особых обстоятельств и условий, в которых обрабатываются данные. Кроме этого, субъект данных должен быть проинформирован о наличии профиля и его последствиях. Если персональные данные получены от субъекта данных, он также должен быть проинформирован о том, обязан ли он предоставлять персональные данные, а также о последствиях их непредставления. Указанная информация может предоставляться совместно со стандартизированными графическими обозначениями, для того чтобы в отчетливо видимой, понятной и четкой форме дать общее представление о запланированной обработке. Если графические обозначения представлены в электронной форме, они должны быть машиночитаемы.

(61) Информация относительно обработки персональных данных, относящихся к субъекту данных, должна быть предоставлена субъекту данных в момент сбора у него данных или, если персональные данные получены из других источников, в разумный срок, в зависимости от обстоятельств дела. Если персональные данные могут быть на законных основаниях раскрыты другому получателю, субъект данных должен быть проинформирован, если персональные данные впервые раскрываются получателю. Если контролер намерен обрабатывать персональные данные в целях, отличных от целей, для которых они собирались, он до начала обработки должен представить субъекту данных информацию относительно указанной другой цели и иную необходимую информацию. Если информация о происхождении персональных данных не может быть предоставлена субъекту данных вследствие использования разнообразных ресурсов, должна быть предоставлена общая информация.

(62) Однако, обязанность по предоставлению информации может не налагаться, если субъект данных уже обладает информацией, если регистрация или раскрытие персональных данных установлено на законодательном уровне или если предоставление информации субъекту данных невозможно или влечет за собой несоизмеримые усилия. В частности, в том, что касается последнего обстоятельства, это может быть обработка, которая осуществляется в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях. В этой связи необходимо принять во внимание количество субъектов данных, возраст данных и любые соответствующие гарантии.

(63) Субъект данных должен иметь право доступа к относящимся к нему собранным персональным данным; указанное право должно осуществляться беспрепятственно и с определенной периодичностью в целях получения информации об обработке и проверки ее законности. Сюда относится право субъектов данных на доступ к касающимся их здоровья данным, например, данным в их медицинских документах, содержащих следующую информацию: диагнозы, результаты обследований, наблюдения лечащих врачей и сведения о любом лечении или вмешательствах. Вследствие этого каждый субъект данных должен иметь право знать и получать сведения в отношении целей, для которых обрабатываются персональные данные, по возможности, в отношении срока, в течение которого обрабатываются данные, получателей персональных данных, логической схемы любой автоматизированной обработки персональных данных и последствий указанной обработки, если она как минимум основана на формировании профиля. При наличии соответствующей возможности контролер должен обеспечить удаленный доступ к защищенной системе, которая предоставит субъекту данных прямой доступ к его персональным данным. Указанное право не должно отрицательно влиять на права или свободы других лиц, включая коммерческую тайну или результаты интеллектуальной деятельности и, в частности, авторское право на программное обеспечение. Однако указанные ограничения не должны вести к отказу на предоставление всей информации субъекту данных. Если контролер обрабатывает большое количество информации, касающейся субъекта данных, он

должен иметь возможность до передачи информации запросить субъекта данных уточнить информацию или вид обработки, к которому относится запрос.

(64) Контролер должен использовать все приемлемые способы для того, чтобы проверить и подтвердить личность субъекта данных, который подает запрос на доступ, в частности, в рамках онлайновых служб и в случае онлайновых идентификаторов. Контролер не должен сохранять персональные данные только в целях реагирования на потенциальный запрос.

(65) Субъект данных должен иметь право на исправление относящихся к нему персональных данных, а также "право на забвение", если сохранение указанных данных нарушает положения настоящего Регламента или законодательства Союза или государства-члена ЕС, под действие которого подпадает контролер. В частности, субъект данных должен иметь право на удаление своих персональных данных и на то, чтобы его данные больше не обрабатывались, если в персональных данных относительно целей, для которых они собирались или иным образом обрабатывались, больше нет необходимости, если субъект данных аннулировал свое согласие или возражает против обработки относящихся к нему персональных данных или если обработка персональных данных не соответствует настоящему Регламенту. Указанное право имеет существенное значение в случае, когда субъект данных давал свое согласие, будучи ребенком, и полностью не мог осознавать риски, связанные с обработкой, а позже он хочет удалить персональные данные, особенно, в сети Интернет. Субъект данных должен иметь возможность осуществлять указанное право, невзирая на тот факт, что он больше не является ребенком. Однако дальнейшее хранение персональных данных законно, если оно необходимо для осуществление права на свободу выражения мнения и информации, для соблюдения законной обязанности, для выполнения задачи в интересах общества или при осуществлении должностных полномочий контролера, по причинам общественного интереса в области общественного здравоохранения, в целях архивировании в интересах общества, в целях научного или исторического исследования или в статистических целях, или для обоснования, исполнения или оспаривания исковых требований.

(66) Для того чтобы усилить право на забвение в сети, право на удаление следует расширить таким образом, чтобы контролер, который опубликовал персональные данные, был обязан проинформировать контролеров, которые обрабатывают указанные персональные данные, и удалить все ссылки, копии или репликации указанных персональных данных. При этом указанный контролер должен принять соответствующие меры с учетом имеющихся технологических возможностей и доступных средств, включая технические средства, чтобы проинформировать о запросе субъекта данных контролеров, которые обрабатывают персональные данные.

(67) Методы для ограничения обработки персональных данных могут включать в себя, inter alia, временную передачу отобранных данных другой системе обработки, непредставление пользователям отобранных персональных данных или временное удаление опубликованных данных с интернет-сайта. В автоматизированных файловых системах ограничение обработки должно гарантироваться техническими средствами таким образом, чтобы персональные данные не подлежали дальнейшей обработки и не могли быть изменены. Факт того, что обработка персональных данных ограничена, должен быть четко указан в системе.

(68) Для усиления контроля над собственными данными в случае, если обработка персональных данных осуществляется при помощи автоматизированных средств, субъект данных может получить относящиеся к нему персональные данные, которые он предоставил контролеру, в структурированном, широко используемом, машиночитаемом и функционально совместимом формате, и передать их другому контролеру. Контролеры данных должны усовершенствовать функционально совместимые форматы, чтобы способствовать переносимости данных. Указанное право должно применяться, если субъект данных предоставил персональные данные на основании своего согласия или если обработка необходима для исполнения договора. Оно не применяется, если обработка осуществляется на законном основании, не связанном с согласием или договором. По своему характеру указанное право не должно осуществляться в отношении контролеров, обрабатывающих персональные данные при исполнении своих общественных обязанностей. Вследствие этого, оно не должно применяться, если обработка персональных данных необходима для соблюдения законного обязательства, под действие которого подпадает контролер, или для выполнения задачи в интересах общества или при осуществлении должностных обязанностей контролера. Право субъекта данных на передачу или получение относящихся к нему персональных данных

не должно порождать обязательство для контролеров принимать или сохранять технически совместимые системы обработки. Если персональные данные в рамках определенного ряда касаются более одного субъекта данных, право на получение персональных данных должно действовать без ущерба правам и свободам остальных субъектов данных в соответствии с настоящим Регламентом. При этом указанное право не должно наносить ущерб праву субъекта данных на удаление персональных данных и ограничение указанного права согласно настоящему Регламенту и, в частности, не должно подразумевать удаление персональных данных, касающихся субъекта данных, которые были предоставлены им для исполнения договора, в той степени и покуда персональные данные необходимы для исполнения указанного договора. Если это технически возможно, субъект данных должен иметь право на прямую передачу персональных данных от одного контролера другому.

(69) В случае если персональные данные могут обрабатываться на законном основании вследствие того, что обработка необходима для выполнения задачи в интересах общества или при осуществлении должностных полномочий контролера, или на основании законных интересов контролера или третьей стороны, тем не менее, субъект данных должен иметь право на возражение против обработки любых персональных данных, относящихся к определенной ситуации. Контролер должен доказать, что его законный интерес превалирует над интересами или основными правами и свободами субъекта данных.

(70) В случае если персональные данные обрабатываются в целях адресного маркетинга, субъект данных в любое время и на бесплатной основе должен иметь право на возражение против указанной, первоначальной или последующей, обработки, включая формирование профиля, в той степени, в какой обработка связана с указанным адресным маркетингом. Необходимо обратить внимание субъекта данных на указанное право; о нем необходимо сообщить в четкой форме, отдельно от любой другой информации.

(71) Субъект данных должен иметь право на то, чтобы не подпадать под действие решения, которое может включать в себя меру, для оценки относящихся к нему персональных аспектов, которое основано исключительно на автоматизированной обработке и которое порождает юридические последствия в отношении субъекта данных или аналогичным образом существенно влияет на него, например, автоматический отказ в заявке на получение кредита онлайн или онлайновый процесс отбора кадров без вмешательства оператора. Указанная обработка включает в себя "формирования профиля", состоящее из любой формы автоматизированной обработки персональных данных при оценке относящихся к физическому лицу персональных аспектов, в частности, для анализа или прогнозирования аспектов, касающихся производственных показателей указанного лица, экономической ситуации, здоровья, индивидуальных предпочтений, интересов, надежности, поведения, месторасположения или передвижения, если это порождает юридические последствия в отношении субъекта данных или аналогичным образом влияет на него. Однако процесс принятия решения, основанный на указанной обработке, включая формирование профиля, необходимо разрешить, если это допустимо законодательством Союза или государства-члена ЕС, под действие которого подпадает контролер, в том числе в целях мониторинга и предупреждения мошенничества и незаконного сокрытия доходов в соответствии с регламентами, стандартами и рекомендациями институтов Союза или национальных органов надзора, а также для гарантии безопасность и надежности услуги, предоставляемой контролером, или если это необходимо для заключения или исполнения договора между субъектом данных или контролером, или если субъект данных дал свое прямое согласие. В любом случае указанная обработка должна осуществляться в соответствии с надлежащими гарантиями, включающими в себя особое информирование субъекта данных и право на вмешательство оператора, на высказывание своей точки зрения, получение объяснения в отношении решения, принятого после оценки, а также на оспаривание такого решения. Указанная мера не должна касаться ребенка.

Для того чтобы гарантировать справедливую и прозрачную обработку в отношении субъекта данных, с учетом особых обстоятельств и контекста, в котором обрабатываются персональные данные, контролер должен использовать соответствующие математические и статистические методы для формирования профиля, имплементировать технические и организационные меры в целях гарантии того, что факторы, которые приводят к неточностям персональных данных, исправлены, а риски возникновения ошибок минимизированы, защитить персональные данные таким образом, чтобы принять во внимание потенциальные риски для интересов и прав субъекта данных и не допустить дискриминационного воздействия на физических лиц на основе расового или этнического происхождения, политических убеждений, религии и воззрений, членства в профессиональном союзе, генетических

предрасположенностей, состояния здоровья или сексуальной ориентации, или не допустить принятия мер, которые могут иметь указанное воздействие. Автоматизированный процесс принятия решения и формирование профиля на основе особых категорий персональных данных должны осуществляться только при определенных условиях.

(72) Формирование профиля осуществляется в соответствии с положениями настоящего Регламента, регулирующими обработку персональных данных, например, законные основания для обработки или принципы защиты данных. В указанном контексте Европейский совет по защите данных ("Совет") должен иметь возможность издавать руководящие указания.

(73) В законодательстве Союза или государства-члена ЕС могут быть предусмотрены ограничения в отношении особых принципов и прав на получение информации, доступ к данным и исправление или уничтожение персональных данных, в отношении права на переносимость данных, права на возражение, в отношении решений, основанных на формировании профиля, а также в отношении сообщения субъекту данных об утечке персональных данных и в отношении определенных соответствующих обязанностей контролеров, при условии, что это необходимо и пропорционально в демократическом обществе для обеспечения общественной безопасности, в том числе для защиты жизни людей, особенно, вследствие природных и техногенных катастроф, для обеспечения предотвращения и расследования преступлений и уголовного преследования или исполнения наказаний, включая предотвращение угроз общественной безопасности или нарушений этики для регулируемых профессий, для обеспечения других важных целей общественного интереса Союза или государства-члена ЕС, в частности, важного экономического или финансового интереса Союза или государства-члена ЕС; а также в отношении ведения общественных реестров по причинам общественного интереса, дальнейшей обработки архивированных персональных данных для предоставления особой информации, связанной с политическим поведением в бывших тоталитарных режимах, или защиты субъекта данных или прав и свобод других лиц, включая социальную защиту, общественное здравоохранение и гуманитарные цели. Указанные ограничения должны соответствовать требованиям, установленным в Хартии и в Европейской Конвенции о защите прав человека и основных свобод.

(74) Необходимо установить ответственность и обязательства контролера в отношении любой обработки персональных данных, осуществляемой контролером или от его имени. В частности контролер обязан имплементировать соответствующие и эффективные меры и иметь возможность продемонстрировать соответствие обработки настоящему Регламенту, включая эффективность мер. Указанные меры должны учитывать характер, сферу применения, контекст и цели обработки и риск для прав и свобод физических лиц.

(75) Риски для прав и свобод физических лиц, разной степени вероятности и серьезности, могут возникать в результате обработки персональных данных, которая может привести к физическому, материальному или нематериальному ущербу, в частности: если обработка может привести к дискриминации, хищению персональных данных или мошенничеству с персональными данными, финансовым потерям, ущербу для репутации, нарушению конфиденциальности персональных данных, находящихся под защитой профессиональной тайны, несанкционированной отмене псевдонимизации, или к иному неблагоприятному экономическому или социальному положению; если субъекты данных могут быть лишены своих прав и свобод или возможности осуществлять контроль над своими персональными данными; если обрабатываются персональные данные, которые раскрывают расовое или этническое происхождение, политические убеждения, религиозные и философские воззрения, членство в профессиональном союзе, а также генетические данные, данные, касающиеся здоровья или данные о половой жизни или уголовных судимостях и преступлениях или соответствующих мерах безопасности; если оцениваются персональные аспекты, в частности, для анализа или прогнозирования аспектов, касающихся производственных показателей, экономической ситуации, здоровья, индивидуальных предпочтений, интересов, надежности, поведения, месторасположения или передвижения, в целях создания или использования персональных профилей; если обрабатываются персональные данные социально незащищенных физических лиц, в частности, детей; или если обработка охватывает большое количество персональных данных и влияет на большое количество субъектов данных.

(76) Вероятность и серьезность риска для прав и свобод субъекта данных должны определяться исходя из характера, сферы применения, контекста и целей обработки. Риск должен оцениваться на основе

объективной оценки, посредством которой будет установлено, влечет ли обработка данных риск или риск высокой степени.

(77) Руководства по имплементации соответствующих мер и по подтверждению соблюдения требований контролером или обрабатывающим данные лицом, особенно в отношении идентификации риска, связанного с обработкой, оценки относительно происхождения, характера, вероятности и серьезности, а также идентификации передового опыта по снижению риска, могут предоставляться, в частности, в форме утвержденных норм поведения, утвержденных сертификационных процедур, руководящих указаний Совета или указаний инспектора по защите персональных данных. Совет может также издать руководящие указания в отношении обработки, которая рассматривается в качестве обработки, которая не может привести к риску высокой степени для прав и свобод физических лиц, и указать, какие меры могут быть достаточными в указанных случаях для устранения указанного риска.

(78) Защита прав и свобод физических лиц при обработке персональных данных требует принятия соответствующих технических и организационных мер в целях гарантии того, что соблюдаются требования настоящего Регламента. Для того чтобы подтвердить соблюдение настоящего Регламента, контролер должен принять внутренние правила и имплементировать меры, которые, в частности, соответствуют принципам защиты данных по умолчанию и на основе продуманных действий. Указанные меры могут включать, inter alia, минимизацию обработки персональных данных, псевдонимизацию персональных данных в максимально короткие сроки, прозрачность в отношении функций и обработки персональных данных, которые позволят субъекту данных контролировать процесс обработки данных, а контролеру позволят создать и улучшить средства защиты. При разработке, проектировании, выборе и использовании приложений, услуг и товаров, которые основаны на обработке персональных данных или обрабатывают персональные данные для выполнения своих задач, производители товаров, услуг и приложений могут принять во внимание право на защиту данных при разработке и проектировании указанных товаров, услуг и приложений, и с учетом современного состояния техники убедиться в том, что контролеры и обрабатывающие данные лица в состоянии исполнять свои обязанности, связанные с защитой данных. Принципы защиты данных по умолчанию и на основе продуманных действий должны учитываться в контексте публичных торгов.

(79) Защита прав и свобод субъектов данных, а также ответственность и обязанность контролеров и обрабатывающих данные лиц, также в отношении мониторинга со стороны надзорных органов и их мер, требует четкого распределения обязанностей согласно настоящему Регламенту, в том числе, если контролер определяет цели и средства обработки совместно с другими контролерами или если обработка осуществляется от имени контролера.

(80) Если контролер или обрабатывающее данные лицо, не учрежденные в Союзе, обрабатывают персональные данные находящихся в Союзе субъектов данных и если их деятельность по обработке связана с предложением товаров и услуг указанным субъектам данных в Союзе, вне зависимости от того, требуется ли оплата от субъекта данных, или связана с мониторингом их линии поведения постольку, поскольку оно имеет место в Союзе, контролер или обрабатывающее данные лицо должно назначить представителя за исключением случаев, когда обработка носит случайный характер, не включает в себя масштабную обработку специальных категорий персональных данных, или обработка персональных данных, связанных с уголовными приговорами и преступлениями, вероятно, не приведет к возникновению риска для прав и свобод физических лиц, с учетом характера, обстоятельств, сферы применения и целей обработки, или если контролер является органом или учреждением государственной власти. Представитель должен действовать от имени контролера или обрабатывающего данные лица и являться для любого надзорного органа контактным центром. Представитель должен быть назначен посредством письменного предписания контролера или обрабатывающего данные лица на выполнение деятельности от их имени относительно обязанностей согласно настоящему Регламенту. Назначение указанного представителя не влияет на ответственность или обязанности контролера или обрабатывающего данные лица согласно настоящему Регламенту. Указанный представитель должен выполнять свои задачи согласно предписанию, полученному от контролера или обрабатывающего данные лица, включая сотрудничество с компетентными надзорными органами в отношении любых мер, принятых в целях гарантии соблюдения настоящего Регламента. Назначенный представитель подлежит исполнительному производству в случае несоответствия контролера или обрабатывающего данные лица.

(81) Для того чтобы гарантировать соблюдение требований настоящего Регламента в отношении обработки, осуществляемой обрабатывающим данные лицом от имени контролера, при возложении на указанное лицо обязанности по обработке данных контролер должен использовать обрабатывающих данные лиц, которые предусматривают соответствующие гарантии, в частности, в отношении экспертных знаний, надежности и ресурсов, для того чтобы имплементировать технические и организационные меры, которые будут отвечать требованиям настоящего Регламента, в том числе в отношении безопасности обработки. Соблюдение обрабатывающим данные лицом утвержденных норм поведения или утвержденного сертификационного механизма может использоваться в качестве элемента для подтверждения соблюдения обязанностей контролера. Осуществление обработки лицом, обрабатывающим данные, должно регулироваться договором или иным законодательным актом согласно законодательству Союза или государства-члена ЕС, привязывающим обрабатывающее данные лицо к контролеру, устанавливающим предмет и продолжительность обработки, характер и цели обработки, тип персональных данных и категории субъектов данных, с учетом определенных задач и обязанностей обрабатывающего данные лица в контексте обработки и риска для прав и свобод субъекта данных. Контролер и обрабатывающее данные лицо могут по выбору использовать индивидуальный договор или стандартные договорные условия, принятые или Европейской Комиссией, или надзорным органом в соответствии с механизмом сопоставимости, а затем утвержденные Европейской Комиссией. После завершения обработки от имени контролера обрабатывающее данные лицо должно по выбору контролера вернуть или удалить персональные данные, за исключением случаев, когда существует требование о хранении персональных данных в соответствии с законодательством Союза или государства-члена ЕС, под действие которого подпадает обрабатывающее данные лицо.

(82) Для того чтобы подтвердить соблюдение настоящего Регламента, контролер или обрабатывающее данные лицо должны вести учет обработки, осуществляемой под их ответственностью. Каждый контролер и обрабатывающее данные лицо обязано сотрудничать с надзорным органом и по запросу предоставлять в его распоряжение указанные учетные сведения в целях мониторинга процесса обработки.

(83) Для того чтобы обеспечить безопасность и предотвратить обработку в нарушение настоящего Регламента, контролер или обрабатывающее данные лицо должно оценить риски, присущие обработке, и имплементировать меры по снижению указанных рисков, например, криптографическую защиту. Указанные меры должны гарантировать соответствующий уровень защиты, в том числе конфиденциальности, с учетом уровня развития техники и расходов на имплементацию в отношении рисков и характера подлежащих защите персональных данных. При оценке риска для защиты данных необходимо уделить внимание рискам, имеющим место при обработке персональных данных, например, случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или несанкционированному доступу к переданным, сохраненным или иным образом обрабатываемым данным, которые могут привести к физическому, материальному или нематериальному ущербу.

(84) Для того чтобы улучшить соблюдение положений настоящего Регламента, если обработка может привести к риску высокой степени для прав и свобод физических лиц, контролер должен отвечать за выполнение оценки воздействия на защиту данных для того, чтобы определить, в частности, характер, специфику и серьезность указанного риска. Необходимо принять во внимание результат оценки при определении соответствующих мер, которые должны быть приняты для подтверждения того, что обработка персональных данных соответствует настоящему Регламенту. Если оценка воздействия на защиту данных указывает на то, что обработка влечет риск высокой степени, который контролер не может смягчить посредством соответствующих мер в отношении имеющихся технологий и расходов на имплементацию, до начала обработки необходимо проконсультироваться с надзорным органом.

(85) Утечка персональных данных, если она не была вовремя и соответствующим образом устранена, может привести к физическому, материальному или нематериальному ущербу для физических лиц, например, потере контроля над персональными данными или ограничению прав, дискриминации, хищению персональных данных или мошенничеству с данными, финансовым потерям, несанкционированному отказу от псевдонимизации, ущербу репутации, нарушению конфиденциальности персональных данных, защищенных обязанностью соблюдать профессиональную тайну, или любому другому неблагоприятному экономическому или социальному положению для соответствующего лица. Вследствие этого, как только контролеру станет известно об утечке персональных данных, он должен уведомить об этом надзорный

орган незамедлительно и, при наличии возможности, не позднее 72 часов после того, как он узнал об утечке, за исключением случаев, когда контролер способен доказать, в соответствии с принципом предоставления отчетности, что утечка персональных данных не приведет к риску для прав и свобод физических лиц. Если указанное уведомление не может быть сделано в течение 72 часов, причины отсрочки необходимо указать в уведомлении, информация может быть предоставлена поэтапно без дальнейшего промедления.

(86) Контролер незамедлительно должен сообщить субъекту данных об утечке персональных данных, если указанная утечка может привести к возникновению риска высокой степени для прав и свобод физического лица, для того чтобы указанное лицо приняло необходимые меры предосторожности. В сообщении необходимо описать характер нарушения, а также дать рекомендации физическому лицу по снижению возможного негативного воздействия. Указанные сообщения субъектам данных должны быть сделаны как можно быстрее и в тесном сотрудничестве с надзорным органом в соответствии с руководящим указанием данного органа или иного соответствующего органа, например, правоохранительных органов. Например, чтобы снизить непосредственный риск ущерба, необходимо мгновенно уведомить субъекты данных, при этом, если необходимо имплементировать соответствующие меры против продолжения совершения утечки персональных данных, может потребоваться больше времени для общения.

(87) Необходимо удостовериться, все ли соответствующие технологические и организационные меры были имплементированы для того, чтобы незамедлительно установить факт утечки персональных данных и проинформировать об этом надзорный орган и субъект данных. Тот факт, что уведомление необходимо сделать незамедлительно, должен быть установлен с учетом, в частности, характера и серьезности утечки персональных данных, ее последствий и негативного воздействия на субъект данных. Указанное уведомление может привести к вмешательству надзорного органа в соответствии с его задачами и полномочиями, установленными в настоящем Регламенте.

(88) При установлении подробных правил относительно формата и процедур, применяемых к уведомлению об утечке персональных данных, необходимо должное внимание уделить обстоятельствам указанной утечки, в том числе тому, была ли обеспечена защита персональных данных посредством соответствующих технических мер, которые эффективным образом снижают вероятность мошенничества с персональными данными или иных форм противоправного использования данных. Кроме того, указанные правила и процедуры должны учитывать законные интересы правоохранительных органов, если раннее раскрытие данных может воспрепятствовать расследованию обстоятельств утечки персональных данных.

(89) Директива 95/46/ЕС предусматривает общую обязанность по уведомлению надзорных органов об обработке персональных данных. Поскольку указанная обязанность связана с административной и финансовой нагрузкой, она не всегда содействовала улучшению защиты персональных данных. Вследствие этого указанные бессистемные общие обязанности в отношении уведомления должны быть отменены и заменены эффективными процедурами и механизмами, которые фокусируются на тех типах обработки данных, которые могут привести к возникновению риска высокой степени для прав и свобод физических лиц в соответствии с их характером, сферой применения, контекстом и целями. К указанным типам обработки могут относиться, в частности, те типы, которые включают в себя использование новых технологий, или которые сами являются новыми, и если контролер не проводил оценку воздействия на защиту данных или если они необходимы с учетом времени, которое прошло с момента первоначальной обработки.

(90) В указанных случаях оценка воздействия на защиту данных должна осуществляться контролером до обработки данных с тем, чтобы оценить особую вероятность и серьезность риска высокой степени, с учетом характера, сферы применения, контекста и целей обработки, а также источников риска. Указанная оценка воздействия должна включать в себя, в частности, меры, гарантии и механизмы, предусмотренные для устранения указанного риска, гарантии защиты персональных данных и подтверждения соблюдения настоящего Регламента.

(91) В частности, это должно применяться в отношении масштабной обработки, которая направлена на обработку значительного количества персональных данных на региональном, национальном и наднациональному уровне, и может повлиять на большое количество субъектов данных, и может привести

к риску высокой степени, например, на основании их уязвимости, если в соответствии с достигнутым уровнем технологических знаний в большом количестве используются новые технологии, а также в отношении иных видов обработки, которые могут привести к риску высокой степени для прав и свобод субъектов данных, в частности, если указанная обработка затрудняет осуществление прав субъектами данных. Оценка воздействия на защиту данных должна быть проведена, если персональные данные обрабатываются в целях принятия решений в отношении определенных физических лиц в соответствии с систематической и всесторонней оценкой персональных аспектов в отношении физических лиц, основанных на формировании профиля указанных данных, или в соответствии с обработкой особых категорий персональных данных, биометрических данных или данных об уголовных приговорах и преступлениях или о соответствующих мерах безопасности. Оценка воздействия на защиту данных требуется для мониторинга открытых для общего доступа областей, особенно, если используются оптоэлектронные устройства, или для иных действий, если компетентный надзорный орган считает, что обработка может привести к риску высокой степени для прав и свобод субъектов данных, в частности, вследствие того, что они препятствуют субъектам данных осуществлять право или использовать услугу или договор, или вследствие того, что они осуществляются систематически и в большом количестве. Обработка персональных данных не должна считаться масштабной, если она касается персональных данных пациентов или клиентов и осуществляется лечащим врачом, иным медицинским работником или юристом. В указанных случаях оценка воздействия на защиту данных не считается обязательной.

(92) При определенных обстоятельствах может быть приемлемо и целесообразно с экономической точки зрения не относить оценку воздействия на защиту данных к определенному проекту, например, если органы государственной власти или учреждения намерены установить общее применение или платформу для обработки информации или если несколько контролеров планируют ввести общее применение или условие обработки для промышленном сектора, или сегмента, или для широко применяемой горизонтальной деятельности.

(93) В контексте применения законодательства государства-члена ЕС, на основе которого орган государственной власти или частная организация выполняют свои задачи и которое регулирует особый вид обработки или ряд соответствующих обработок, государства-члены ЕС могут счесть необходимым провести указанную оценку до осуществления обработки.

(94) Если оценка воздействия на защиту данных указывает на то, что обработка, при отсутствии гарантий, мер безопасности и механизмов для снижения риска, может привести к высокой степени риска для прав и свобод физических лиц, и контролер считает, что риск не может быть снижен при помощи имеющихся технологических средств и расходов на имплементацию, до начала процесса обработки необходимо проконсультироваться с надзорным органом. Указанная высокая степень риска может возникнуть в результате определенных типов обработки, объема и периодичности обработки, и может также повлечь за собой ущерб или посягательство на права и свободы физического лица. Надзорный орган в установленный срок должен ответить на запрос о проведении консультации. Однако отсутствие ответа надзорного органа в указанный срок действует без ущерба любому вмешательству надзорного органа в соответствии с его задачами и полномочиями, установленными в настоящем Регламенте, включая полномочие на запрет процесса обработки. В рамках процесса консультации результат оценки воздействия на защиту данных, проведенной в отношении рассматриваемой обработки, может быть представлен надзорному органу, в частности, меры по снижению риска для прав и свобод физических лиц.

(95) Обрабатывающее данные лицо должно оказывать содействие контролеру, в соответствующем случае и по запросу, при обеспечении соблюдения обязанностей, возникающих из осуществления оценки воздействия на защиту данных и из предварительной консультации надзорного органа.

(96) Консультация надзорного органа также должна проводиться в ходе подготовки законодательной или регулятивной меры, которая предусматривает обработку персональных данных для обеспечения соответствия запланированной обработки настоящему Регламенту и, в частности, смягчения риска для субъекта данных.

(97) В случае если обработка осуществляется органом государственной власти, за исключением судов или независимых судебных органов, действующих в рамках своей судейской дееспособности, если в частном секторе обработка осуществляется контролером, целевая деятельность которого состоит в

обработке, требующей регулярного и систематического мониторинга субъектов данных, или если целевая деятельность контролера или обрабатывающего данные лица состоит в масштабной обработке специальных категорий персональных данных и данных, связанных с уголовными судимостями и преступлениями, лицо, обладающее экспертными знаниями в области законодательства и практики о защите персональных данных, должно содействовать контролеру или обрабатывающему данные лицу при мониторинге внутреннего соблюдения настоящего Регламента. В частном секторе целевая деятельность контролера относится к его основной деятельности и не относится к обработке персональных данных в качестве вспомогательного вида деятельности. Необходимый уровень экспертных знаний должен определяться, в частности, в соответствии с проведенной обработкой данных и требуемой защитой для персональных данных, обработанных контролером или обрабатывающим данные лицом. Инспекторы по защите персональных данных, вне зависимости от того, являются ли они работниками контролера, должны быть в состоянии независимо исполнять свои обязанности и выполнять свои задачи.

(98) Объединения или иные органы, представляющие определенные категории контролеров или обрабатывающих данные лиц, могут в рамках настоящего Регламента разработать нормы поведения для того, чтобы способствовать эффективному применению настоящего Регламента, при этом необходимо учитывать характеристики обработки, осуществляемой в определенных секторах, и специфические потребности микропредприятий, малых и средних предприятий. В частности, указанные нормы поведения могут точно определять обязательства контролеров и обрабатывающих данные лиц, с учетом риска для прав и свобод физических лиц в результате обработки.

(99) При разработке нормы поведения, при изменении или расширении указанной нормы объединения и иные органы, представляющие определенные категории контролеров или обрабатывающих данные лиц, должны проконсультироваться с соответствующими участниками, и при наличии возможности с субъектами данных, и принять во внимание полученные при этом заключения и мнения.

(100) Для того чтобы повысить прозрачность и улучшить соблюдение настоящего Регламента, необходимо содействовать установлению сертификационных механизмов, а также печатей и маркировочных знаков о защите данных, которые позволят субъектам данных быстро оценить уровень защиты данных соответствующих товаров и услуг.

(101) Потоки данных в третьи страны и международные организации, а также из третьих стран и международных организаций необходимы для расширения внешней торговли и международного сотрудничества. Увеличение объемов указанных потоков привело к новым вызовам и требованиям, связанным с защитой персональных данных. Однако если персональные данные передаются из Союза контролерам, обрабатывающим данные лицам или иным получателям в третьих странах или международным организациям, уровень защиты физических лиц, гарантированный в Союзе настоящим Регламентом, не должен быть ослаблен, в том числе в случаях передачи персональных данных из третьей страны или международной организации контролерам, обрабатывающим данные лицам в той же самой или другой третьей стране или международной организации. В любом случае, передача данных третьим странам и международным организациям может осуществляться только при полном соблюдении положения настоящего Регламента. Передача может осуществляться только, если в соответствии с другими положениями настоящего Регламента, контролер или обрабатывающее данные лицо соблюдает условия, установленные в положениях настоящего Регламента относительно передачи персональных данных третьим странам или международным организациям.

(102) Настоящий Регламент действует без ущерба международным соглашениям между Союзом и третьими странами в отношении передачи персональных данных, включая соответствующие гарантии для субъектов данных. Государства-члены ЕС могут заключить международные соглашения, касающиеся передачи персональных данных третьим странам и международным организациям, поскольку указанные соглашения не влияют на настоящий Регламент или на иные положения законодательства Союза и включают в себя соответствующий уровень защиты основных прав субъектов данных.

(103) Европейская Комиссия может принять действительное для всего Союза решение о том, что третья страна, территория или определенный сектор в третьей стране или международная организация гарантирует соответствующий уровень защиты данных, таким образом обеспечивается юридическая определенность и единообразие на территории Союза в отношении третьей страны или международной

организации, которая гарантирует указанный уровень защиты. В указанных случаях передача персональных данных третьей стране или международной организации может осуществляться без получения дальнейшего разрешения. Европейская Комиссия может также отменить указанное решение и сообщить об этом, с указанием причин, третьей стране или международной организации.

(104) В соответствии с основополагающими ценностями Союза, к которым, в частности, относится защита прав человека, Европейская Комиссия при оценке третьей страны или территории или определенного сектора в третьей стране должна принять во внимание то, каким образом третья страна соблюдает принципы правового государства, обеспечивает доступность правосудия, а также соблюдает нормы и стандарты международного права в области прав человека, основного и секторального законодательства, включая законодательство относительно общественной безопасности, обороны и внутренней безопасности, а также общественный порядок и уголовное законодательство. При принятии решения о соответствии в отношении территории или определенного сектора в третьей стране следует учитывать четкие и объективные критерии, например, определенный вид обработки и область применения правовых стандартов и действующего в третьей стране законодательства. Третья страна должна предоставить гарантии, обеспечивающие соответствующий уровень защиты, эквивалентный уровню, гарантированному в Союзе, в особенности, если персональные данные обрабатываются в одном или нескольких особых секторах. В частности, третья страна должна гарантировать эффективный и независимый мониторинг защиты данных и должна предусмотреть механизмы сотрудничества с органами государств-членов ЕС по защите данных, субъектам данных должны быть предоставлены обеспеченные законодательством эффективные права и эффективные административные и судебные средства защиты.

(105) Наряду с международными обязательствами, которые приняла на себя третья страна или международная организация, Европейская Комиссия должна принять во внимание обязательства, возникающие вследствие участия третьей страны или международной организации в многосторонних или региональных системах, в частности, в отношении защиты персональных данных, а также имплементацию указанных обязательств. В частности, необходимо учесть присоединение третьей страны к Конвенции Совета Европы от 28 января 1981 г. о защите физических лиц при автоматизированной обработке персональных данных и к ее дополнительному протоколу. Европейская Комиссия должна проконсультироваться с Советом при оценке уровня защиты в третьих странах или международных организациях.

(106) Европейская Комиссия должна контролировать исполнение решений об уровне защиты в третьей стране, территории или определенном секторе в третьей стране или в международной организации, а также контролировать исполнение решений, принятых на основе Статьи 25(6) или Статьи 26(4) Директивы 95/46/ЕС. В своих решениях о соответствии Европейская Комиссия должна предусмотреть механизм периодической проверки их исполнения. Периодическая проверка должна проводиться по согласованию с третьей страной или международной организацией и учитывать все соответствующие изменения в третьей стране или международной организации. В целях контроля и осуществления периодических проверок Европейская Комиссия должна учитывать мнения и замечания Европейского Парламента и Совета ЕС, а также всех других соответствующих органов и источников. Европейская Комиссия в приемлемый срок должна оценить исполнение указанных решений и направить отчет со всеми соответствующими выводами Комитету в значении Регламента (ЕС) 182/2011 Европейского Парламента и Совета ЕС <*> в установленном согласно настоящему Регламенту порядке, а также Европейскому Парламенту и Совету ЕС.

<*> Регламент (ЕС) 182/2011 Европейского Парламента и Совета ЕС от 16 февраля 2011 г., устанавливающий правила и общие принципы механизмов контроля со стороны государств-членов ЕС за осуществлением Европейской Комиссией имплементационных полномочий (ОЖ N L 55, 28.02.2011, стр. 13).

(107) Европейская Комиссия может признать, что третья страна, территория или определенный сектор в третьей стране или международная организация больше не гарантируют соответствующий уровень защиты данных. Следовательно, передача данных указанной третьей стране или международной организации должна быть запрещена кроме случаев, когда соблюдаются требования настоящего Регламента в отношении передачи данных в соответствии с приемлемыми гарантиями, включая

юридически обязывающие корпоративные правила, и частичные отступления от определенных ситуаций. В указанном случае следует предусмотреть консультации между Европейской Комиссией и указанными третьими странами или международными организациями. Европейская Комиссия своевременно должна проинформировать третью страну или международную организацию о причинах и начать консультации для устранения возникших затруднений.

(108) При отсутствии решения о соответствии контролер или обрабатывающее данные лицо должно принять меры для восполнения недостатка в защите данных в третьей стране посредством соответствующих гарантий для субъекта данных. Указанные соответствующие гарантии могут включать в себя использование юридически обязывающих корпоративных правил, установленных Европейской Комиссией стандартных условий по защите данных, установленных надзорным органом стандартных условий по защите данных или договорных условий, разрешенных надзорным органом. Указанные гарантии должны обеспечить соблюдение требований по защите данных и прав субъектов данных, связанных с обработкой в Союзе, включая наличие обеспеченных прав субъекта данных и доступность эффективных средств правовой защиты, в том числе права на получение эффективной административной и судебной помощи и требование компенсации в Союзе или в третьей стране. Они должны относиться, в частности, к соблюдению общих принципов в отношении обработки персональных данных, принципов запланированной защиты данных или защиты данных по умолчанию. Передача данных может также осуществляться органами государственной власти или учреждениями совместно с органами государственной власти или учреждениями в третьей стране или с международными организациями с соответствующими обязанностями или задачами, в том числе на основе положений, которые должны быть внесены в административные соглашения, например, протокол о взаимопонимании, с учетом обеспеченных законодательством и эффективных прав для субъектов данных. Разрешение компетентного надзорного органа должно быть получено, если гарантии предусмотрены в административных соглашениях, не имеющих обязательную юридическую силу.

(109) Возможность контролера или обрабатывающего данные лица использовать стандартные условия для защиты данных, утвержденные Европейской Комиссией или надзорным органом, не должна препятствовать контролерам или обрабатывающим данные лицам включать стандартные условия для защиты данных в расширенный договор, например, договор между обрабатывающим данные лицом и иным лицом по обработке данных, а также добавлять иные условия или дополнительные гарантии, при условии, что они прямо или косвенно не противоречат стандартным договорным условиям, утвержденным Европейской Комиссией или надзорным органом, или не причиняют вред основным правам и свободам субъектов данных. Контролеры или обрабатывающие данные лица могут предусматривать дополнительные гарантии посредством договорных обязательств, которые дополняют стандартные условия защиты.

(110) Группа предприятий или группа компаний, участвующих в совместной экономической деятельности, должна иметь возможность использовать утвержденные обязательные корпоративные правила для международной передачи своих данных из Союза организациям в рамках той же группы предприятий или группы компаний, участвующих в совместной экономической деятельности, при условии, что указанные корпоративные правила включают в себя все существенные принципы и защищенные законодательством права для обеспечения соответствующих гарантий передачи или категорий передачи персональных данных.

(111) При определенных условиях необходимо предусмотреть возможность передачи данных, если субъект данных дал свое прямое согласие, если передача носит периодический характер и необходима в рамках договора или судебного иска, вне зависимости от того, происходит ли это в рамках судебной процедуры, административной или внесудебной процедуры, включая процедуру рассмотрения регулятивными органами. Также необходимо предусмотреть возможность передачи данных, если это требуется по важным причинам общественного интереса согласно законодательству Союза или государства-члена ЕС или если передача осуществляется из установленного законодательством реестра и предназначена для ознакомления общественности или лиц, имеющих законный интерес. В последнем случае указанная передача не должна затрагивать все персональные данные или категории данных, содержащиеся в реестре, и, если реестр предназначен для ознакомления лиц, имеющих законный интерес, передача должна осуществляться только по запросу указанных лиц или, если они являются получателями, необходимо полностью учитывать интересы и основные права субъекта данных.

(112) Указанные частичные отступления, в частности, должны применяться в отношении передачи данных, необходимых по важным причинам общественного интереса, например, в случаях международного обмена данными между антимонопольными, налоговыми и таможенными органами, между органами финансового надзора, между службами, отвечающими за социальное обеспечение или общественное здравоохранение, например, в случае прослеживания контакта при инфекционных заболеваниях или в целях сокращения и/или исключения допинга в спорте. Передача персональных данных также считается законной, если она необходима для защиты интереса, который имеет существенное значение для жизненно важных интересов субъекта данных или иного лица, включая физическую неприкосновенность или жизнь, если субъект данных не в состоянии дать свое согласие. При отсутствии решения о соответствии законодательство Союза или государства-члена ЕС может по важным причинам общественного интереса прямо ограничить передачу особых категорий данных третьей стране или международной организации. Государства-члены ЕС должны уведомить об указанных положениях Европейскую Комиссию. Любая передача международной гуманитарной организации персональных данных субъекта данных, который физически или юридически не в состоянии дать свое согласие, в целях выполнения задачи, возложенной Женевской Конвенцией, или в целях соблюдения международного гуманитарного права, применяемого в период вооруженных конфликтов, может рассматриваться в качестве необходимой исходя из важных причин общественного интереса или вследствие того, что она относится к жизненно важному интересу субъекта данных.

(113) Передача, которая может быть квалифицирована как не носящая повторяющийся характер и которая касается только ограниченного числа субъектов данных, также может быть возможна в целях соблюдения законных интересов контролера, если указанные интересы не превалируют над интересами или правами и свободами субъекта данных и если контролер проверил все обстоятельства, связанные с передачей данных. Контролер должен уделить особое внимание характеру персональных данных, цели и продолжительности запланированной обработки, а также ситуации в стране происхождения, третьей стране или стране конечного адресата, а также должен предусмотреть приемлемые гарантии для защиты основных прав и свобод физических лиц при обработке персональных данных. Указанная передача возможна в оставшихся случаях только, когда не применяются иные основания для передачи данных. В целях научного или исторического исследования или в статистических целях следует принять во внимание правомерные ожидания общества относительно расширения знаний. Контролер должен проинформировать надзорный орган и субъекта данных о передаче данных.

(114) В любом случае, если Европейская Комиссия не приняла решения относительно соответствующего уровня защиты данных в третьей стране, контролер или обрабатывающее данные лицо должно использовать решения, посредством которых субъектам данных предоставляются осуществимые и эффективные права в отношении обработки их персональных данных в Союзе после передачи указанных данных с тем, чтобы они могли и дальше пользоваться основными правами и гарантиями.

(115) Некоторые третьи страны принимают законодательные, регламентарные и другие правовые акты, которые предназначены для непосредственного регулирования связанной с обработкой деятельности физических и юридических лиц, которые подпадают под юрисдикцию государств-членов ЕС. Это может включать в себя приговоры судов или трибуналов или решения административных органов в третьих странах, которые требуют от контролера или обрабатывающего данные лица передачи или раскрытия персональных данных и которые не основаны на действующем международном соглашении, например, договоре о взаимной правовой помощи, между запрашивающей третьей страной и Союзом или государством-членом ЕС. Экстерриториальное применение указанных законодательных, регламентарных и иных правовых актов может нарушать международное право и может препятствовать защите физических лиц, гарантированной в Союзе настоящим Регламентом. Передача данных должна быть разрешена только, если соблюдаются условия настоящего Регламента в отношении передачи данных третьим странам. Это, inter alia, может являться случаем, когда разглашение необходимо по причине важного общественного интереса, который признан законодательством Союза или государства-члена ЕС, под действие которого подпадает контролер.

(116) Если персональные данные перемещаются за пределы Союза, это может подвергнуть повышенному риску способность физических лиц осуществлять права на защиту данных, в частности, защитить себя от незаконного использования или разглашения информации. В то же время надзорные органы могут быть не в состоянии рассмотреть жалобу или провести расследование в отношении

деятельности, осуществляемой за пределами границ их государства-члена ЕС. Их попытки сотрудничать в трансграничном контексте также могут быть затруднены недостаточными превентивными или корректирующими полномочиями, противоречивыми правовыми режимами и практическими препятствиями, например, ограничением на ресурсы. Вследствие этого существует необходимость содействовать тесному сотрудничеству между надзорными органами по защите персональных данных для того, чтобы они могли обмениваться информацией и проводить расследования с надзорными органами других стран. В целях разработки механизмов международного сотрудничества для содействия и обеспечения международной взаимной помощи при исполнении законодательства о защите персональных данных, Европейская Комиссия и надзорные органы должны обмениваться информацией и сотрудничать в рамках деятельности, которая связана с осуществлением их полномочий, с компетентными органами в третьих странах на основе взаимности и в соответствии с настоящим Регламентом.

(117) Учреждение надзорных органов в государствах-членах ЕС, уполномоченных на полностью независимое выполнение своих задач и осуществление своих полномочий, является существенным компонентом защиты физических лиц при обработке персональных данных. Государства-члены ЕС должны иметь возможность учреждать более одного надзорного органа, если это соответствует их конституционной, организационной и административной структуре.

(118) Независимость надзорных органов не означает, что они не могут подлежать контролю или мониторингу в отношении своих финансовых расходов или судебному надзору.

(119) В случае если государство-член ЕС учреждает несколько надзорных органов, он должен на законодательном уровне установить механизмы для обеспечения эффективного участия указанных надзорных органов в рамках механизма сопоставимости. Указанное государство-член ЕС должно, в частности, назначить надзорный орган, который будет функционировать в качестве единственного контактного центра для эффективного участия указанных органов в механизме и для обеспечения быстрого и бесперебойного сотрудничества с другими надзорными органами, Советом и Европейской Комиссией.

(120) Каждый надзорный орган должен быть обеспечен финансовыми и кадровыми ресурсами, помещениями и инфраструктурой, необходимой для эффективного выполнения своих задач, в том числе задач, связанных с взаимной помощью и сотрудничеством с другими надзорными органами на территории Союза. Каждый надзорный орган должен иметь отдельный, публичный, годовой бюджет, который может являться частью общего государственного или национального бюджета.

(121) На законодательном уровне в каждом государстве-члене ЕС необходимо установить общие условия для члена или членов надзорного органа; они должны, в частности, предусматривать, что указанные члены назначаются посредством прозрачной процедуры или парламентом, правительством или главой государства члена ЕС на основе предложения правительства, члена правительства, парламента или палаты парламента или независимым надзорным органом, уполномоченный согласно законодательству государства-члена ЕС. Для того чтобы гарантировать независимость надзорного органа, член или члены должны действовать добросовестно, воздерживаться от любых действий, несовместимых с их задачами, и не должны в течение срока действия полномочий участвовать в любой несовместимой возмездной или безвозмездной деятельности. Надзорный орган должен обладать своим собственным персоналом, который выбран надзорным органом или независимым органом, учрежденным в соответствии с законодательством государства-члена ЕС, и который находится в подчинении члена или членов надзорного органа.

(122) Каждый надзорный орган должен быть компетентным на территории своего собственного государства-члена ЕС и осуществлять полномочия и выполнять задачи, возложенные на него в соответствии с настоящим Регламентом. В частности, это относится к обработке в рамках деятельности учреждения контролера или обрабатывающего данные лица на территории его государства-члена ЕС, к обработке персональных данных органами государственной власти или частными организациями, действующими в общественных интересах, к обработке, затрагивающей субъекты данных на его территории, или обработке контролером или обрабатывающим данные лицом, не учрежденным в Союзе, если целью являются субъекты данных, проживающие на его территории. Это также включает в себя обработку жалоб, поданных субъектом данных, проведение расследований о применении настоящего Регламента, а также содействие информированности общественности о рисках, нормах, гарантиях и правах

в отношении обработки персональных данных.

(123) Надзорные органы должны контролировать применение положений настоящего Регламента и способствовать его согласованному применению на территории Союза для защиты физических лиц при обработке их персональных данных и для содействия свободному обращению персональных данных на внутреннем рынке. Для указанной цели надзорные органы должны сотрудничать друг с другом и с Европейской Комиссией, при этом соглашения между государствами-членами ЕС о предоставлении взаимной помощи или о таком сотрудничестве могут не заключаться.

(124) В случае если обработка персональных данных осуществляется в рамках деятельности учреждения контролера или обрабатывающего данные лица в Союза и контролер или обрабатывающее данные лицо учреждены в нескольких государствах-членах ЕС, или если обработка, осуществляемая в рамках деятельности единственного учреждения контролера или обрабатывающего данные лица в Союзе, существенно влияет или может существенно повлиять на субъекты данных в нескольких государствах-членах ЕС, надзорный орган в отношении основного учреждения контролера или обрабатывающего данные лица или в отношении единственного учреждения контролера или обрабатывающего данные лица должен выступать в роли главного органа. Он должен сотрудничать с другими соответствующими органами вследствие того, что учреждение контролера или обрабатывающего данные лица находится на территории их государства-члена ЕС, что на субъекты данных, проживающих на их территории, оказывается существенное воздействие, или что им была подана жалоба. Также если субъект данных, не проживающий в указанном государстве-члене ЕС, подал жалобу, надзорный орган, в который была подана жалоба, должен также являться соответствующим надзорным органом. В рамках своих задач по изданию руководящих указаний по любому вопросу, затрагивающему применение настоящего Регламента, Совет должен иметь возможность издавать указания, в частности, в отношении критериев, которые должны быть приняты во внимание, для того чтобы удостовериться, влияет ли обработка на субъекты данных в нескольких государствах-членах ЕС, а также относительно того, что представляет собой существенное и мотивированное возражение.

(125) Главный орган должен быть вправе принимать юридически обязательные решения в отношении мер, посредством которых осуществляются полномочия, предоставленные ему в соответствии с настоящим Регламентом. В качестве главного органа надзорный орган должен содействовать привлечению надзорных органов к участию в процессе принятия решения, а также их координированию. Если принимается решение относительно полного или частичного отклонения жалобы субъекта данных, указанное решение должно быть принято надзорным органом, в который была подана жалоба.

(126) Решение должно быть согласовано совместно главным надзорным органом и соответствующими надзорными органами и должно быть адресовано основному или единственному учреждению контролера или обрабатывающего данные лица и иметь обязательную силу для контролера и обрабатывающего данные лица. Контролер или обрабатывающее данные лицо должно принять необходимые меры для обеспечения соблюдения настоящего Регламента и для имплементации решения, о котором главный надзорный орган уведомил основное учреждение контролера или обрабатывающего данные лицо в отношении обработки в Союзе.

(127) Каждый надзорный орган, не выступающий в роли главного надзорного органа, должен иметь право на рассмотрение местных случаев, если контролер или обрабатывающее данные лицо учреждено в нескольких государствах-членах ЕС, но предмет особой обработки касается только обработки, осуществляемой в одном государстве-члене ЕС, и только субъектов данных в указанном государстве-члене ЕС, например, если предмет рассмотрения касается обработки персональных данных работников при выполнении особых должностных обязанностей государства-члена ЕС. В указанных случаях надзорный орган незамедлительно должен проинформировать главный надзорный орган об указанном обстоятельстве. После получения соответствующей информации главный надзорный орган должен решить, будет ли он рассматривать дело в соответствии с положением о сотрудничестве между главным надзорным органом и другими соответствующими органами ("механизм сотрудничества и сопоставимости") или надзорный орган, который его проинформировал, должен рассмотреть дело на местном уровне. При решении вопроса относительно рассмотрения дела главный надзорный орган должен принять во внимание, находится ли учреждение контролера или обрабатывающего данные лица в государстве-члене ЕС надзорного органа, который его проинформировал, в целях гарантии эффективного исполнения решения в

отношении контролера или обрабатывающего данные лица. Если главный надзорный орган решает рассматривать дело, проинформировавший его надзорный орган должен иметь возможность представить проект решения, который главный надзорный орган должен принять во внимание при подготовке своего проекта решения в рамках механизма сотрудничества и сопоставимости.

(128) Положения о главном надзорной органе и о механизме сотрудничества и сопоставимости не должны применяться, если обработка осуществляется органами государственной власти или частными организациями в области общественного интереса. В указанных случаях единственным надзорным органом, компетентным осуществлять полномочия, предоставленные ему в соответствии с настоящим Регламентом, должен являться надзорный орган государства-члена ЕС, в котором учрежден орган государственной власти или частная организация.

(129) Для того чтобы обеспечить согласованный мониторинг и исполнение настоящего Регламента в Союзе, надзорный орган в каждом государстве-члене ЕС должен иметь одинаковые задачи и осуществлять эффективные полномочия, в том числе следственные и корректирующие полномочия, полномочия санкций, разрешительные и консультативные полномочия, в частности, в случаях жалоб физических лиц, и без ущерба полномочиям органов уголовного преследования согласно законодательству государства-члена ЕС довести до сведения судебных органов факт нарушения настоящего Регламента и участвовать в судебном процессе. Указанные полномочия также должны включать в себя полномочие по установлению временного или окончательного ограничения на обработку, в том числе запрета. Государства-члены ЕС могут определить иные задачи, связанные с защитой персональных данных согласно настоящему Регламенту. Полномочия надзорных органов должны осуществляться беспристрастно, справедливо и в разумный срок в соответствии с процессуальными гарантиями, установленными в законодательстве Союза или государства-члена ЕС. В частности, каждая мера должна быть соответствующей, необходимой и пропорциональной с учетом гарантии соблюдения настоящего Регламента, принимая во внимание обстоятельства каждого отдельного дела, должна соблюдать право каждого лица быть выслушанным до принятия определенной меры, которая может отрицательно повлиять на него, и не должна допускать излишних расходов и чрезмерных затруднений для соответствующего лица. Следственные полномочия в отношении доступа к помещениям должны осуществляться в соответствии со специальными требованиями в процессуальном законодательстве государства-члена ЕС, например, требованием о получении предварительного судебного разрешения. Каждая юридически обязательная мера надзорного органа должна быть оформлена в письменной форме, должна быть четкой и недвусмысленной, указывать надзорный орган, который принял меру, дату принятия меры, подпись главы или уполномоченного им члена надзорного органа, причины принятия меры и отсылку к праву на эффективное средство правовой защиты. Это не должно исключать дополнительных требований в соответствии с процессуальным законодательством государства-члена ЕС. Принятие юридически обязательного решения подразумевает, что оно может послужить основанием судебному пересмотру в государстве-члене ЕС надзорного органа, который принял решение.

(130) В случае если надзорный орган, в который была подана жалоба, не является главным надзорным органом, главный надзорный орган должен тесно сотрудничать с надзорным органом, в который была подана жалоба, в соответствии с положениями о сотрудничестве и сопоставимости, установленными в настоящем Регламенте. В указанных случаях главный надзорный орган при принятии мер, которые должны породить юридические последствия, включая наложение административных штрафов, должен учесть мнение надзорного органа, которому была подана жалоба и который должен оставаться компетентным при осуществлении расследования на территории его собственного государства-члена ЕС совместно с компетентным надзорным органом.

(131) В случае если другой надзорный орган должен выступать в качестве главного надзорного органа в отношении обработки контролера или обрабатывающего данные лица, но конкретный предмет жалобы или возможное нарушение касается только обработки контролера или обрабатывающего данные лица в государстве-члене ЕС, в котором жалоба была подана или было обнаружено возможное нарушение, и обстоятельство дела существенно не влияет или не должно влиять на субъекты данных в других государствах-членах ЕС, надзорный орган, в который подается жалоба или который установил или иным образом был проинформирован о ситуациях, которые влекут за собой возможные нарушения настоящего Регламента, должен прилагать усилия для мирного разрешения споров с контролером и, если это окажется безрезультатным, должен использовать все свои полномочия. Это должно включать в себя следующее:

особую обработку на территории государства-члена ЕС надзорного органа или в отношении субъектов данных на территории указанного государства-члена ЕС; обработку в рамках предложения товаров или услуг, предназначенных для субъектов данных на территории государства-члена ЕС надзорного органа; или обработку, которая должна быть оценена с учетом соответствующих правовых обязательств согласно законодательству государства-члена ЕС.

(132) Мероприятия надзорного органа, направленные на повышение осведомленности населения, должны включать в себя специальные меры в отношении контролеров и обрабатывающих данные лиц, включая микропредприятия, малые и средние предприятия, а также физических лиц, в частности, в сфере образования.

(133) Надзорные органы должны поддерживать друг друга при выполнении своих задач и оказывать взаимную помощь, чтобы обеспечить согласованное применение и исполнение настоящего Регламента на внутреннем рынке. Надзорный орган, запросивший предоставление взаимной помощи, может принять временную меру, если он не получит ответ на свой запрос о взаимной помощи в течение одного месяца после получения указанного запроса другим надзорным органом.

(134) Каждый надзорный орган должен, при необходимости, участвовать в совместной деятельности с другими надзорными органами. Запрашиваемый надзорный орган обязан ответить на запрос в течение определенного срока.

(135) В целях обеспечения согласованного применения настоящего Регламента на территории Союза необходимо установить механизм сопоставимости для сотрудничества между надзорными органами. Указанный механизм, в частности, должен применяться, если надзорный орган намерен принять меру для порождения юридических последствий в отношении процесса обработки, который существенно влияет на определенное количество субъектов данных в нескольких государствах-членах ЕС. Он также должен применяться, если соответствующий надзорный орган или Европейская Комиссия запрашивают рассмотрение указанного вопроса в рамках механизма сопоставимости. Указанный механизм должен действовать без ущерба любым мерам, которые Европейская Комиссия может принять при осуществлении своих полномочий согласно Договорам.

(136) При применении механизма сопоставимости Совет в течение определенного промежутка времени должен дать заключение, если так решает большинство его членов или если так запросил любой соответствующий надзорный орган или Европейская Комиссия. Совет должен также обладать полномочием на принятие юридически обязательных решений, если существуют разногласия между надзорными органами. Для указанной цели в четко определенных случаях он большинством в две трети голосов своих членов должен принять юридически обязательные решения, если между надзорными органами, в частности, в рамках механизма сотрудничества между главным надзорным органом и соответствующими надзорными органами, имеются противоречия по существу дела, в частности, по вопросу о нарушении настоящего Регламента.

(137) Может существовать острая необходимость для защиты прав и свобод субъектов данных, в частности, если имеется риск того, что осуществление права субъекта данных может быть затруднено. Вследствие этого надзорный орган должен иметь возможность принять должным образом обоснованные временные меры на своей территории с определенным сроком действия, который не должен превышать трех месяцев.

(138) Применение указанного механизма в случаях, когда оно обязательно, должно являться условием законности меры надзорного органа, которая порождает юридические последствия. В других случаях трансграничной обоснованности должен применяться механизм сотрудничества между главным надзорным органом и соответствующими надзорными органами; соответствующие надзорные органы могут на двусторонней или многосторонней основе предоставлять взаимную помощь и осуществлять совместные действия без использования механизма сопоставимости.

(139) В целях содействия согласованному применению настоящего Регламента Совет должен быть учрежден в качестве независимого органа Союза. Для достижения своей цели Совет должен обладать правосубъектностью. Совет должен быть представлен Президиумом. Он заменяет Рабочую группу по защите физических лиц при обработке персональных данных, учрежденную Директивой 95/46/ЕС. Он

должен включать в себя главу надзорного органа каждого государства-члена ЕС и Европейского инспектора по защите персональных данных или их представителей. Европейская Комиссия должна принимать участие в деятельности Совета без права голоса, Европейский инспектор по защите данных должен обладать специальным правом голоса. Совет должен способствовать согласованному применению настоящего Регламента в Союзе, в том числе посредством консультирования Европейской Комиссии, в частности, в отношении уровня защиты в третьих странах или международных организациях, а также посредством содействия сотрудничеству надзорных органов в Союзе. Совет должен действовать независимо при выполнении своих задач.

(140) Совету оказывает содействие секретариат, который обеспечивается Европейским инспектором по защите персональных данных. Персонал Европейского инспектора по защите персональных данных, который участвует в осуществлении задач, возложенных на Совет настоящим Регламентом, должен выполнять свои задачи только на основании указаний Президиума Совета, он также должен представлять ему отчеты.

(141) Каждый субъект данных обладает правом на подачу жалобы в один надзорный орган, в частности, в государстве-члене ЕС места своего проживания, и правом на эффективное средство судебной защиты в соответствии со Статьей 47 Хартии, если субъект данных считает, что его права согласно настоящему Регламенту нарушены, или если надзорный орган не принимает меры в отношении жалобы, полностью или частично отклоняет жалобу или отказывает в ее удовлетворении или не действует, если такая мера необходима для защиты прав субъекта данных. На основании жалобы следует провести расследование в соответствии с судебным пересмотром в той мере, в какой это необходимо в особом случае. Надзорный орган в приемлемый срок должен проинформировать субъекта данных о ходе и результатах рассмотрения жалобы. Если дело требует дальнейшего расследования или сотрудничества с другим надзорным органом, субъекту данных должна быть представлена промежуточная информация. В целях содействия рассмотрению жалобы каждый надзорный орган должен принять такие меры, как предоставление формы жалобы, которая может быть заполнена электронным способом, не исключая других средств связи.

(142) В случае если субъект данных считает, что его права согласно настоящему Регламенту нарушены, он вправе передать некоммерческому органу, организации или объединению, которые были основаны в соответствии с законодательством государства-члена ЕС, имеют уставные задачи в сфере общественного интереса, а также осуществляют деятельность в области защиты персональных данных, право подавать в надзорный орган жалобу от его имени, осуществлять права на судебную защиту от имени субъектов данных или в случаях, предусмотренных законодательством государства-члена ЕС, осуществлять право на получение компенсации от его имени субъектов данных. Государство-член ЕС может предусмотреть, что любой такой орган, организация или объединение, независимо от поручения субъекта данных, имеет право подавать в указанном государстве-члене ЕС жалобу и право на эффективное средство судебной защиты, если он считает, что права субъектов данных были нарушены в результате обработки данных, которая нарушает настоящий Регламент. Указанному органу, организации или объединению можно запретить требовать компенсацию от имени субъекта данных, независимо от поручения субъекта данных.

(143) Любое физическое или юридическое лицо имеет право на возбуждение судебного процесса об аннулировании решений Совета согласно условиям, предусмотренным в Статье 263 TFEU. В качестве адресатов таких решений соответствующие надзорные органы, которые хотят их оспорить, должны предъявить иск в течение двух месяцев с момента получения уведомления об указанных решениях в соответствии со Статьей 263 TFEU. Если решения Совета касаются непосредственно и персонально контролера, обрабатывающего данные лица или заявителя, указанные лица могут возбудить судебный процесс об аннулировании указанных решений в течение двух месяцев после их опубликования на интернет-сайте Совета в соответствии со Статьей 263 TFEU. Без ущерба указанному праву согласно Статье 263 TFEU каждое физическое или юридическое лицо должно иметь право на эффективное средство защиты в компетентном национальном суде в отношении решения надзорного органа, которое порождает юридические последствия в отношении указанного лица. Указанное решение касается, в частности, осуществления следственных, корректирующих и разрешительных полномочий надзорного органа или отклонения жалобы или отказа в ее удовлетворении. Однако право на эффективное средство судебной защиты не включает в себя принятые надзорным органом меры, которые не являются юридически

обязательными, например, его заключения или рекомендации. Судебное производство в отношении надзорного органа должно быть возбуждено в судах государства-члена ЕС, в котором учрежден надзорный орган, и должно осуществляться в соответствии с процессуальным законодательством указанного государства-члена ЕС. Указанные суды должны осуществлять юрисдикцию, которая должна включать в себя полномочия на изучение всех вопросов факта и права, относящихся к рассматриваемому ими спору.

Если надзорный орган отклоняет жалобу или отказывает в ее удовлетворении, заявитель может возбудить производство в судах того же самого государства-члена ЕС. В контексте судебной защиты прав в отношении применения настоящего Регламента национальные суды, которые считают, что для вынесения судебного решения им необходимо решение по указанному вопросу, могут или в случае, предусмотренном в Статье 267 TFEU, должны запросить Европейский суд о вынесении предварительного постановления о толковании законодательства Союза, в том числе настоящего Регламента. Также, если решение надзорного органа, имплементирующее решение Совета, оспаривается в национальном суде и действительность решения Совета является спорной, указанный национальный суд не обладает полномочием признавать решение Совета недействительным, но должен передать вопрос о действительности Европейскому суду в соответствии со Статьей 267 TFEU в толковании Европейского суда, если он считает решение недействительным. Однако национальный суд может не передавать вопрос о действительности решения Совета по запросу физического или юридического лица, которое имело возможность возбудить производство об аннулировании указанного решения, в частности, если указанное решение напрямую и персонально касалось его, но не сделало этого в срок, указанный в Статье 263 TFEU.

(144) В случае если суд, начавший производство против решения надзорного органа, имеет основание полагать, что производство, касающееся той же самой обработки, например, того же самого предмета рассмотрения в отношении обработки одним и тем же контролером или обрабатывающим данные лицом, или тех же оснований для иска, возбуждено в компетентном суде в другом государстве-члене ЕС, он должен связаться с указанным судом для того, чтобы подтвердить существование указанного соответствующего производства. Если соответствующее производство рассматривается в суде другого государства-члена ЕС, любой суд, рассматривающий дело позже, может приостановить производство по делу или по заявлению одной из сторон может отказаться от юрисдикции в пользу суда, который начал рассмотрение дела, если указанный суд уполномочен рассматривать указанные дела и его законодательство разрешает объединение соответствующих производств. Производства считаются смежными, если они настолько тесно взаимосвязаны, что целесообразно рассмотреть их вместе, для того чтобы избежать риска принятия противоречащих друг другу приговоров в результате отдельных производств.

(145) В случае производства в отношении контролера или обрабатывающего данные лица истец может возбудить дело в судах государств-членов ЕС, в которых находится учреждение контролера или обрабатывающего данные лица или в которых проживает субъект данных, за исключением случаев, когда контролер является органом государственной власти государства-члена ЕС, действующим при осуществлении своих официальных полномочий.

(146) Контролер или обрабатывающее данные лицо должно компенсировать любой ущерб, который лицо может понести в результате обработки, нарушающей настоящий Регламент. Контролер или обрабатывающее данные лицо освобождается от ответственности, если оно докажет, что оно никоим образом не несет ответственность за ущерб. Понятие ущерба должно широко толковаться в свете прецедентной практики суда таким образом, чтобы полностью соответствовать целям настоящего Регламента. Это положение действует без ущерба любым искам о возмещении ущерба в результате нарушения других норм законодательства Союза или государства-члена ЕС. Обработка, которая нарушает настоящий Регламент, также включает в себя обработку, которая нарушает делегированные акты и имплементационные акты, принятые в соответствии с настоящим Регламентом и с законодательством государства-члена ЕС для уточнения положений настоящего Регламента. Субъекты данных должны получить полную и эффективную компенсацию за понесенный ими ущерб. В случае если контролеры или обрабатывающие данные лица участвуют в одной и той же обработке данных, каждый контролер или обрабатывающее данные лицо должно нести ответственность за ущерб в целом. Однако если они в соответствии с законодательством государства-члена ЕС привлекаются к одному и тому же судебному процессу, компенсация может быть соразмерно распределена согласно ответственности каждого контролера или обрабатывающего данные лица за ущерб, причиненный обработкой, при условии гарантии

полной и эффективной компенсации для понесшего ущерб субъекта данных. Любой контролер или обрабатывающее данные лицо, которое заплатило полную компенсацию, может впоследствии обратиться в суд с регрессным требованием относительно других контролеров или обрабатывающих данные лиц, участвовавших в одной и той же обработке.

(147) В случае если в настоящем Регламенте содержаться особые нормы о юрисдикции, в частности, относительно процедуры о судебной защите прав, в том числе о получении компенсации от контролера или обрабатывающего данные лица, общие нормы о юрисдикции, например положения Регламента (ЕС) 1215/2012 Европейского Парламента и Совета ЕС <*>, должны действовать без ущерба применению указанных особых норм.

<*> Регламент (ЕС) 1215/2012 Европейского Парламента и Совета ЕС от 12 декабря 2012 г. о юрисдикции, признании и исполнении судебных решений по гражданским и коммерческим делам (ОЖ N L 351, 20.12.2012, стр. 1).

(148) В интересах последовательного осуществления положений настоящего Регламента, санкции, в том числе административные штрафы, должны налагаться за любое нарушение настоящего Регламента, в дополнение или вместо соответствующих мер, налагаемых надзорным органом согласно настоящему Регламенту. В случае если нарушение незначительное или если вероятное наложение штраф может повлечь несоразмерную нагрузку для физического лица, вместо штрафа может быть объявлен выговор. Однако следует принять во внимание характер, тяжесть и продолжительность нарушения, преднамеренный характер нарушения, меры, принятые для смягчения причиненного ущерба, степень ответственности или любые другие ранее совершенные нарушения, способ, посредством которого надзорному органу стало известно о нарушении, соблюдение мер, принятых в отношении контролера или обрабатывающего данные лица, соблюдение нормы поведения, а также любые другие отягчающие или смягчающие вину обстоятельства. Для назначения наказаний, в том числе для наложения административных штрафов, необходимо наличие соответствующих процессуальных гарантий в соответствии с общими принципами законодательства Союза и Хартии, включая эффективную судебную защиту и должную правовую процедуру.

(149) Государства-члены ЕС могут установить нормы об уголовном наказании за нарушение настоящего Регламента, включая нарушения национальных положений, принятых согласно и в рамках настоящего Регламента. Указанные уголовные наказания могут также предусматривать лишение преимуществ, полученных вследствие нарушения настоящего Регламента. Однако наложение уголовных наказаний за нарушения указанных национальных положений и наложение административных штрафов не должны вести к нарушению принципа ne bis in idem в толковании Суда.

(150) Для того чтобы гармонизировать и усилить воздействие административных наказаний за нарушения настоящего Регламента, каждый надзорный орган должен обладать полномочием налагать административные штрафы. В настоящем Регламенте должны быть указаны нарушения, а также верхнее ограничение и критерии для установления соответствующих административных штрафов, которые должны определяться компетентным надзорным органом в каждом отдельном случае, принимая во внимание все соответствующие обстоятельства специфической ситуации, с учетом, в частности, характера, тяжести и продолжительности нарушения и его последствий, а также мер, принятых для обеспечения соблюдения обязанностей согласно настоящему Регламенту и для предотвращения или смягчения последствий нарушения. В случае если административные штрафы налагаются на предприятие, для указанных целей оно должно являться предприятием в значении Статей 101 и 102 TFEU. Если административные штрафы налагаются на физических лиц, в отношении которых речь не идет о предприятии, надзорный орган при определении соответствующего размера штрафа должен принять во внимание общий уровень дохода в государстве-члене ЕС, а также экономическую ситуацию физического лица. Для содействия согласованному применению административных штрафов также может использоваться механизм сопоставимости. Государства-члены ЕС могут определить, подлежат ли надзорные органы административным штрафам и если да, то в какой мере. Наложение административного штрафа или выдача предупреждения не влияет на применение иных полномочий надзорных органов или других санкций в рамках настоящего Регламента.

(151) Правовая система Дании и Эстонии не допускает административные штрафы, предусмотренные в настоящем Регламенте. Нормы об административных штрафах могут применяться таким образом, что в Дании штраф налагается компетентными национальными судами в качестве уголовного наказания, в Эстонии штраф налагается надзорным органом в рамках процедуры административного правонарушения, при условии, что применение норм в указанных государствах-членах ЕС имеет воздействие, эквивалентное воздействию административных штрафов, налагаемых надзорными органами. Вследствие этого компетентные национальные суды должны учитывать рекомендации надзорного органа, инициировавшего наложение штрафа. В любом случае налагаемые штрафы должны быть эффективными, пропорциональными и оказывать сдерживающее воздействие.

(152) В случае если настоящий Регламент не гармонизирует административные наказания или если это необходимо в других случаях, например, в случае серьезных нарушений настоящего Регламента, государства-члены ЕС должны имплементировать систему, которая предусматривает эффективные, пропорциональные и оказывающие сдерживающее воздействие санкции. Характер указанных санкций, уголовный или административный, должен определяться в соответствии с законодательством государства-члена ЕС.

(153) В законодательстве государств-членов ЕС должны быть согласованы нормы, регулирующие свободу выражения мнений и свободу информации, включая свободу журналистского, научного, художественного и/или литературного самовыражения, с правом на защиту персональных данных согласно настоящему Регламенту. Обработка персональных данных только в журналистских целях или в целях научного, художественного или литературного самовыражения подлежит частичному отступлению или исключению из определенных положений настоящего Регламента, если это необходимо для того, чтобы согласовать право на защиту персональных данных со свободой выражения мнений и информации согласно Статье 11 Хартии. Это положение должно применяться, в частности, в отношении обработки персональных данных в аудиовизуальной области, а также в новостных и печатных архивах. Вследствие этого, государства-члены ЕС должны принять законодательные меры, регулирующие исключения и отступления, необходимые для целей гармоничного сочетания указанных основных прав. Государства-члены ЕС должны принять указанные отступления и исключения в отношении общих принципов, прав субъектов данных, контролера и обрабатывающего данные лица, передачи персональных данных третьим странам или международным организациям, независимых надзорных органов, сотрудничества и сопоставимости, и особых ситуаций обработки данных. Если указанные отступления или исключения отличаются от одного государства-члена ЕС к другому, должно применяться законодательство государства-члена ЕС, под действие которого подпадает контролер. Для того чтобы принять во внимание важность права на свободу выражения мнения в каждом демократическом обществе, необходимо разъяснить понятия, относящиеся к указанной свободе, например, понятие "журналистика".

(154) Настоящий Регламент учитывает принцип доступа общественности к официальным документам при применении настоящего Регламента. Доступ общественности к официальным документам может рассматриваться в качества общественного интереса. Персональные данные в документах, которые находятся в распоряжении органов государственной власти или правительственных учреждений, должны быть опубликованы указанными органами или учреждениями, если раскрытие информации предусмотрено законодательством Союза или государства-члена ЕС, под действие которого подпадает орган государственной власти или правительственное учреждение. Указанное законодательство должно согласовывать доступ общественности к официальным документам и вторичное использование информации публичного сектора с правом на защиту персональных данных и вследствие этого может предусмотреть необходимое согласование с правом на защиту персональных данных согласно настоящему Регламенту. Ссылка на органы государственной власти и учреждения должна включать в себя в указанном контексте все органы или другие учреждения, подпадающие под действие законодательства государства-члена ЕС о доступе общественности к документам. Директива 2003/98/ЕС Европейского Парламента и Совета ЕС <*> не затрагивает и никоим образом не влияет на уровень защиты физических лиц в отношении обработки персональных данных в рамках положений законодательства Союза или государства-члена ЕС, а также, в частности, не изменяет обязанности и права, установленные в настоящем Регламенте. В частности, указанная Директива не применяется в отношении документов, доступ к которым исключен или ограничен в силу действия режимов доступа по причинам защиты персональных данных, или в отношении части документов, которые доступны в силу указанных режимов, если они содержат персональные данные, вторичное использование которых предусмотрено законодательством,

несовместимым с законодательством относительно защиты персональных данных при обработке персональных данных.

<*> Директива 2003/98/ЕС Европейского Парламента и Совета ЕС от 17 ноября 2003 г. о вторичном использовании информации публичного сектора (ОЖ N L 345, 31.12.2003, стр. 90).

(155) В законодательстве государства-члена ЕС или коллективных договорах, в том числе в "договорах о производстве работ", могут быть предусмотрены специальные положения об обработке персональных данных работников при выполнении должностных обязанностей, в частности, условия, согласно которым персональные данные могут обрабатываться на основе согласия работника, в целях приема на работу, выполнения трудового договора, включая исполнение обязательств, установленных в соответствии с законодательством или коллективным договором, в целях управления, планирования и организации работы, равноправия и многообразия на рабочем месте, охраны труда и производственной безопасности, а также в целях осуществления связанных с занятостью индивидуальных или коллективных прав и гарантий и в целях прекращения трудовых отношений.

(156) Обработка персональных данных в целях архивирования в интересах общества, в целях научного или исторического исследования, а также в статистических целях должна подлежать соответствующим гарантиям для прав и свобод субъекта данных согласно настоящему Регламенту. Указанные гарантии должны обеспечить наличие технических и организационных мер, для того чтобы, в частности, гарантировать принцип минимизации данных. Дальнейшая обработка персональных данных в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях должна осуществляться, если контролер оценил технические возможности для достижения указанных целей посредством обработки данных, при которой невозможно провести идентификацию субъектов данных, при условии, что имеются соответствующие гарантии (например, псевдонимизация данных). Государства-члены ЕС должны предусмотреть соответствующие гарантии для обработки персональных данных в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях. Государства-члены ЕС вправе на специальных условиях и согласно соответствующим гарантиям для субъектов данных предусмотреть спецификации и частичные отступления относительно требований к информации, а также относительно прав на исправление, уничтожение, на забвение, ограничение обработки, на переносимость данных, на возражение, если персональные данные обрабатываются в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях. В рамках соответствующих условий и гарантий могут быть предусмотрены специальные процедуры для осуществления указанных прав субъектами данных, если это соответствует целям особой обработки, в сочетании с техническими и организационными мерами, направленными на минимизацию обработки персональных данных согласно принципам пропорциональности и необходимости. Обработка персональных данных в научных целях должна также соответствовать другим законодательным актам, например, о клинических испытаниях.

(157) Путем объединения информации из реестров исследователи могут получать новые сведения большой ценности в отношении распространенных медицинских состояний таких, как сердечнососудистые заболевания, рак и депрессивный синдром. Посредством использования реестров могут быть получены улучшенные результаты исследований, так как они основываются на большей части населения. В рамках общественных наук исследование на основе реестров дает исследователям возможность получить существенные знания о долговременном соотношении ряда социальных условий, например, безработицы и образования, с другими условиями жизни. Результаты исследований, полученные посредством реестров, обеспечивают твердые и достоверные знания, которые могут являться основанием для разработки и имплементации политических мер, основанных на знаниях, а также могут улучшить качество жизни ряда лиц и повысить эффективность общественных услуг. Для облегчения научных исследований персональные данные могут обрабатываться в целях научного исследования согласно соответствующим условиям и гарантиям, предусмотренным в законодательстве Союза или государства-члена ЕС.

(158) Настоящий Регламент также применяется в отношении обработки персональных данных в целях архивирования; необходимо учесть, что настоящий Регламент не применяется в отношении умерших лиц. Органы государственной власти, правительственные учреждения или частные организации, которые ведут

учет общественного интереса, согласно законодательству Союза или государства-члена ЕС должны быть юридически обязаны получать, сохранять, оценивать, классифицировать, описывать, сообщать, содействовать, распространять учетные сведения непреходящей ценности в интересах общества, а также предоставлять к ним доступ. Государства-члены ЕС также вправе предусмотреть дальнейшую обработку персональных данных в целях архивирования, например, в отношении представления специальной информации, относящейся к политическому поведению в прежних тоталитарных режимах, геноциду, преступлениям против человечества, в частности, Холокосту, или военным преступлениям.

(159) Настоящий Регламент также применяется в отношении обработки персональных данных в целях научного исследования. В целях настоящего Регламента обработка персональных данных для целей научного исследования должна трактоваться более широко, включая, например, развитие технологий и презентацию, фундаментальные исследования, прикладные исследования и исследования, финансируемые за счет частных средств. В дополнение к этому также необходимо принять во внимание цель Союза согласно Статье 179(1) TFEU о создании Европейского исследовательского пространства. Цели научного исследования также должны включать в себя исследования, проводимые в интересах общества в сфере общественного здравоохранения. Для того чтобы соответствовать особенностям обработки персональных данных в целях научных исследований, необходимо применять специальные условия, в частности, в отношении публикации или иного раскрытия персональных данных в контексте целей научного исследования. Если результат научного исследования, в частности, в сфере здравоохранения обосновывает принятие дальнейших мер в интересах субъекта данных, общие положения настоящего Регламента должны применяться в отношении указанных мер.

(160) Настоящий Регламент также применяется в отношении обработки персональных данных в целях исторического исследования. Сюда относится историческое исследование и исследование в области генеалогии, с учетом того, что настоящий Регламент не применяется в отношении умерших лиц.

(161) В целях согласия на участие в научно-исследовательской деятельности в рамках клинических испытаний должны применяться соответствующие положения Регламента (ЕС) 536/2014 Европейского Парламента и Совета ЕС <*>.

<*> Регламент (ЕС) 536/2014 Европейского Парламента и Совета ЕС от 16 апреля 2014 г. о клинических испытаниях лекарственных средств, предназначенных для использования человеком, и об отмене Директивы 2001/20/ЕС (ОЖ N L 158, 27.05.2014, стр. 1).

(162) Настоящий Регламент применяется в отношении обработки персональных данных в статистических целях. Законодательство Союза или государства-члена ЕС в рамках настоящего Регламента должно определить статистическое содержание, контроль доступа, спецификации для обработки персональных данных в статистических целях и соответствующие меры для гарантии прав и свобод субъекта данных и для обеспечения статистической конфиденциальности. Под понятием "статистические цели" понимается любая деятельность по сбору и обработке персональных данных, необходимых для статистического изучения или для подготовки статистических результатов. Указанные статистические результаты могут быть в дальнейшем использованы в других целях, в том числе в целях научного исследования. Статистическая цель подразумевает, что результатом обработки в статистических целях являются не персональные данные, а сводные данные, и что указанный результат или персональные данные не используются для обеспечения выполнения мер и решений, относящихся к определенному физическому лицу.

(163) Конфиденциальная информация, которую национальные статистические органы и статистические органы Союза собирают для подготовки официальной европейской и официальной национальной статистики, должна находиться под защитой. Европейские статистические данные должны разрабатываться, подготавливаться и распространяться в соответствии со статистическими принципами, установленными в Статье 338(2) TFEU; при этом национальные статистические данные также должны соответствовать законодательству государства-члена ЕС. Регламент (ЕС) 223/2009 Европейского Парламента и Совета ЕС <*> предусматривает дополнительные спецификации относительно статистической конфиденциальности европейской статистики.

<*> Регламент (ЕС) 223/2009 Европейского Парламента и Совета ЕС от 11 марта 2009 г. о Европейской статистике и об отмене Регламента (ЕС, Евратом) 1101/2008 Европейского Парламента и Совета ЕС о передаче данных при условии соблюдения их конфиденциальности Статистическому бюро Европейских Сообществ, Регламента (ЕС) 322/97 Совета ЕС о статистике Сообщества, а также Решения 89/382/ЕЭС Совета ЕС, Евратома об учреждении комитета по статистическим программам Европейских Сообществ (ОЖ N L 87, 31.03.2009, стр. 164).

(164) В том, что касается полномочий надзорных органов в отношении получения от контролера или обрабатывающего данные лица доступа к персональным данным и доступа к их помещениям, государства-члены ЕС могут на законодательном уровне, в рамках настоящего Регламента принять особые нормы для обеспечения обязанностей по соблюдению профессиональной или иной эквивалентной тайны, в той мере, в какой это необходимо для согласования права на защиту персональных данных с обязанностью соблюдать профессиональную тайну. Это положение действует без ущерба существующим обязанностям государства-члена по принятию норм относительно соблюдения профессиональной тайны, если этого требует законодательство Союза.

(165) В соответствии со Статьей 17 TFEU настоящий Регламент соблюдает и не ухудшает статус церквей и религиозных организаций или общин в государствах-членах ЕС, согласно существующему конституционному праву.

(166) Для достижения целей настоящего Регламента, а именно защиты основных прав и свобод физических лиц и, в частности, их права на защиту персональных данных и обеспечения свободного обращения персональных данных в Союзе, полномочие по принятию актов в соответствии со Статьей 290 TFEU должно быть делегировано Европейской Комиссии. В частности, делегированные акты должны приниматься в отношении критериев и требований для сертификационных механизмов, информации, представленной посредством стандартизированных графических обозначений, и процедур для предоставления указанных обозначений. Особое значение имеет то, что Европейская Комиссия осуществляет соответствующие консультации в ходе подготовительной работы, в том числе на экспертном уровне. При подготовке и составлении делегированных актов Европейская Комиссия должна гарантировать одновременную, своевременную и соответствующую передачу релевантных документов Европейскому Парламенту и Совету ЕС.

(167) Для того чтобы гарантировать единообразные условия имплементации настоящего Регламента, имплементационные полномочия должны быть предоставлены Европейской Комиссии, если это предусмотрено настоящим Регламентом. Указанные полномочия должны осуществляться в соответствии с Регламентом (ЕС) 182/2011. В рамках указанных полномочий Европейская Комиссия должна рассмотреть особые меры в отношении микропредприятий, малых и средних предприятий.

(168) Процедура проверки должна использоваться для принятия имплементационных актов относительно стандартных договорных условий между контролерами и обрабатывающими данные лицами, а также между обрабатывающими данные лицами; норм поведения; технических стандартов и механизмов для сертификации; соответствующего уровня защиты, предусмотренного третьей страной, территорией или определенным сектором в указанной третьей стране или международной организацией; стандартных условий защиты; формата и процедур для обмена электронной информацией между контролерами, обрабатывающими данные лицами и надзорными органами в отношении юридически обязывающих корпоративных правил; взаимной помощи; и соглашений об обмене электронной информацией между надзорными органами, а также между надзорными органами и Советом.

(169) Европейская Комиссия должна незамедлительно принять имплементационные акты в случае, если имеется доказательство относительно того, что третья страна, территория или определенный сектор в указанной третьей стране или международная организация не гарантирует соответствующий уровень защиты, и если это необходимо по причинам безотлагательной срочности.

(170) Так как цель настоящего Регламента, а именно обеспечение эквивалентного уровня защиты физических лиц и свободного обращения персональных данных на территории Союза, не может быть в достаточной степени достигнута государствами-членами ЕС, но может быть эффективнее достигнута на

уровне Союза, в силу своего масштаба и воздействия, Союз может принять меры в соответствии с принципом субсидиарности, указанным в Статье 5 Договора о Европейском Союзе (TEU). В соответствии с принципом пропорциональности, указанным в данной Статье, настоящий Регламент не выходит за пределы того, что необходимо для достижения указанной цели.

(171) Директива 95/46/EC заменяется настоящим Регламентом. Обработка, уже осуществляемая на момент применения настоящего Регламента, должна быть приведена в соответствии с настоящим Регламентом в течение двух лет после его вступления в силу. Если обработка основана на согласии в соответствии с Директивой 95/46/EC, субъекту данных необязательно давать свое согласие снова, если способ, которым было получено согласие, соответствует условиям настоящего Регламента, чтобы контролер мог продолжить указанную обработку после даты применения настоящего Регламента. Решения Европейской Комиссии и разрешения надзорных органов, принятые на основе Директивы 95/46/EC, сохраняют свою силу до тех пор, пока они не будут изменены, заменены или отменены.

(172) В соответствии со Статьей 28(2) Регламента (EC) 45/2001 была проведена консультация с Европейским инспектором по защите персональных данных, и 7 марта 2012 г. он дал свое заключение <*>.

<*> ОЖ N C 192, 30.06.2012, стр. 7.

(173) Настоящий Регламент должен применяться в отношении всех вопросов, связанных с защитой основных прав и свобод при обработке персональных данных, которые не подлежат обязанностям, установленным в Директиве 2002/58/EC Европейского Парламента и Совета ЕС <*> и преследующим одну и ту же цель, включая обязанности контролера и права физических лиц. Для того чтобы уточнить соотношение между настоящим Регламентом и Директивой 2002/58/EC, в указанную Директиву необходимо внести соответствующие изменения. Как только настоящий Регламент будет принят, Директива 2002/58/EC должна быть пересмотрена для обеспечения соответствия с настоящим Регламентом,

---

<*> Директива 2002/58/EC Европейского Парламента и Совета ЕС от 12 июля 2002 г. в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи) (ОЖ N L 201, 31.07.2002, стр. 37).

приняли настоящий Регламент:

ГЛАВА I. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1

Предмет и цели

1. Настоящий Регламент устанавливает правила в отношении защиты физических лиц при обработке персональных данных и правила в отношении свободного обращения персональных данных.

2. Настоящий Регламент защищает основные права и свободы физических лиц и, в частности, право на защиту персональных данных.

3. Свободное обращение персональных данных в Союзе не должно быть ни ограничено, ни запрещено по причинам, связанным с защитой физических лиц при обработке персональных данных.

Статья 2

Фактическая сфера применения

1. Настоящий Регламент применяется в отношении обработки персональных данных полностью либо частично при помощи автоматизированных средств, а также в отношении обработки персональных данных

иными способами, которые являются частью файловой системы или которые имеют целью стать частью файловой системы.

2. Настоящий Регламент не применяется в отношении обработки персональных данных:

(a) в процессе деятельности, которая не подпадает под действие законодательства Союза;

(b) государствами-членами ЕС при осуществлении деятельности, которая подпадает под действие Главы 2 Раздела V TEU;

(c) физическим лицом в процессе осуществления исключительно личной или бытовой деятельности;

(d) компетентными органами в целях предупреждения, расследования, выявления уголовных преступлений, или привлечения к ответственности, или приведения в исполнение уголовных наказаний, включая защиту и предотвращение угроз общественной безопасности.

3. В том, что касается обработки персональных данных институтами, органами, учреждениями и агентствами Союза, применяется Регламент (ЕС) 45/2001. Регламент (ЕС) 45/2001 и другие законодательные акты Союза в области обработки персональных данных должны быть изменены в соответствии с принципами и правилами настоящего Регламента согласно Статье 98.

4. Настоящий Регламент действует без ущерба применению Директивы 2000/31/ЕС, в частности, нормы об ответственности поставщиков посреднических услуг в Статьях 12 - 15 указанной Директивы.

Статья 3

Территориальное действие

1. Настоящий Регламент применяется в отношении обработки персональных данных в контексте деятельности учреждения контролера или обрабатывающего данные лица в Союзе, вне зависимости от того, проводится обработка в Союзе или нет.

2. Настоящий Регламент применяется в отношении обработки персональных данных субъектов данных, находящихся в Союзе, контролером или обрабатывающим данные лицом, не учрежденными в Союзе, если обработка данных касается:

(a) предоставления товаров и услуг субъектам данных в Союзе вне зависимости от того, требуется ли оплата от указанного субъекта данных, или

(b) мониторинга их деятельности при условии, что деятельность осуществляется на территории Союза.

3. Настоящий Регламент применяется в отношении обработки персональных данных контролером, не учрежденным в Союзе, но учрежденным в месте, где законодательство государства-члена ЕС применяется в соответствии с международным публичным правом.

Статья 4

Определения

Для целей настоящего Регламента:

(1) под термином "персональные данные" понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу ("субъект данных"); идентифицируемое лицо - это лицо, которое может быть идентифицировано, прямо или косвенно, в частности, посредством таких идентификаторов как имя, идентификационный номер, сведения о местоположении, идентификатор в режиме онлайн или через один или несколько признаков, характерных для физической, психологической, генетической, умственной, экономической, культурной или социальной идентичности указанного

физического лица;

(2) под термином "обработка" понимается любая операция или набор операций, осуществляемых с персональными данными, с применением автоматизированных средств или без таковых, например сбор, запись, организация, структурирование, хранение, модификация и изменение, извлечение, консультирование, использование, раскрытие посредством передачи, распространение или предоставление иным способом, упорядочение или комбинирование, ограничение, стирание или разрушение;

(3) под термином "ограничение обработки" понимается маркировка сохраненных персональных данных в целях ограничения их обработки в будущем;

(4) под термином "формирование профиля" понимается любая форма автоматизированной обработки персональных данных, состоящая из использования персональных данных в целях оценки определенных индивидуальных аспектов, касающихся физического лица, в частности, для анализа или определения аспектов, относящихся к производственным показателям указанного лица, экономической ситуации, здоровью, индивидуальным предпочтениям, интересам, надежности, поведению, месторасположению или передвижению;

(5) под термином "псевдонимизация" понимается обработка персональных данных таким образом, что персональные данные не могут быть больше отнесены к определенному субъекту данных без использования дополнительной информации, при условии, что дополнительная информация хранится отдельно и подлежит техническим и организационным мерам, гарантирующим, что персональные данные не отнесены к идентифицированному или идентифицируемому физическому лицу;

(6) под термином "файловая система" понимается любой структурированный набор персональных данных, доступных в соответствии с определенными критериями, вне зависимости от того используется ли при этом централизованный, децентрализованный, функциональный или географический принцип;

(7) под термином "контролер" понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и способы обработки персональных данных; если цели и способы указанной обработки определены законодательством Союза или законодательством государства-члена ЕС, контролер или определенные критерии для его назначения могут быть предусмотрены законодательством Союза или государства-члена ЕС;

(8) под термином "обрабатывающее данные лицо" понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, который обрабатывает персональные данные от имени контролера;

(9) под термином "получатель" понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, которому раскрываются персональные данные, вне зависимости от того, является ли он третьим лицом или нет. Однако органы государственной власти, которые могут получать персональные данные в рамках частного запроса в соответствии с законодательством Союза или государства-члена ЕС, не должны рассматриваться в качестве получателей; обработка данных указанными органами государственной власти должна соответствовать применимым нормам о защите данных согласно целям обработки;

(10) под термином "третья сторона" понимается физическое или юридическое лицо, органы государственной власти, агентство или орган, отличный от субъекта данных, контролера, обрабатывающего данные лица или лиц, которые уполномочены проводить обработку персональных данных под непосредственным руководством контролера или обрабатывающего данные лица;

(11) под термином "согласие субъекта данных" понимается любое свободно данное, конкретное, содержательное и определенное указание о своей воле, посредством которого субъект персональных данных оповещает о своем согласии на обработку относящихся к нему персональных данных;

(12) под термином "утечка персональных данных" понимается нарушение безопасности, ведущее к

случайному или незаконному разрушению, потере, изменению, несанкционированному раскрытию или доступу к переданным, сохраненным или иным образом обработанным персональным данным;

(13) под термином "генетические данные" понимаются персональные данные, касающиеся унаследованных или приобретенных генетических характеристик физического лица, которые предоставляют уникальную информацию о физиологии или здоровье указанного физического лица и которые являются результатом, в частности, анализа биологического образца соответствующего физического лица;

(14) под термином "биометрические данные" понимаются персональные данные, возникающие в результате особой технической обработки, касающиеся физических, физиологических или поведенческих характеристик физического лица, которые предусматривают или подтверждают уникальную идентификацию указанного физического лица, например, изображение лица человека или дактилоскопические данные;

(15) под термином "данные в отношении здоровья" понимаются персональные данные, касающиеся физического или психического здоровья физического лица, в том числе предоставление медицинских услуг, которые раскрывают информацию о состоянии его/ее здоровья;

(16) под термином "основное учреждение" понимается:

(a) в отношении контролера с учреждениями в нескольких государствах-членах ЕС, месторасположение его центральной администрации в Союзе, кроме случаев, когда решения о целях и способах обработки персональных данных принимаются в другом учреждении контролера в Союзе, и последнее учреждение обладает правом на имплементацию указанных решений, в этом случае учреждение, принимающее такие решения, должно рассматриваться в качестве основного учреждения;

(b) в отношении лица, обрабатывающего данные, с учреждениями в нескольких государствах-членах ЕС, месторасположение его центральной администрации в Союзе, или, если лицо, обрабатывающее данные, не имеет центральной администрации в Союзе, учреждение указанного лица в Союзе, где производится основная обработка в контексте деятельности учреждения лица, обрабатывающего данные, в той степени, в какой указанное лицо ограничено специальными обязательствами в соответствии с настоящим Регламентом;

(17) под термином "представитель" понимается физическое или юридическое лицо, учрежденное в Союзе, которое в письменной форме назначается контролером или лицом, обрабатывающим данные, в соответствии со Статьей 27 и представляет контролера или лицо, обрабатывающее данные, с учетом их соответствующих обязательств согласно настоящему Регламенту;

(18) под термином "компания" понимается физическое или юридическое лицо, участвующее в экономической деятельности, вне зависимости от организационно-правовой формы, в том числе товарищества или объединения, регулярно участвующие в экономической деятельности;

(19) под термином "группа предприятий" понимается контролирующее предприятие и подконтрольные ему предприятия;

(20) под термином "юридически обязывающие корпоративные правила" понимаются меры по обеспечению защиты персональных данных, которые обязаны соблюдать контролер или обрабатывающее данные лицо, учрежденные на территории государства-члена ЕС, относительно передачи или совокупности передач персональных данных контролеру или обрабатывающему данные лицу в одной или нескольких третьих странах в рамках группы предприятий или группы компаний, участвующих в совместной экономической деятельности;

(21) под термином "надзорный орган" понимается независимый орган государственной власти, который учрежден государством-членом ЕС согласно Статье 51;

(22) под термином "соответствующий надзорный орган" понимается надзорный орган, который занимается обработкой персональных данных, так как:

(a) контролер или обрабатывающее данные лицо учреждено на территории государства-члена ЕС указанного надзорного органа;

(b) обработка данных в значительной степени оказывает воздействие или может оказывать воздействие на субъекты данных, находящихся в государстве-члене ЕС указанного надзорного органа; или

(c) в указанный надзорный орган подана жалоба;

(23) под термином "трансграничная обработка" понимается:

(a) обработка персональных данных, которая осуществляется в контексте деятельности учреждений в нескольких государствах-членах ЕС контролера или осуществляющего обработку лица в Союзе, если контролер или лицо, осуществляющее обработку, учреждены в нескольких государствах-членах ЕС;

(b) обработка персональных данных, которая осуществляется в контексте деятельности единичного учреждения контролера или лица, осуществляющего обработку, в союзе, но которая существенно влияет или может существенно влиять на субъекты данных в нескольких государствах-членах ЕС.

(24) под термином "существенное и мотивированное возражение" понимается возражение против проекта решения относительно того, имеется ли нарушение настоящего Регламента или соответствует ли намеченная деятельность контролера или обрабатывающего данные лица настоящему Регламенту, что четко демонстрирует важность рисков, возникших в результате проекта решения в отношении основных прав и свобод субъектов данных и при необходимости свободного потока персональных данных на территории Союза;

(25) под термином "услуга информационного общества" понимается услуга, в значении определения, указанного в пункте (b) Статьи 1(1) Директивы (ЕС) 2015/1535 Европейского Парламента и Совета ЕС <*>;

<*> Директива (ЕС) 2015/1535 Европейского Парламента и Совета ЕС от 9 сентября 2015 г. о процедуре предоставления информации в области технических регламентов, а также правил оказания услуг в информационном обществе (ОЖ N L 241, 17.09.2015, стр. 1).

(26) под термином "международная организация" понимается организация и ее подведомственные органы, регулируемые международным публичным правом, или любой другой орган, установленный соглашением между двумя или более странами или установленный на основе такого соглашения.

ГЛАВА II. ПРИНЦИПЫ

Статья 5

Принципы, связанные с обработкой персональных данных

1. Персональные данные должны:

(a) обрабатываться законно, беспристрастно и прозрачным образом в отношении субъекта данных ("законность, беспристрастность и прозрачность");

(b) собираться для определенных, явных и законных целей и в дальнейшем не должны обрабатываться несовместим с этими целями способом; дальнейшая обработка для достижения целей общественного интереса, а также целей научного или исторического исследования или статистических целей не должна в соответствии со Статьей 89(1) рассматриваться в качестве несовместимой с первоначальными целями ("целевое ограничение")"

(c) быть адекватными, соответствующими и должны ограничиваться тем, что необходимо относительно целей, для которых они обрабатываются ("минимизация данных");

(d) быть точными и, при необходимости, актуальными; необходимо принимать обоснованные меры для того, чтобы гарантировать своевременное удаление или исправление неточных данных с учетом целей, для которых они обрабатываются ("точность");

(e) храниться в форме, которая позволяет идентифицировать субъектов данных, в течение срока, необходимого для целей, относительно которых обрабатываются персональные данные; персональные данные могут храниться в течение более длительного срока, если они будут обрабатываться исключительно в целях общественного интереса, а также в целях научного или исторического исследования или в статистических целях в соответствии со Статьей 89(1), с учетом имплементации соответствующих технических и организационных мер, требуемых настоящим Регламентом для защиты прав и свобод субъекта данных ("ограничение по хранению");

(f) обрабатываться способом, гарантирующим соответствующую безопасность персональных данных, включая защиту от несанкционированной или незаконной обработки и от случайной потери, разрушения или уничтожения данных, с использованием соответствующих технических и организационных мер ("целостность и конфиденциальность");

2. Контролер несет ответственность за соблюдение требований параграфа 1, он должен быть в состоянии продемонстрировать это ("ответственность").

Статья 6

Законность обработки

1. Обработка должна быть законной, только если и поскольку применяется одно из следующих условий:

(a) субъект данных дал согласие на обработку своих персональных данных для одной или нескольких конкретных целей;

(b) обработка необходима для исполнения договора, в котором субъект данных является одной из сторон, или для принятия мер по требованию субъекта данных до заключения договора;

(c) обработка необходима для соблюдения юридической обязанности, объектом которой является контролер;

(d) обработка необходима для защиты жизненных интересов субъекта данных или другого физического лица;

(e) защита необходима для выполнения задачи, осуществляемой в интересах государства или при осуществлении государственной власти, закрепленной за контролером;

(f) обработка необходима для целей обеспечения законных интересов контролера или третьей стороны, за исключением случаев, когда такие интересы перекрываются интересами или основными правами и свободами субъекта данных, которые требуют защиты персональных данных, в частности, если субъектом данных является ребенок.

Пункт (f) первого подпараграфа не применяется в отношении обработки, осуществляемой органами государственной власти при выполнении ими своих задач.

2. Государства-члены ЕС могут сохранить или предусмотреть более конкретные положения для применения норм настоящего Регламента в отношении обработки для выполнения пунктов (c) и (e) параграфа 1 посредством определения более точных специальных требований для обработки и других мер для того, чтобы гарантировать законную и справедливую обработку, в том числе для иных особых ситуаций обработки, предусмотренных в Главе IX.

3. Основание для обработки, указанной в пункте (c) и (e) параграфа 1, должно устанавливаться:

(a) законодательством Союза; или

(b) законодательством государства-члена ЕС, под действие которого подпадает контролер.

Цель обработки должна определяться в рамках указанного юридического основания или, в том, что касается обработки, указанной в пункте (e) параграфа 1, должна быть необходимой для выполнения задачи, осуществляемой в интересах государства или при осуществлении государственной власти, закрепленной за контролером. Указанное юридическое основание может содержать конкретные положения для применения норм настоящего Регламента, inter alia: общие условия, регулирующие законность обработки контролером; типы данных, подлежащих обработке; соответствующие субъекты данных; субъекты, которым могут быть раскрыты данные, и цели, для которых персональные данных раскрываются; целевое ограничение; сроки хранения; и процедуры и процесс обработки данных, в том числе меры, гарантирующие законную и справедливую обработку, как например, для иных особых ситуаций обработки, предусмотренных в Главе IX. Законодательство Союза или государства-члена ЕС должно соответствовать цели государственных интересов и быть пропорциональным в отношении законной цели.

4. Если обработка для цели, отличной от цели, для которой были получены персональные данные, не основывается на согласии субъекта данных или на законодательстве Союза или государства-члена ЕС, которое представляет собой необходимую и пропорциональную меру в демократическом обществе для защиты целей, указанных в Статье 23(1), контролер в целях проверки того, соответствует ли обработка, проводимая для иных целей, цели, для которой первоначально собирались персональные данные, должен принять во внимание, inter alia:

(a) любую связь между целями, для которых были получены персональные данные, и целями предполагаемой последующей обработки;

(b) обстановку, в которой собирались персональные данные, в частности, отношения между субъектами данных и контролером;

(c) характер персональных данных, в частности, производится ли обработка особых категорий данных, согласно Статье 9, или производится ли обработка персональных данных, связанных с судимостями и преступлениями, согласно Статье 10;

(d) возможные последствия предполагаемой последующей обработки для субъектов данных;

(e) существование средств по обеспечению безопасности, которые могут включать в себя криптографическое закрытие или псевдонимизацию.

Статья 7

Условия для согласия

1. Если обработка основывается на согласии, контролер должен иметь возможность доказать, что субъект данных согласился на обработку своих персональных данных.

2. Если согласие субъекта данных дается в виде письменного заявления, которое также касается других обстоятельств, запрос о предоставлении согласия должен быть представлен в понятной и легкодоступной форме на ясном и доступном языке в том виде, который четко отличал бы его от других обстоятельств. Любая часть такого заявления, которая представляет собой нарушение настоящего Регламента, не является обязательной для исполнения.

3. Субъект данных должен иметь право в любое время отозвать свое согласие. Отзыв согласия не должен влиять на законность обработки, основанной на согласии до его отзыва. Прежде чем давать согласие, субъект данных должен быть проинформирован об этом. Процедура отзыва согласия должна быть такой же простой, как и процедура предоставления согласия.

4. При проведении оценки относительно того, было ли согласие дано по доброй воле, основное внимание необходимо уделить тому, inter alia, зависит ли выполнение договора, включая предоставление

услуги, от согласия на обработку персональных данных, которые не являются необходимыми для выполнения указанного договора.

Статья 8

Условия, применимые к согласию ребенка,
в отношении услуг информационного общества

1. Если применяется пункт (a) Статьи 6(1) при предоставлении услуг информационного общества непосредственно ребенку, обработка персональных данных ребенка является законной только в случае, если ребенку исполнилось как минимум 16 лет. Если ребенок еще не достиг возраста 16 лет, такая обработка является законной, только если и поскольку согласие было дано лицом, обладающим родительской ответственностью в отношении ребенка, или было дано с его одобрения.

Государства-члены ЕС могут законодательно предусмотреть меньший возраст для указанных целей при условии, что такой возраст не ниже 13 лет.

2. Контролер с учетом имеющихся технологических возможностей должен принять разумные меры для того, чтобы в указанных случаях подтвердить, что согласие было дано лицом, обладающим родительской ответственностью в отношении ребенка, или было дано с его одобрения.

3. Параграф 1 не должен влиять на общее договорное право государств-членов ЕС, например, на нормы о действительности, вступлении в силу или правовых последствиях договора в отношении ребенка.

Статья 9

Обработка особых категорий персональных данных

1. Обработка персональных данных, раскрывающих расовое или этническое происхождение, политические взгляды, религиозные убеждения или философские воззрения, членство в профессиональном союзе, а также обработка генетических данных, биометрических данных для однозначной идентификации физического лица, данных касающихся здоровья, половой жизни или сексуальной ориентации физического лица, должна быть запрещена.

2. Параграф 1 не применяется в случае, если:

(a) субъект данных дал прямое согласие на обработку указанных персональных данных для одной или нескольких установленных целей, кроме случаев, когда законодательство Союза или государства-члена ЕС предусматривает, что запрет, указанный в параграфе 1, не может быть отменен субъектом данных;

(b) обработка необходима в целях исполнения обязательств и особых прав контролера или субъекта данных в сфере трудового законодательства, права социального обеспечения и социальной защиты постольку, поскольку это допускается законодательством Союза или государства-члена ЕС или коллективным договором согласно законодательству государства-члена ЕС, предусматривающему соответствующие средства защиты основных прав и интересов субъекта данных;

(c) обработка необходима для защиты жизненных интересов субъекта данных или другого физического лица, если субъект данных физически или юридически неспособен дать свое согласие;

(d) обработка осуществляется фондом, объединением или некоммерческой организацией в рамках их законной деятельности с соответствующими гарантиями в политических, философских, религиозных или профсоюзных целях и при условии, что обработка относится исключительно к членам, бывшим членам организации или лицам, которые осуществляют постоянный контакт с нею в связи с ее целями, и что персональные данные не раскрываются третьим лицам без согласия на это субъекта персональных данных;

(e) обработка относится к персональным данным, которые субъект данных явно сделал

общедоступными;

(f) обработка необходима для предъявления, исполнения или защиты судебных исков или в случаях, когда суды действуют в пределах своей судейской дееспособности;

(g) обработка необходима по причинам особого общественного интереса на основании законодательства Союза или государства-члена ЕС, которое должно быть пропорционально преследуемой цели, должно соответствовать сущности права на защиту данных и предусматривать приемлемые и конкретные меры для защиты основных прав и интересов субъекта данных;

(h) обработка необходима в целях превентивной или профессиональной медицины, для оценки трудоспособности работника, для диагностики медицинского состояния, предоставления медицинской или социальной помощи или лечения или для управления системами и услугами здравоохранения и социального обеспечения на основании законодательства Союза или государства-члена ЕС или на основании договора с работником здравоохранения и в соответствии с условиями и гарантиями, указанными в параграфе 3.

(i) обработка необходима по причинам общественного интереса в области общественного здравоохранения, например, защиты от серьезных трансграничных угроз здоровью или для обеспечения высоких стандартов качества и надежности медицинского обслуживания и лекарственных средств или медицинской техники, на основании законодательства Союза или государства-члена ЕС, которое предусматривает приемлемые и конкретные меры для защиты прав и свобод субъекта данных, в частности, профессиональной тайны;

(j) обработка необходима для целей архивизации информации в интересах государства, для научных, исторических или статистических целей в соответствии со Статьей 89(1), основанных на законодательстве Союза или государства-члена ЕС, которое должно быть пропорционально преследуемой цели, должно соответствовать сущности права на защиту данных и предусматривать приемлемые и конкретные меры для защиты основных прав и интересов субъекта данных;

3. Персональные данные, указанные в параграфе 1, могут обрабатываться для целей, указанных в пункте (h) параграфа 2, если указанные данные обрабатываются специалистом или под его ответственность и указанный специалист обязан соблюдать профессиональную тайну согласно законодательству Союза или государства-члена ЕС или согласно нормам, установленным национальными компетентными органами, или если обработка осуществляется иным лицом, которое обязано соблюдать конфиденциальность согласно законодательству Союза или государства-члена ЕС или согласно правилам, установленным национальными компетентными органами.

4. Государства-члены ЕС могут сохранять или вводить дополнительные условия, в том числе ограничения, в отношении обработки генетических данных, биометрических данных или данных о здоровье.

Статья 10

Обработка персональных данных, касающихся уголовных приговоров и преступлений

Обработка персональных данных, касающихся уголовных приговоров и преступлений или соответствующих мер по обеспечению безопасности на основании Статьи 6(1), должна осуществляться только под контролем официального органа или, если обработка разрешена законодательством Союза или государства-члена ЕС, которое предусматривает соответствующие гарантии правам и свободам субъектов данных. Полный реестр уголовных приговоров должен вестись только под контролем официального органа.

Статья 11

Обработка, не требующая идентификации соответствующего лица

1. Если цели, для которых контролер обрабатывает персональные данные, не требуют

идентификации субъекта данных контролером, контролер не обязан сохранять, получать или обрабатывать дополнительную информацию для установления личности субъекта данных только лишь в целях соблюдения настоящего Регламента.

2. Если в случаях, указанных в параграфе 1 настоящей Статьи, контролер может подтвердить, что он не в состоянии установить личность субъекта данных, он должен проинформировать об этом субъекта данных, при наличии соответствующей возможности. В указанных случаях Статьи 15 - 20 не применяются, кроме случаев, когда субъект данных для осуществления своих прав согласно указанным Статьям, предоставляет дополнительную информацию, которая обеспечивает его/ее идентификацию.

ГЛАВА III. ПРАВА СУБЪЕКТА ДАННЫХ

Раздел 1

ПРОЗРАЧНОСТЬ И УСЛОВИЯ

Статья 12

Прозрачная информация, связь и условия для осуществления прав субъектов данных

1. Контролер должен принять соответствующие меры для предоставления субъекту данных любой информации, указанной в Статьях 13 и 14, и любых сведений согласно Статьям 15 - 22 и Статьей 34, которые касаются обработки, в сжатой, прозрачной, понятной и легкодоступной форме на понятном и простом языке, в частности в отношении любой информации, адресованной ребенку. Информация должна предоставляться в письменной форме или при помощи иных средств, в том числе, при необходимости, при помощи электронных средств связи. По просьбе субъекта данных информация может быть предоставлена в устной форме, при условии, что личность субъекта данных установлена иным способом.

2. Контролер должен содействовать осуществлению прав субъекта данных согласно Статьям 15 - 22. В случаях, указанных в Статье 11(2), контролер может отказаться действовать по запросу субъекта данных в целях осуществления его/ее прав согласно Статьям 15 - 22 только тогда, когда он подтверждает, что он не в состоянии установить личность субъекта данных.

3. Контролер должен незамедлительно предоставить субъекту данных информацию о мерах, принятых в рамках запроса согласно Статьям 15 - 22, и в любом случае в течение одного месяца после получения запроса. Указанный срок может быть продлен еще на два месяца, при необходимости, с учетом сложности и количества запросов. Контролер должен проинформировать субъекта данных о любом таком продлении в течение одного месяца после получения запроса, с указанием причин превышения срока. Если субъект данных подает запрос посредством электронной формы, информация должна быть предоставлена по возможности электронным способом, если субъект данных не запрашивает иной способ передачи информации.

4. Если контролер не принимает меры по запросу субъекта данных, он должен незамедлительно или не позднее одного месяца после получения запроса проинформировать субъекта данных о причинах непринятия мер, а также о возможности подачи жалобы надзорному органу и о возможности судебной защиты прав.

5. Информация согласно Статьям 13 и 14, а также любые сведения и принятые меры согласно Статьям 15 - 22 и Статье 34 должны предоставляться бесплатно. Если запросы субъекта данных являются явно необоснованными или носят чрезмерный характер в частности вследствие многочисленных повторов, контролер может:

(a) взимать приемлемую плату с учетом административных расходов на предоставление информации или сведений или принятие запрашиваемых мер; или

(b) отказаться действовать в соответствии с запросом.

Контролер должен нести бремя доказывания явной необоснованности запроса или его чрезмерного характера.

6. Без ущерба действию Статьи 11, если контролер имеет достаточные основания для сомнения относительно идентификации личности физического лица, подающего запрос согласно Статьям 15 - 21, он может затребовать предоставление дополнительной информации, необходимой для подтверждения личности субъекта данных.

7. Информация, которая должна быть предоставлена субъектам данных согласно Статьям 13 и 14, может предоставляться в сочетании со стандартизированными графическими обозначениями для того, чтобы в отчетливо видимой, понятной и разборчивой форме дать общее представление о предполагаемой обработке. Если графические изображения представлены в электронной форме, они должны быть пригодными для машинного считывания.

8. Европейская Комиссия должна иметь возможность принимать делегированные акты в соответствии со Статьей 92 в целях определения информации, которая должны быть представлена посредством графических обозначений, и определения процедур для предоставления стандартизированных графических обозначений.

Раздел 2

ИНФОРМАЦИЯ И ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

Статья 13

Информация, которая должна предоставляться в случае получения персональных данных от субъекта данных

1. Если относящиеся к субъекту данных персональные данные предоставляются субъектом данных, контролер в момент получения персональных данных должен предоставить субъекту данных следующую информацию:

(a) идентификационную информацию и контактные данные контролера и, при необходимости, его представителя;

(b) контактные данные инспектора по защите персональных данных, в соответствующих случаях;

(c) цели обработки, для которых предназначаются персональные данные, а также юридическое основание для обработки;

(d) в случае если обработка основывается на пункте (f) Статьи 6(1), законные интересы, преследуемые контролером или третьей стороной;

(e) получатели или категории получателей персональных данных, при наличии;

(f) в соответствующих случаях, намерение контролера передать персональные данные третьей стране или международной организации, а также наличие или отсутствие решения Европейской Комиссии о соразмерности, или в случае передачи согласно Статье 46 или 47 или согласно второму подпараграфу Статьи 49(1) - ссылка на соответствующие и надлежащие гарантии и способы, посредством которых может быть получена их копия, или где они могут быть предоставлены.

2. В дополнение к информации, указанной в параграфе 1, контролер в момент получения персональных данных должен предоставить субъекту данных дополнительно следующую информацию, необходимую для обеспечения справедливой и прозрачной обработки:

(a) срок, в течение которого будут храниться персональные данные, или если это не представляется возможным, критерии для определения указанного срока;

(b) существование права требования от контролера доступа к соответствующим персональным данным и их исправления или удаления или ограничения обработки или возражение против обработки, а также права на переносимость данных;

(c) в случае если обработка основывается на пункте (a) Статьи 6(1) или на пункте (a) Статьи 9(2), существование права на отзыв своего согласия, без воздействия на законность обработки, основанной на согласии до его отзыва;

(d) право подачи жалобы в надзорный орган;

(e) является ли предоставление персональных данных требованием, предусмотренным законодательством или договором, или требованием, которое необходимо для заключения договора, а также обязан ли субъект данных предоставлять персональные данные и возможные последствия непредставления указанных данных;

(f) наличие автоматизированного процесса принятия решения, в том числе формирование профиля согласно Статье 22(1) и (4) и, как минимум в указанных случаях, достоверная информация о соответствующей логической схеме, а также о значимости и предполагаемых последствиях обработки для субъекта данных.

3. Если контролер собирается в дальнейшем обрабатывать персональные данные в целях, отличных от целей, для которых персональные данные были получения, до начала указанной обработки он должен предоставить субъекту данных информацию относительно иной цели, а также любую дополнительную информацию, указанную в параграфе 2.

4. Параграфы 1, 2 и 3 не должны применяться, поскольку и если субъект данных уже располагает соответствующей информацией.

Статья 14

Информация, которая должна предоставляться при получении персональных данных не от субъекта данных

1. В случае если персональные данные получены не от субъекта данных, контролер должен предоставить субъекту данных следующую информацию:

(a) идентификационную информацию и контактные данные контролера и, при необходимости, его представителя;

(b) контактные данные инспектора по защите персональных данных, в соответствующих случаях;

(c) цели обработки, для которых предназначаются персональные данные, а также юридическое основание для обработки;

(d) категории соответствующих персональных данных;

(e) получатели или категории получателей персональных данных, при наличии;

(f) в соответствующих случаях, намерение контролера передать персональные данные получателю в третьей стране или международной организации, а также наличие или отсутствие решения Европейской Комиссии о соразмерности, или в случае передачи согласно Статье 46 или 47 или согласно второму подпараграфу Статьи 49(1) - ссылка на соответствующие и надлежащие гарантии и способы получения их копии или того, где они могут быть предоставлены.

2. В дополнение к информации, указанной в параграфе 1, контролер должен предоставить субъекту данных следующую информацию, необходимую для обеспечения справедливой и прозрачной обработки в отношении субъекта данных:

(a) срок, в течение которого будут храниться персональные данные, или если это не представляется возможным, критерии для определения указанного срока;

(b) в случае если обработка основывается на пункте (f) Статьи 6(1), законные интересы, преследуемые контролером или третьей стороной;

(c) существование права требования от контролера доступа к соответствующим персональным данным и их исправления или удаления или ограничения обработки или возражение против обработки, а также права на переносимость данных;

(d) в случае если обработка основывается на пункте (a) Статьи 6(1) или на пункте (a) Статьи 9(2), существование права на отзыв своего согласия, без воздействия на законность обработки, основанной на согласии до его отзыва;

(e) право подачи жалобы в надзорный орган;

(f) из каких источников происходят персональные данные и, при необходимости, взяты ли они из общедоступных источников;

(g) наличие автоматизированного процесса принятия решения, в том числе формирование профиля согласно Статье 22(1) и (4) и, как минимум в указанных случаях, достоверная информация о соответствующей логической схеме, а также о значимости и предполагаемых последствиях указанной обработки для субъекта данных.

3. Контролер должен предоставить информацию, указанную в параграфах 1 и 2:

(a) в приемлемый срок после получения персональных данных, но как минимум в течение одного месяца, с учетом особых условий обработки персональных данных;

(b) если персональные данные должны использоваться для общения с субъектом данных, как минимум во время первого обращения к указанному субъекту данных; или

(c) если предусмотрено раскрытие информации другому получателю, как минимум в момент первоначального раскрытия персональных данных.

4. Если контролер намерен в дальнейшем обрабатывать персональные данные в целях, отличных от целей, для которых они были получены, перед последующей обработкой он должен предоставить субъекту данных информацию об указанных иных целях, а также любую существенную дополнительную информацию, указанную в параграфе 2.

5. Параграфы 1 - 4 не должны применять в том случае, если:

(a) субъект данных уже располагает информацией;

(b) предоставление указанной информации оказывается невозможным или требует непропорционального усилия, в частности, для обработки в целях архивирования в интересах общества, в целях научных или исторических исследований или в статистических целях, с учетом условий и гарантий, указанных в Статье 89(1), или постольку, поскольку обязанность, указанная в параграфе 1 настоящей Статьи, может сделать невозможным или негативно отразиться на достижении целей указанной обработки. В указанных случаях контролер должен принять соответствующие меры для защиты прав, свобод и законных интересов субъекта данных, включая доведение информации до всеобщего сведения;

(c) получение или раскрытие информации прямо установлено законодательством Союза или государства-члена ЕС, под действие которого подпадает контролер и которое обеспечивает соответствующие меры для защиты законных интересов субъекта данных; или

(d) если персональные данные не должны разглашаться в соответствии с обязательством о соблюдении профессиональной тайны согласно законодательству Союза или государства-члена ЕС, включая установленные законодательством обязательства о сохранении профессиональной тайны.

Статья 15

Право субъекта данных на доступ к данным

1. Субъект данных имеет право запрашивать у контролера подтверждение относительно того, обрабатываются ли относящиеся к нему персональные данные, и если дело обстоит именно так, он имеет право на доступ к персональным данным и следующей информации:

(a) цели обработки;

(b) категории обрабатываемых персональных данных;

(c) получатели или категории получателей, которым были или будут раскрыты персональные данные, в частности, получатели в третьих странах или международные организации;

(d) по мере возможности, предусмотренный срок, в течение которого будут храниться персональные данные, или, при отсутствии соответствующей возможности, критерии, используемые для определения указанного периода;

(e) существование права требования от контролера исправления или удаления соответствующих персональных данных, или ограничения их обработки, или возражения против указанной обработки;

(f) право подачи жалобы в надзорный орган;

(g) в случае если персональные данные получены не от субъекта данных, любая доступная информация об их источнике;

(h) наличие автоматизированного процесса принятия решения, в том числе формирование профиля согласно Статье 22(1) и (4) и, как минимум в указанных случаях, достоверная информация о соответствующей логической схеме, а также о значимости и предполагаемых последствиях указанной обработки для субъекта данных.

2. В случае если персональные данные передаются третьей стране или международной организации, субъект данных вправе получить информацию о соответствующих гарантиях согласно Статье 46 относительно передачи данных.

3. Контролер должен обеспечить наличие копии обрабатываемых персональных данных. За любые иные копии, запрашиваемые субъектом данных, контролер может взимать приемлемую плату на основании административных расходов. Если субъект данных подает запрос электронным способом, информация должна предоставляться в принятой электронной форме, если субъект данных не запрашивает иное.

4. Право на получение копии, указанной в параграфе 3, не должно отрицательно влиять на права и свободы других лиц.

Раздел 3

ВНЕСЕНИЕ ИСПРАВЛЕНИЙ И УДАЛЕНИЕ ИНФОРМАЦИИ

Статья 16

Право на внесение исправлений

Субъект данных вправе потребовать от контролера незамедлительного изменения относящихся к нему неточных персональных данных. Принимая во внимание цели обработки, субъект данных имеет право на внесение дополнений в персональные данные, в том числе посредством предоставления дополнительного заявления.

Статья 17

Право на удаление ("право на забвение")

1. Субъект данных имеет право требовать от контролера незамедлительного удаления относящихся к нему персональных данных, контролер должен незамедлительно удалить персональные данные, если применяется одно из следующих оснований:

(a) персональные данные больше не требуются для целей, для которых они были получены или обрабатывались в иных случаях;

(b) субъект данных отзывает свое согласие, на основании которого согласно пункту (a) Статьи 6(1) или пункту (a) Статьи 9(2) проводилась обработка, и если отсутствует иное юридическое основание для обработки;

(c) субъект данных возражает против обработки согласно Статье 21(1), и отсутствуют имеющую преимущественную юридическую силу законные основания для обработки, или субъект данных возражает против обработки согласно Статье 21(2);

(d) персональные данные обрабатывались незаконно;

(e) персональные данные должны быть уничтожены в целях соблюдения юридической обязанности согласно законодательству Союза или государства-члена ЕС, под действие которого подпадает контролер;

(f) персональные данные собирались в отношении предоставления услуг информационного общества согласно Статье 8(1).

2. Если контролер обнародовал персональные данные и он согласно параграфу 1 обязан удалить персональные данные, он с учетом имеющихся технологических возможностей и расходов на имплементацию должен принять необходимые меры, в том числе технические меры, чтобы проинформировать контролеров, которые обрабатывают персональные данные, о том, что субъект данных затребовал от них удаление любых ссылок, копий или точных повторений указанных персональных данных.

3. Параграфы 1 и 2 не должны применяться в тех случаях, когда обработка необходима:

(a) для осуществления права на свободу выражения мнения и распространения информации;

(b) в целях соблюдения юридической обязанности, которая требует проведение обработки согласно законодательству Союза или государства-члена ЕС, под действие которого подпадает контролер, или для выполнения задачи, осуществляемой в интересах общества, или при осуществлении официальных полномочий, возложенных на контролера;

(c) по причинам государственного интереса в области общественного здравоохранения в соответствии с пунктами (h) и (i) Статьи 9(2), а также Статьи 9(3);

(d) в целях архивирования в интересах общества, в целях научных или исторических исследований или в статистических целях, указанных в Статье 89(1), постольку, поскольку право, указанное в параграфе 1, может сделать невозможным или негативно отразиться на достижении целей указанной обработки; или

(e) для обоснования, исполнения или ведения защиты по судебным искам.

Статья 18

Право на ограничение обработки

1. Субъект данных вправе потребовать от контролера ограничить обработку, если применяется одно из следующих условий:

(a) точность персональных данных оспаривается субъектом данных, в течение срока, необходимого контролеру для подтверждения точности персональных данных;

(b) обработка является незаконной, и субъект данных возражает против удаления персональных данных, вместо этого он требует ограничить их использование;

(c) контролеру больше не требуются персональные данные для целей обработки, но они требуются субъекту данных для обоснования, исполнения или ведения защиты по судебным искам;

(d) субъект данных возражал против обработки согласно Статье 21(1) до установления факта относительно того, превалируют ли законные основания контролера над законными основаниями субъекта данных.

2. Если обработка была ограничена согласно параграфу 1, указанные персональные данные, за исключением хранения, должны обрабатываться только с согласия субъекта данных, или для обоснования, исполнения или ведения защиты по судебным искам, или для защиты прав другого физического или юридического лица, или по причинам важного общественного интереса Союза или государства-члена ЕС.

3. Субъект данных, который добился ограничения обработки согласно параграфу 1, должен быть проинформирован контролером прежде, чем ограничение будет снято.

Статья 19

Обязанность уведомления относительно
изменения или уничтожения персональных данных
или ограничения обработки

Контролер должен сообщить о любом изменении или уничтожении персональных данных или ограничении обработки, осуществляемой в соответствии со Статьей 16, Статьей 17(1) и Статьей 18, каждому получателю, которому были раскрыты персональные данные, кроме случаев, когда это оказывается невозможным или требует несоразмерного усилия. Контролер должен проинформировать субъекта данных об указанных получателях, если субъект данных этого требует.

Статья 20

Право на переносимость данных

1. Субъект данных имеет право получить относящиеся к нему персональные данные, которые он предоставил контролеру, в структурированном, универсальном и машиночитаемом формате; он имеет право передать указанные данные другому контролеру беспрепятственно со стороны контролера, которому были предоставлены персональные данные, если:

(a) обработка основывается на согласии в соответствии с пунктом (a) Статьи 6(1), или пунктом (a) Статьи 9(2), или пунктом (b) Статьи 6(1); и

(b) обработка осуществляется при помощи автоматизированных средств.

2. При осуществлении своего права на переносимость данных согласно параграфу 1 субъект данных должен иметь право на передачу персональных данных непосредственно от одного контролера другому, если это технически осуществимо.

3. Осуществление права, указанного в параграфе 1 настоящей Статьи, должно действовать без ущерба Статье 17. Указанное право не должно применяться для обработки, необходимой для выполнения задачи, осуществляемой в рамках общественного интереса или при исполнении официальных полномочий, возложенных на контролера.

4. Право, указанное в параграфе 1, не должно отрицательно влиять на права и свободы других лиц.

Раздел 4

ПРАВО НА ВОЗРАЖЕНИЕ И АВТОМАТИЗИРОВАННЫЙ ПРОЦЕСС ПРИНЯТИЯ РЕШЕНИЯ В КОНКРЕТНОМ СЛУЧАЕ

Статья 21

Право на возражение

1. Субъект данных на основаниях, вытекающих из его конкретной ситуации, имеет право на возражение против обработки относящихся к нему персональных данных на основе пункта (e) или (f) Статьи 6(1), включая формирование профиля, основанного на указанных положениях. Контролер не должен больше обрабатывать персональные данные, кроме случаев, когда он может подтвердить наличие веских законных оснований для обработки, которые превалируют над интересами, правами и свободами субъекта данных, или обработка необходима для обоснования, исполнения или ведения защиты по судебным искам.

2. Если персональные данные обрабатываются для целей прямого маркетинга, субъект данных должен иметь право на возражение против обработки относящихся к нему персональных данных для целей указанного маркетинга, включая формирование профиля в той мере, в какой это связано с прямым маркетингом.

3. В случае если субъект данных возражает против обработки в целях прямого маркетинга, персональные данные больше не должны обрабатываться для указанных целей.

4. Как минимум при первом общении с субъектом данных до его сведения необходимо довести информацию о наличии права, указанного в параграфах 1 и 2, указанная информация должна быть представлена четко и отдельно от любой другой информации.

5. В связи с использованием услуг информационного общества и безотносительно Директивы 2002/58/EC субъект данных может осуществлять свое право на возражение при помощи автоматизированных средств с использованием технических спецификаций.

6. В случае если персональные данные обрабатываются в целях научного или исторического исследования согласно Статье 89(1), субъект данных на основании связанной с ним конкретной ситуации должен иметь право на возражение против обработки относящихся к нему персональных данных, за исключением случаев, когда обработка необходима для выполнения задачи, осуществляемой по причинам общественного интереса.

Статья 22

Автоматизированный процесс принятия решения в конкретном случае, в том числе формирование профиля

1. Субъект данных должен иметь право не подпадать под действие решения, основанного исключительно на автоматической обработке, включая формирование профиля, которое порождает юридические последствия в отношении него или нее или существенно воздействует на него или на нее.

2. Параграф 1 не должен применяться, если решение:

(a) необходимо для заключения или исполнения договора между субъектом данных и контролером данных;

(b) допускается законодательством Союза или государства-члена ЕС, под действие которого подпадает контролер и которое также устанавливает приемлемые меры защиты прав, свобод и законных интересов субъекта данных; или

(c) основывается на прямом согласии субъекта данных.

3. В случаях, указанных в пунктах (a) и (c) параграфа 2, контролер данных должен имплементировать приемлемые меры защиты прав, свобод и законных интересов субъекта данных, как минимум права требования принятия решительных мер со стороны контролера, права на выражение своей точки зрения и на оспаривание решения.

4. Решения, указанные в параграфе 2, не должны основываться на особых категориях персональных данных, указанных в Статье 9(1), кроме случаев, когда применяется пункт (a) или (g) Статьи 9(2) и имеются приемлемые меры защиты прав, свобод и законных интересов субъекта данных.

Раздел 5

ОГРАНИЧЕНИЯ

Статья 23

Ограничения

1. Законодательство Союза или государства-члена ЕС, под действие которого подпадает контролер или лицо, обрабатывающее данные, может посредством законодательных мер ограничить объем и содержание обязательств и прав, предусмотренных в Статьях 12 - 22 и в Статье 34, а также в Статье 5 постольку, поскольку его положения соответствуют правам и обязанностям, предусмотренным в Статьях 12 - 22, если указанное ограничение соответствует сущности основных прав и свобод и является необходимой и пропорциональной мерой в демократическом обществе для обеспечения:

(a) национальной безопасности;

(b) обороны;

(c) общественной безопасности;

(d) предотвращения, расследования, раскрытия и обвинения по уголовным преступлениям или исполнения уголовных наказаний, включая защиту и предупреждение угроз общественной безопасности;

(e) иных важных целей общественного интереса Союза или государства-члена ЕС, в частности важных экономических или финансовых интересов Союза или государства-члена ЕС, включая денежные, бюджетные и налоговые вопросы, общественное здравоохранение и общественную безопасность;

(f) защиты независимости судебной власти и защиты судебного производства;

(g) предотвращения, расследования, раскрытия и уголовного преследования в отношении нарушения этики для регулируемых профессий;

(h) функции мониторинга, инспекционной и регулятивной функции, связанной, даже случайно, с осуществлением официальных полномочий в случаях, указанных в пунктах (a) - (e) и (g);

(i) защиты субъекта данных или прав и свобод других лиц;

(j) исполнения решения по гражданско-правовым искам.

2. В частности, любые законодательные меры, указанные в параграфе 1, должны содержать особые положения в отношении как минимум:

(a) целей обработки или категорий обработки;

(b) категорий персональных данных;

(c) объема и содержания введенных ограничений;

(d) гарантий против неправомерного использования, или несанкционированного доступа, или

несанкционированной передачи;

(e) спецификации контролера или категорий контролеров;

(f) сроков хранения и существующих гарантий с учетом характера, объема и целей обработки или категорий обработки;

(g) рисков для прав и свобод субъектов данных; и

(h) права субъекта данных получить информацию об ограничении, кроме случаев, когда это может нанести ущерб цели ограничения.

ГЛАВА IV. КОНТРОЛЕР И ЛИЦО, ОБРАБАТЫВАЮЩЕЕ ДАННЫЕ

Раздел 1

ОБЩИЕ ОБЯЗАТЕЛЬСТВА

Статья 24

Ответственность контролера

1. Принимая во внимание характер, объем, особенности и цели обработки, а также вероятностное возникновение рисков и опасности для прав и свобод физических лиц, контролер должен имплементировать соответствующие технические и организационные меры, гарантирующие и подтверждающие, что обработка осуществляется в соответствии с настоящим Регламентом. Указанные меры должны своевременно пересматриваться и уточняться, при необходимости.

2. Если это соизмеримо с обработкой данных, меры, указанные в параграфе 1, должны включать в себя имплементацию соответствующих мер по обеспечению защиты данных контролером.

3. Следование утвержденным нормам поведения согласно Статье 40 или утвержденным сертификационным механизмам согласно Статье 42 может быть использовано в качестве элемента для подтверждения соблюдения обязанностей контролера.

Статья 25

Защита данных по умолчанию и на основе продуманных действий

1. Принимая во внимание состояние развития науки и техники, расходы на имплементацию, характер, объем, особенности и цели обработки, а также вероятностное возникновение рисков и опасности для прав и свобод физических лиц в результате обработки, контролер должен как во время определения средств обработки, так и во время самой обработки имплементировать соответствующие технические и организационные меры, например, псевдонимизацию, которые предназначены для эффективной имплементации принципов защиты данных, например, минимизации данных, и для интегрирования необходимых гарантий в обработку в целях выполнения требований настоящего Регламента и защиты прав субъектов данных.

2. Контролер должен имплементировать соответствующие технические и организационные меры для обеспечения того, что по умолчанию обрабатываются только те персональные данные, которые необходимы для каждой конкретной цели обработки. Указанная обязанность применяется в отношении большого количества собранных персональных данных, объема их обработки, срока их хранения и возможности доступа к ним. В частности, указанные меры должны гарантировать, что по умолчанию доступ к персональным данным не будет предоставлен неопределенному количеству физических лиц без участия отдельного лица.

3. Утвержденный сертификационный механизм согласно Статье 42 может использоваться в качестве элемента для подтверждения соблюдения требований, установленных в параграфах 1 и 2 настоящей

Статьи.

Статья 26

Контролеры, осуществляющие совместную обработку

1. В случае если два или более контролера совместно определяют цели и средства обработки, они должны считаться контролерами, осуществляющими совместную обработку. Они должны посредством соглашения и с соблюдением принципов прозрачности определить соответствующие обязанности для соблюдения обязательств согласно настоящему Регламенту, в частности, в отношении осуществления прав субъекта данных, а также определить соответствующие обязанности по предоставлению информации согласно Статьям 13 и 14, за исключением случаев, когда и поскольку соответствующие обязанности контролера определены законодательством Союза или государства-члена ЕС, под действие которого подпадают контролеры. В соглашении может быть указан контрольный пункт связи для субъектов данных.

2. Соглашение, указанное в параграфе 1, должно отражать соответствующие функции и отношения осуществляющих совместную обработку контролеров относительно субъектов данных. Существование соглашения должно быть доведено до сведения субъекта данных.

3. Независимо от условий соглашения, указанного в параграфе 1, субъект данных может осуществлять свои права в рамках настоящего Регламента в отношении каждого из контролеров и в противовес каждому из них.

Статья 27

Представители контролеров или обрабатывающих данные лиц, не учрежденных в Союзе

1. В случае если применяется Статья 3(2), контролер или лицо, обрабатывающее данные, должны в письменной форме назначить представителя в Союзе.

2. Обязанность, установленная в параграфе 1 настоящей Статьи, не применяется в отношении:

(a) обработки, которая носит случайный характер, не включает в себя масштабную обработку особых категорий данных в значении Статьи 9(1) или масштабную обработку персональных данных, связанных с судимостями и уголовными преступлениями в значении Статьи 10, и которая, с учетом характера, особенностей, объема и целей обработки, предположительно не приведет к риску для прав и свобод физических лиц; или

(b) органа государственной власти или правительственного учреждения.

3. Представитель должен быть учрежден в одном из государств-членов ЕС, в котором находятся субъекты данных, персональные данные которых обрабатываются в отношении предлагаемых им товаров и услуг или поведенческая активность которых находится под наблюдением.

4. Контролер или обрабатывающее данные лицо должны уполномочить представителя решать совместно с ними или вместо них все связанные с обработкой вопросы в целях обеспечения соблюдения настоящего Регламента, особенно для надзорных органов и субъектов данных.

5. Назначение представителя контролером или обрабатывающим данные лицом должно действовать без ущерба правовым мерам в отношении самого контролера или лица, обрабатывающего данные.

Статья 28

Лицо, обрабатывающее данные

1. В случае если обработка осуществляется от имени контролера, он должен работать только с теми обрабатывающими данные лицами, которые предоставят надлежащие гарантии того, что соответствующие

технические и организационные меры будут проведены таким образом, что обработка будет соответствовать требованиям настоящего Регламента и гарантирует защиту прав субъекта данных.

2. Лицо, обрабатывающее данные, не должно привлекать к работе другое лицо, обрабатывающее данные, без предварительного особого или общего письменного разрешения контролера. В случае общего письменного разрешения лицо, обрабатывающее данные, должно проинформировать контролера о любых запланированных изменениях, касающихся привлечения или замены других лиц, обрабатывающих данные, тем самым давая контролеру возможность высказать возражение против таких изменений.

3. Обработка, осуществляемая лицом, обрабатывающим данные, должна регулироваться договором или иным юридическим актом в рамках законодательства Союза или государства-члена ЕС, который имеет обязательную силу для обрабатывающего данные лица относительно контролера и в котором указываются предмет и продолжительность обработки, характер и цель обработки, тип персональных данных и категории субъектов данных и обязанности и права контролера. Указанный договор или иной юридический акт должны в частности предусматривать, что обрабатывающее данные лицо:

(a) обрабатывает персональные данные только на основании документально подтвержденных указаний контролера, также в отношении передачи персональных данных третьей стране или международной организации, кроме случаев, когда этого требует законодательство Союза или государства-члена ЕС, под действие которого подпадает лицо, обрабатывающее данные; в таком случае лицо, обрабатывающее данные, должно проинформировать контролера об указанном законном требовании до начала обработки, за исключением случаев, когда указанное законодательство запрещает передачу указанной информации исходя из соображений общественного интереса;

(b) гарантирует, что лица, уполномоченные на обработку персональных данных, обязались соблюдать конфиденциальность или по законодательству обязаны соблюдать конфиденциальность;

(c) принимает все меры, необходимые согласно Статье 32;

(d) соблюдает условия, указанные в параграфах 2 и 4, для привлечения к работе иного лица, обрабатывающего данные;

(e) с учетом характера обработки, по мере возможности посредством соответствующих технических и организационных мер содействует контролеру в выполнении его обязанности реагировать на требования по осуществлению прав субъекта данных, установленных в Главе III;

(f) содействует контролеру при соблюдении обязанностей согласно Статьям 32 - 36, с учетом характера обработки и информации, доступной лицу, обрабатывающему данные;

(g) по выбору контролера удаляет или возвращает все персональные данные контролеру после предоставления услуг, связанных с обработкой, и удаляет существующие копии, кроме случаев, когда законодательством Союза или государства-члена ЕС требуется хранение персональных данных;

(h) предоставляет в распоряжение контролера всю информацию, необходимую для подтверждения соблюдения обязанностей, установленных в настоящей Статье, а также предусматривает возможность и содействует аудиторским проверкам, включая инспекционные проверки, проводимые контролером или аудитором, уполномоченным контролером.

С учетом пункта (h) первого подпараграфа, обрабатывающее данные лицо должно незамедлительно проинформировать контролера, если, по его мнению, указание нарушает настоящий Регламент или другие положения Союза или государства-члена ЕС по защите данных.

4. Если лицо, обрабатывающее данные, привлекает к работе другое лицо для выполнения определенной обработки данных от имени контролера, те же самые обязанности по защите данных, указанные в договоре или другом юридическом акте между контролером и лицом, обрабатывающем данные, согласно параграфу 3, должны возлагаться на указанное иное лицо, обрабатывающее данные, посредством договора или иного юридического акта в рамках законодательства Союза или государства-члена ЕС, при этом должны быть предоставлены достаточные гарантии для имплементации

соответствующих технических и организационных мер с тем, чтобы обработка соответствовала требованиям настоящего Регламента. Если указанное другое лицо, обрабатывающее данные, не выполняет обязательства по защите данных, первое лицо, обрабатывающее данные, несет ответственность перед контролером за выполнение обязанностей указанного другого лица, обрабатывающего данные.

5. Следование лицом, обрабатывающим данные, утвержденным нормам поведения согласно Статье 40 или утвержденным сертификационным механизмам согласно Статье 42 может быть использовано в качестве элемента для подтверждения достаточных гарантий, указанных в параграфах 1 - 4 настоящей Статьи.

6. Без ущерба действию индивидуального договора между контролером и лицом, обрабатывающим данные, договор или другой юридический акт, указанный в параграфах 3 и 4 настоящей Статьи, может полностью или частично основываться на стандартных договорных условиях, указанных в параграфах 7 и 8 настоящей Статьи, в том числе, если они являются составной частью сертификата, выданного контролеру или лицу, обрабатывающему данные, согласно Статьям 42 и 43.

7. Европейская Комиссия может определить стандартные договорные условия для регулирования вопросов, указанных в параграфах 3 и 4 настоящей Статьи, в соответствии с процедурой проверки согласно Статье 93(2).

8. Надзорный орган может утвердить стандартные договорные условия для регулирования вопросов, указанных в параграфах 3 и 4 настоящей Статьи, в соответствии с механизмом сопоставимости, указанным в Статье 63.

9. Договор или иной юридический акт, указанный в параграфах 3 и 4, должен быть составлен в письменном виде, в том числе в электронной форме.

10. Без ущерба Статьям 82, 83 и 84 обрабатывающее данные лицо, которое с нарушением требований настоящего Регламента определяет цели и способы обработки, должно считаться контролером в отношении указанной обработки.

Статья 29

Обработка от имени контролера
или обрабатывающего данные лица

Лицо, обрабатывающее данные, и любое лицо, действующее от имени контролера или обрабатывающего данные лица и имеющее доступ к персональным данным, должны обрабатывать указанные данные только по распоряжению контролера, за исключением случаев, предусмотренных законодательством Союза или государства-члена ЕС.

Статья 30

Учетные сведения об обработке данных

1. Каждый контролер и, в соответствующих случаях, представитель контролера должен вести учет всей деятельности, связанной с обработкой данных и подпадающей под его ответственность. Учетные сведения должны содержать всю следующую информацию:

(a) фамилию и контактные сведения контролера и, в соответствующих случаях, контролера, осуществляющего обработку совместно с ним, представителя контролера и инспектора по защите персональных данных;

(b) цели обработки;

(c) описание категорий субъектов данных и категорий персональных данных;

(d) категории получателей, которым были или будут раскрыты персональные данные, включая получателей в третьих странах или международных организациях;

(e) в соответствующих случаях, передачи персональных данных третьей стране или международной организации, включая идентификационные данные указанной третьей страны или международной организации, и в случае передачи, указанной во втором подпараграфе Статьи 49(1), документальное подтверждение надлежащих гарантий;

(f) при наличии возможности, предусмотренные сроки для уничтожения различных категорий данных;

(g) при наличии возможности, общее описание технических и организационных мер безопасности, указанных в Статье 32(1).

2. Каждое лицо, обрабатывающее данные, и, в соответствующих случаях, его представитель должны вести учет всех категорий обработки данных, осуществляемой от имени контролера; учетные сведения должны содержать следующее:

(a) фамилию и контактные сведения обрабатывающего данные лица или лиц и каждого контролера, от имени которого действует указанное лицо, и, в соответствующих случаях, представителя контролера или обрабатывающего данные лица, и инспектора по защите персональных данных;

(b) категории обработки, осуществляемой от имени контролера;

(c) в соответствующих случаях, передачи персональных данных третьей стране или международной организации, включая идентификационные данные указанной третьей страны или международной организации, и в случае передачи, указанной во втором подпараграфе Статьи 49(1), документальное подтверждение надлежащих гарантий;

(d) при наличии возможности, общее описание технических и организационных мер безопасности, указанных в Статье 32(1).

3. Учетные сведения, указанные в параграфах 1 и 2, должны сохраняться в письменном виде, в том числе в электронной форме.

4. Контролер или лицо, обрабатывающее данные, и, в соответствующих случаях, их представитель должны предоставить учетные сведения в распоряжение надзорных органов по их требованию.

5. Обязанности, указанные в параграфах 1 и 2, не должны применяться в отношении предприятия или организации, на которых занято менее 250 человек, кроме случаев, когда осуществляемая ими обработка может повлечь за собой возникновение риска для прав и свобод субъектов данных, обработка не носит случайный характер или включает в себя специальные категории данных, указанных в Статье 9(1), или персональные данные, связанные с судимостями и преступлениями согласно Статье 10.

Статья 31

Сотрудничество с надзорным органом

Контролер и обрабатывающее данные лицо, и, в соответствующих случаях, их представители, должны сотрудничать по требованию с надзорным органом при осуществлении своих задач.

Раздел 2

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 32

Безопасность обработки

1. Принимая во внимание состояние развития науки и техники, расходы на имплементацию, характер, объем, особенности и цели обработки, а также вероятностное возникновение рисков и опасности для прав и свобод физических лиц, контролер и обрабатывающее данные лицо должны имплементировать соответствующие технические и организационные меры, чтобы гарантировать соразмерный риску уровень безопасности, включая inter alia следующее:

(a) псевдонимизацию и криптографическую защиту персональных данных;

(b) способность гарантировать постоянную конфиденциальность, целостность, доступность и устойчивость систем и услуг, связанных с обработкой;

(c) способность своевременно восстанавливать доступность и доступ к персональным данным в случае возникновения инцидента физического или технического свойства;

(d) процедуру регулярной проверки и оценки эффективности технических и организационных мер для обеспечения безопасности обработки.

2. При оценке соответствующего уровня безопасности необходимо учесть риски, связанные с процессом обработки, в частности со случайным или незаконным уничтожением, потерей, изменением, несанкционированным распространением или доступом к персональным данным, которые передаются, хранятся или иным образом обрабатываются.

3. Следование утвержденным нормам поведения согласно Статье 40 или утвержденному сертификационному механизму согласно Статье 42 может быть использовано в качестве элемента для подтверждения соблюдения требований, указанных в параграфе 1 настоящей Статьи.

4. Контролер и обрабатывающее данные лицо должно принять меры для того, чтобы гарантировать, что любое физическое лицо, действующее от имени контролера или обрабатывающего данные лица и имеющее доступ к персональным данным, должно обрабатывать указанные данные только по распоряжению контролера, за исключением случаев, предусмотренных законодательством Союза или государства-члена ЕС.

Статья 33

Уведомление надзорного органа об утечке персональных данных

1. В случае утечки персональных данных контролер незамедлительно и при наличии соответствующей возможности в течение 72 часов, после того как ему стало известно об утечке, должен уведомить об этом компетентный в соответствии со Статьей 55 надзорный орган, кроме случаев, когда утечка персональных данных вероятно не приведет к риску для прав и свобод физических лиц. В случае если уведомление надзорного органа не было сделано в течение 72 часов, в нем необходимо указать причины задержки.

2. Лицо, обрабатывающее данные, должно уведомить контролера об утечке персональных данных сразу же, как только ему стало известно об этом.

3. Уведомление, указанное в параграфе 1, должно содержать в себе как минимум следующую информацию:

(a) описание характера утечки персональных данных, в том числе по возможности указание категорий и приблизительного количества субъектов данных и категории и приблизительного количество записей персональных данных;

(b) фамилию и контактные данные инспектора по защите персональных данных или иного координационного центра, в котором можно получить более подробную информацию;

(c) описание возможных последствий утечки персональных данных;

(d) описание принятых или планируемых контролером мер для устранения нарушения, в том числе, в соответствующих случаях, мер по смягчению его возможного отрицательного воздействия.

4. В случае если и постольку, поскольку в то же самое время предоставление информации не возможно, она может быть предоставлена поэтапно без дальнейшего промедления.

5. Контролер должен документировать любые утечки персональных данных, в том числе все относящиеся к утечке персональных данных факты, ее последствия и принятые корректирующие меры. Указанная документация должна обеспечить возможность проверки надзорным органом соблюдения настоящей Статьи.

Статья 34

Информирование субъекта данных об утечке персональных данных

1. В случае если утечка персональных данных может привести к высокой степени риска для прав и свобод физических лиц, контролер должен незамедлительно уведомить субъекта данных об утечке персональных данных.

2. Уведомление субъекта данных, указанное в параграфе 1 настоящей Статьи, должно описывать ясным и простым языком характер утечки персональных данных и содержать как минимум информацию и меры, указанные в пунктах (b), (c) и (d) Статьи 33(3).

3. Уведомление субъекта данных, указанное в параграфе 1, не требуется, если соблюдается любое из следующих условий:

(a) контролер имплементировал соответствующие технические и организационные меры защиты, и указанные меры применялись в отношении затронутых утечкой персональных данных, в особенности те меры, посредством которых персональные данные будут непонятны всем лицам, не обладающим доступом к ним, например, криптографическая защита;

(b) контролер принял дополнительные меры, которые гарантируют, что не возникнет высокая степень риска для прав и свобод субъектов данных согласно параграфу 1;

(c) оно требует несоразмерного усилия. В указанном случае, вместо этого делается сообщение для информирования общественности или принимается аналогичная мера, посредством которой информируются субъекты данных.

4. Если контролер еще не проинформировал субъекта данных об утечке персональных данных, надзорный орган, изучив вероятность возникновения высокой степени риска вследствие утечки персональных данных, может потребовать от контролера проинформировать субъекта данных или может принять решение о том, что соблюдается одно из условий, указанных в параграфе 3.

Раздел 3

ОЦЕНКА ВОЗДЕЙСТВИЯ НА ЗАЩИТУ ДАННЫХ
И ПРЕДВАРИТЕЛЬНАЯ КОНСУЛЬТАЦИЯ

Статья 35

Оценка воздействия на защиту данных

1. В случае если тип обработки данных, особенно при использовании новых технологий и с учетом характера, объема, особенностей и целей обработки, может привести к высокой степени риска для прав и свобод физических лиц, контролер перед обработкой осуществляет оценку воздействия предусмотренного процесса обработки данных на защиту персональных данных. Отдельная оценка может быть проведена в отношении совокупности аналогичных процессов обработки данных с аналогичной высокой степенью риска.

2. При проведении оценки воздействия на защиту данных контролер должен обратиться за советом к инспектору по защите персональных данных, если он был назначен.

3. Оценка воздействия на защиту данных, указанная в параграфе 1, требуется, в частности, в случае:

(a) систематической и масштабной оценки личностных аспектов физических лиц, которая основывается на автоматизированной обработке, включая формирование профиля, и которая служит основой для решений, порождающих юридические последствия в отношении физического лица или аналогичным образом существенно влияющих на физическое лицо;

(b) масштабной обработки особых категорий данных, указанных в Статье 9(1), или персональных данных, относящихся к уголовным приговорам и преступлениям согласно Статье 10; или

(c) систематического обширного мониторинга открытой для общего доступа области.

4. Надзорный орган должен создать и опубликовать перечень процессов обработки данных, относительно которых должна осуществляться оценка воздействия на защиту данных согласно параграфу 1. Надзорный орган должен передать данные перечни Совету, указанному в Статье 68.

5. Надзорный орган может также создать и опубликовать перечень видов обработки данных, для которых не требуется оценка воздействия на защиту данных. Надзорный орган должен передать указанные перечни Совету.

6. До утверждения перечней, указанных в параграфах 4 и 5, компетентный надзорный орган должен применить механизм сопоставимости, указанный в Статье 63, если указанные перечни охватывают обработку данных, связанных с предложением товаров и услуг субъектам данных или с мониторингом их поведенческой активности в нескольких государствах-членах ЕС или могущих существенно повлиять на свободное обращение персональных данных на территории Союза.

7. Оценка должна содержать как минимум следующее:

(a) систематическое описание предусмотренных процессов обработки данных и целей обработки, в том числе, в соответствующих случаях, законного интереса контролера;

(b) оценку необходимости и пропорциональности обработки данных относительно целей;

(c) оценку рисков для прав и свобод субъектов данных, указанных в параграфе 1; и

(d) меры, предусмотренные для устранения рисков, включая гарантии, меры безопасности и механизмы для обеспечения защиты персональных данных и подтверждения соблюдения настоящего Регламента с учетом прав и законных интересов субъектов данных и других заинтересованных лиц.

8. Соблюдение утвержденных норм поведения согласно Статье 40 соответствующими контролерами или лицами, обрабатывающими данные, следует учитывать при оценке воздействия обработки данных, проведенной указанными контролерами или лицами, обрабатывающими данные, в частности в целях оценки воздействия на защиту данных.

9. В соответствующих случаях контролер должен узнать мнение субъектов данных или их представителей относительно запланированной обработки, без ущерба защите коммерческих или общественных интересов или безопасности обработки данных.

10. В случае если обработка согласно пункту (c) или (e) Статьи 6(1) имеет правовое основание в законодательстве Союза или государства-члена ЕС, под действие которого подпадает контролер, если указанное законодательство регулирует определенный процесс обработки данных или совокупность процессов обработки и если оценка воздействия на защиту данных уже проводилась в рамках общей оценки воздействия в отношении утверждения указанного правового основания, параграфы 1 - 7 не должны применяться кроме случаев, когда государства-члены ЕС считают необходимым провести указанную оценку до обработки данных.

11. При необходимости контролер должен провести проверку для того, чтобы оценить, выполняется ли обработка в соответствии с оценкой воздействия на защиту данных, как минимум, когда имеется изменение относительно риска, связанного с обработкой данных.

Статья 36

Предварительная консультация

1. Контролер должен проконсультироваться с надзорным органом до начала обработки, если оценка воздействия на защиту данных согласно Статье 35 указывает на то, что обработка может привести к возникновению высокой степени риска при отсутствии мер, принятых контролером для снижения риска.

2. Если надзорный орган считает, что запланированная обработка согласно параграфу 1 может нарушить положения настоящего Регламента, в частности, если контролер в недостаточной степени идентифицировал или снизил риск, надзорный орган в течение не более восьми недель с момента получения запроса о проведении консультации должен предоставить контролеру и в соответствующих случаях лицу, обрабатывающему данные, письменные рекомендации и может осуществлять полномочия, указанные в Статье 58. Указанный срок может быть увеличен на шесть недель с учетом сложности запланированной обработки. Надзорный орган должен проинформировать контролера и в соответствующих случаях лицо, обрабатывающее данные, об указанном увеличении срока в течение месяца после получения запроса о проведении консультации и указать причины отсрочки. Указанные сроки могут быть приостановлены до тех пор, пока надзорный орган не получит информацию, запрашиваемую в целях консультации.

3. В случае консультации согласно параграфу 1 контролер должен предоставить надзорному органу следующую информацию:

(a) в соответствующих случаях, сведения об обязанностях контролера, контролеров, совместно осуществляющих обработку, и участвующих в обработке лиц, обрабатывающих данные, в частности при обработке в рамках группы предприятий;

(b) цели и способы запланированной обработки;

(c) меры и гарантии для защиты прав и свобод субъектов данных согласно настоящему Регламенту;

(d) в соответствующих случаях, контактные данные инспектора по защите персональных данных;

(e) оценку воздействия на защиту данных согласно Статье 35; и

(f) любую другую информацию, требуемую надзорным органом.

4. Государства-члены ЕС должны проконсультироваться с надзорным органом при подготовке предложения по законодательной мере, которая должна быть принята национальным парламентом, или при подготовке регулятивной меры, основанной на такой законодательной мере, относящейся к обработке.

5. Безотносительно параграфа 1 законодательство государства-члена ЕС может обязать контролеров проконсультироваться с надзорным органом, а также получить от него предварительное разрешение при обработке для выполнения задачи в интересах общества, в том числе при обработке в целях социальной защиты и общественного здравоохранения.

Раздел 4

ИНСПЕКТОР ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 37

Назначение инспектора по защите персональных данных

1. Контролер и обрабатывающее данные лицо должны назначить инспектора по защите персональных данных в случае, если:

(a) обработка осуществляется органом государственной власти или правительственным учреждением, за исключением судов, действующих в рамках своей судейской дееспособности;

(b) основная деятельность контролера или обрабатывающего данные лица заключается в обработке данных, которая в силу своего характера, объема и/или целей, требует масштабного, регулярного и систематического мониторинга субъектов данных; или

(c) основная деятельность контролера или обрабатывающего данные лица заключается в масштабной обработке особых категорий данных согласно Статье 6 и персональных данных, связанных с уголовными приговорами и преступлениями согласно Статье 10.

2. Группа предприятий может утвердить единого инспектора по защите персональных данных, при условии, что инспектор по защите персональных данных может быть легкодоступен от каждого учреждения.

3. В случае если контролер или обрабатывающее данные лицо является органом государственной власти или правительственным учреждением, единый инспектор по защите персональных данных может быть назначен для нескольких таких органов или учреждений, с учетом их организационной структуры и размера.

4. В случаях, отличных от указанных в параграфе 1, контролер, или обрабатывающее данные лицо, или объединения и иные органы, представляющие категории контролеров или обрабатывающих данные лиц, могут или, если этого требует законодательство Союза или государства-члена ЕС, должны назначить инспектора по защите персональных данных. Инспектор по защите персональных данных может действовать от лица указанных объединений и иных органов, представляющих контролеров или обрабатывающих данные лиц.

5. Инспектор по защите персональных данных должен назначаться на основе профессиональных качеств и, в частности, на основе экспертного знания законодательства и практики в области защиты данных, а также на основе способности выполнять задачи, указанные в Статье 39.

6. Инспектор по защите персональных данных может являться сотрудником контролера или обрабатывающего данные лица, или он может выполнять задачи на основе договора об оказании услуг.

7. Контролер или обрабатывающее данные лицо должно опубликовать контактные данные инспектора по защите персональных данных и сообщить их надзорному органу.

Статья 38

Положение инспектора по защите персональных данных

1. Контролер и обрабатывающее данные лицо должны гарантировать, что инспектор по защите персональных данных принимает своевременное и надлежащее участие в решении всех вопросов, связанных с защитой персональных данных.

2. Контролер и обрабатывающее данные лицо должны оказывать поддержку инспектору по защите персональных данных при выполнении задач, указанных в Статье 39, посредством предоставления ресурсов, необходимых для осуществления указанных задач, и доступа к персональным данным и процессу обработки, а также ресурсов, необходимых для сохранения его/ее экспертных знаний.

3. Контролер и обрабатывающее данные лицо должны гарантировать, что инспектор по защите персональных данных не получает иных указаний относительно выполнения указанных задач. Инспектор по защите персональных данных не должен быть отстранен или оштрафован контролером или обрабатывающим данные лицом за выполнение своих задач. Инспектор по защите персональных данных должен напрямую отчитываться перед руководством высшего уровня контролера или лица, обрабатывающего данные.

4. Субъекты данных могут обращаться к инспектору по защите персональных данных относительно всех вопросов, связанных с обработкой их персональных данных и с осуществлением их прав согласно настоящему Регламенту.

5. Инспектор по защите персональных данных обязан в соответствии с законодательством Союза или государства-члена ЕС соблюдать тайну или конфиденциальность при осуществлении своих задач.

6. Инспектор по защите персональных данных может выполнять иные задачи и обязанности. Контролер или обрабатывающее данные лицо должны гарантировать, что любые такие задачи и обязанности не влекут за собой конфликт интересов.

Статья 39

Задачи инспектора по защите персональных данных

1. Инспектор по защите персональных данных должен выполнять как минимум следующие задачи:

(a) информировать и давать советы контролеру или обрабатывающему данные лицу и сотрудникам, которые осуществляют обработку, относительно их обязанностей согласно настоящему Регламенту, а также согласно иным положениям Союза или государства-члена ЕС о защите данных;

(b) контролировать соблюдение настоящего Регламента, иных положений Союза или государства-члена ЕС о защите данных, а также методов контролера или обрабатывающего данные лица для защиты персональных данных, включая распределение обязанностей, повышение уровня информированности и обучение персонала, занятого в обработке данных, и соответствующие аудиторские проверки.

(c) осуществлять консультирование, при необходимости, относительно оценки воздействия на защиту данных и контролировать ее выполнение согласно Статье 35;

(d) сотрудничать с надзорным органом;

(e) действовать в качестве координационного центра для надзорного органа по вопросам, связанным с обработкой, включая предварительную консультацию согласно Статье 36, и консультировать, в соответствующих случаях, относительно иных вопросов.

2. Инспектор по защите персональных данных при выполнении своих задач должен принимать во внимание риск, связанный с процессом обработки данных, с учетом характера, объема, особенностей и целей обработки.

Раздел 5

НОРМЫ ПОВЕДЕНИЯ И СЕРТИФИКАЦИЯ

Статья 40

Нормы поведения

1. Государства-члены ЕС, надзорные органы, Совет и Европейская Комиссия должны содействовать разработке норм поведения, предназначенных для надлежащего применения настоящего Регламента, с учетом специфических особенностей различных секторов обработки и специфических потребностей микропредприятий, малых и средних предприятий.

2. Объединения и другие организации, представляющие категории контролеров или обрабатывающих данные лиц, могут разработать нормы поведения, внести в них изменения или расширить их в целях определения применения настоящего Регламента, с учетом следующего:

(a) справедливой и прозрачной обработки;

(b) законных интересов контролеров в определенных контекстах;

(c) сбора персональных данных;

(d) псевдонимизации персональных данных;

(e) информации, предоставляемой общественности и субъектам данных;

(f) осуществления прав субъектов данных;

(g) информирования и защиты детей, а также способа, посредством которого должно быть получено согласие лиц, обладающих родительской ответственностью в отношении ребенка;

(h) мер и процедур, указанных в Статьях 24 и 25, а также мер для обеспечения безопасности обработки согласно Статье 32;

(i) уведомления надзорных органов об утечке персональных данных и информирования об указанных утечках персональных данных субъектов данных;

(j) передачи персональных данных третьим странам или национальным организациям; или

(k) внесудебных процедур и иных процедур разрешения спорных вопросов между контролерами и субъектами данных в отношении обработки, без ущерба правам субъектов данных согласно Статьям 77 и 79.

3. В дополнение к соблюдению контролерами или обрабатывающими данные лицами, подпадающими под действие настоящего Регламента, нормы поведения, утвержденные в соответствии с параграфом 5 настоящей Статьи и обладающие общей действительностью согласно параграфу 9 настоящей Статьи, могут соблюдаться контролерами или обрабатывающими данные лицами, которые не подпадают под действие настоящего Регламента согласно Статье 3, для того чтобы предоставить соответствующие гарантии в рамках передачи персональных данных третьим странам или международным организациям в соответствии с пунктом (e) Статьи 46(2). Указанные контролеры или обрабатывающие данные лица должны посредством договора или иных документов, имеющих юридическую силу, взять на себя осуществимые обязательства по применению соответствующих гарантий, в том числе с учетом прав субъектов данных.

4. Норма поведения, указанная в параграфе 2 настоящей Статьи, должна содержать механизмы, которые позволят органу, указанному в Статье 41(1), осуществлять обязательный мониторинг соблюдения положений контролерами или обрабатывающими данные лицами, которые обязаны соблюдать нормы поведения, без ущерба задачам и полномочиям надзорных органов, компетентных в соответствии со Статьей 55 или 56.

5. Объединения и другие органы, указанные в параграфе 2 настоящей Статьи, которые намерены разработать норму поведения, внести изменение или расширить существующую норму, должны представить проект нормы, ее изменения или расширения надзорному органу, который является компетентным в соответствии со Статьей 55. Надзорный орган должен дать свое заключение относительно того, соответствует ли проект нормы, изменения или расширения настоящему Регламенту, и должен утвердить проект нормы, изменения или расширения, если он считает, что он предусматривает соответствующие гарантии.

6. Если проект нормы, ее изменения или расширения утвержден в соответствии с параграфом 5 и если соответствующая норма поведения не относится к обработке данных в нескольких государствах-членах ЕС, надзорный орган должен зарегистрировать и опубликовать норму.

7. В случае если проект нормы поведения относится к обработке данных в нескольких государствах-членах ЕС, надзорный орган, компетентный согласно Статье 55, до утверждения проекта нормы, ее изменения или расширения, должен передать его в соответствии с процедурой, указанной в Статье 63, Совету, который должен дать заключение относительно того, соответствует ли проект нормы, ее изменения или расширения настоящему Регламенту или в случае, указанном в параграфе 3 настоящей

Статьи, предусматривает ли он соответствующие гарантии.

8. В случае если заключение, указанное в параграфе 7, подтверждает, что проект нормы, ее изменения или расширения соответствует настоящему Регламенту или в случае, указанном в параграфе 3, предусматривает соответствующие гарантии, Совет должен представить свое заключение Европейской Комиссии.

9. Европейская Комиссия посредством имплементационных актов может принять решение о том, что переданные ей в соответствии с параграфом 8 настоящей Статьи утвержденные нормы поведения, их изменение или расширение обладают общей действительностью на территории Союза. Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки, указанной в Статье 93(2).

10. Европейская Комиссия должна гарантировать распространение информации об утвержденных нормах, общая действительность которых была признана в соответствии с параграфом 9.

11. Совет должен внести все утвержденные нормы поведения, их изменения или расширения в реестр и посредством соответствующих мер довести их до всеобщего сведения.

Статья 41

Мониторинг утвержденных норм поведения

1. Без ущерба задачам и полномочиям компетентного надзорного органа согласно Статьям 57 и 58 мониторинг соблюдения нормы поведения согласно Статье 40 может осуществляться органом, обладающим соответствующим уровнем компетентности в отношении предмета нормы и уполномоченным для указанной цели компетентным надзорным органом.

2. Орган, указанный в параграфе 1, может быть уполномочен на мониторинг соблюдения нормы поведения, если он:

(a) подтвердил компетентному надзорному органу свою независимость и компетентность в отношении предмета нормы;

(b) установил процедуру, которая позволит ему оценить, могут ли контролеры и обрабатывающие данные лица применять норму, а также проконтролировать соблюдение нормы контролерами и обрабатывающими данные лицами и проводить периодическую проверку ее применения;

(c) установил процедуры и структуры, для того чтобы рассматривать жалобы на нарушения нормы или на способы, при помощи которых норма была имплементирована или имплементируется контролером или обрабатывающим данные лицом, а также для того чтобы сделать указанные процедуры и структуры прозрачными для субъектов данных и общественности; и

(d) подтвердил компетентному надзорному органу, что его задачи и обязанности не приведут к конфликту интересов.

3. Компетентный надзорный орган должен передать проект критерий утверждения органа, указанного в параграфе 1 настоящей Статьи, Совету согласно механизму сопоставимости, указанному в Статье 63.

4. Без ущерба задачам и полномочиям компетентного надзорного органа и положениям Главы VIII орган, указанный в параграфе 1 настоящей Статьи, должен с учетом соответствующих гарантий принять надлежащие меры в случае нарушения нормы контролером или обрабатывающим данные лицом, включая временное или окончательное отстранение контролера или обрабатывающего данные лица от нормы. Он должен проинформировать компетентный надзорный орган об указанных мерах и причинах их принятия.

5. Компетентный надзорный орган должен отозвать утверждение органа, указанного в параграфе 1, если условия его утверждения больше не соблюдаются или если меры, принятые указанным органом, нарушают положения настоящего Регламента.

6. Настоящая Статья не применяется в отношении обработки, осуществляемой компетентными органами государственной власти и правительственными учреждениями.

Статья 42

Сертификация

1. Государства-члены ЕС, надзорные органы, Совет и Европейская Комиссия должны содействовать, особенно на уровне Союза, внедрению сертификационных механизмов защиты данных, а также печатей и маркировочных знаков для защиты данных в целях подтверждения соблюдения настоящего Регламента при обработке, осуществляемой контролерами и лицами, обрабатывающими данные. Необходимо учитывать определенные потребности микропредприятий, малых и средних предприятий.

2. В дополнение к соблюдению контролерами или обрабатывающими данные лицами, подпадающими под действие настоящего Регламента, сертификационные механизмы защиты данных, печати или маркировочные знаки, утвержденные в соответствии с параграфом 5 настоящей Статьи, могут быть установлены в целях подтверждения наличия соответствующих гарантий, предоставляемых контролерами или обрабатывающими данные лицами, которые не подпадают под действие настоящего Регламента согласно Статье 3, в рамках передачи персональных данных третьим странам или международным организациям в соответствии с пунктом (f) Статьи 46(2). Указанные контролеры или обрабатывающие данные лица должны посредством договора или иных документов, имеющих юридическую силу, взять на себя осуществимые обязательства по применению соответствующих гарантий, в том числе с учетом прав субъектов данных.

3. Сертификация должна быть добровольной и доступной посредством прозрачного процесса.

4. Сертификация согласно настоящей Статье не уменьшает ответственность контролера или обрабатывающего данные лица за соблюдение настоящего Регламента и действует без ущерба задачам и полномочиям надзорного органа, компетентного в соответствии со Статьей 55 или 56.

5. Сертификация согласно настоящей Статье должна осуществляться сертификационными органами, указанными в Статье 43, или компетентным надзорным органом на основе критериев, утвержденных указанным компетентным надзорным органом согласно Статье 58(3) или Советом согласно Статье 63. Если критерии утверждаются Советом, это может привести к общей сертификации, к европейской печати о защите данных.

6. Контролер или обрабатывающее данные лицо, которое подвергает осуществляемую им обработку сертификационному механизму, должно предоставить сертификационному органу, указанному в Статье 43, или в соответствующих случаях компетентному надзорному органу всю информацию, необходимую для проведения сертификационной процедуры, и обеспечить доступ к обработке данных.

7. Сертификация должна предоставляться контролеру или обрабатывающему данные лицу на срок не более трех лет, указанный срок может быть продлен на тех же самых условиях в том случае, если продолжают соблюдаться соответствующие требования. Сертификация должна быть отменена сертификационными органами, указанными в Статье 43, или компетентным надзорным органом, если требования для сертификации больше не соблюдаются.

8. Совет должен внести все сертификационные механизмы, печати и маркировочные знаки о защите данных в реестр и посредством соответствующих мер довести их до всеобщего сведения.

Статья 43

Сертификационные органы

1. Без ущерба задачам и полномочиям компетентного надзорного органа согласно Статьям 57 и 58 сертификационные органы, обладающие соответствующим уровнем компетентности в отношении защиты данных, должны после информирования надзорного органа в целях содействия ему в осуществлении его полномочий согласно пункту (h) Статьи 58(2), при необходимости, предоставить и продлить сертификацию.

Государства-члены ЕС должны гарантировать, что указанные сертификационные органы утверждены:

(a) надзорным органом, компетентным согласно Статье 55 или 56; и/или

(b) национальной сертификационной организацией, определенной в соответствии с Регламентом (ЕС) 765/2008 Европейского Парламента и Совета ЕС <*>, в соответствии с EN-ISO/IEC 17065/2012 и с дополнительными требованиями, установленными надзорным органом, компетентным согласно Статье 55 или 56.

<*> Регламент (ЕС) 765/2008 Европейского Парламента и Совета ЕС от 9 июля 2008 г., устанавливающий требования к аккредитации и надзору в отношении продукции, размещаемой на рынке ЕС, и отменяющий Регламент (ЕЭС) 339/93 (ОЖ N L 218, 13.08.2008, стр. 30).

2. Сертификационные органы, указанные в параграфе 1, должны быть аккредитованы в соответствии с указанным параграфом только, если они:

(a) подтвердили компетентному надзорному органу свою независимость и компетентность в отношении предмета сертификации;

(b) приняли на себя обязательство соблюдать критерии, указанные в Статье 42(5) и утвержденные надзорным органом, компетентным согласно Статье 55 или 56, или Советом согласно Статье 63;

(c) установили процедуры для выдачи, периодической проверки и отмены сертификации защиты данных, печатей и маркировочных знаков о защите данных;

(d) установили процедуры и структуры, для того чтобы рассматривать жалобы на нарушения сертификации или на способы, при помощи которых сертификация была имплементирована или имплементируется контролером или обрабатывающим данные лицом, а также для того чтобы сделать указанные процедуры и структуры прозрачными для субъектов данных и общественности; и

(e) подтвердили компетентному надзорному органу, что его задачи и обязанности не приведут к конфликту интересов.

3. Аккредитация сертификационных органов, указанных в параграфах 1 и 2 настоящей Статьи, должна осуществляться на основе критериев, утвержденных надзорным органом, компетентным согласно Статье 55 или 56, или Советом согласно Статье 63. В случае аккредитации согласно пункту (b) параграфа 1 настоящей Статьи, указанные требования должны дополнять требования, предусмотренные Регламентом (ЕС) 765/2008 и техническими нормами, которые описывают методы и процедуры сертификационных органов.

4. Сертификационные органы, указанные в параграфе 1, должны отвечать за надлежащую оценку, которая лежит в основе сертификации или отмены такой сертификации, без ущерба ответственности контролера или обрабатывающего данные лица за соблюдение настоящего Регламента. Аккредитация выдается на срок не более пяти лет и указанный срок может быть продлен на тех же самых условия в случае, если сертификационный орган соблюдает требования, установленные в настоящей Статье.

5. Сертификационные органы, указанные в параграфе 1, должны сообщить компетентному надзорному органу причины предоставления или отмены требуемой сертификации.

6. Требования, указанные в параграфе 3 настоящей Статьи, и критерии, указанные в Статье 42(5), должны быть опубликованы надзорным органом в легкодоступной форме. Надзорные органы должны также передать указанные требования и критерии Совету. Совет должен внести все сертификационные механизмы и печати о защите данных в реестр и посредством соответствующих мер довести их до всеобщего сведения.

7. Без ущерба действию Главы VIII компетентный надзорный орган или национальная

сертификационная организация должны отменить аккредитацию сертификационного органа согласно параграфу 1 настоящей Статьи, если условия аккредитации больше не соблюдаются или если принятые сертификационным органом меры нарушают положения настоящего Регламента.

8. Европейская Комиссия вправе принять делегированные акты в соответствии со Статьей 92 в целях установления требований, которые необходимо учесть для сертификационных механизмов защиты данных, указанных в Статье 42(1).

9. Европейская Комиссия может принять имплементационные акты, устанавливающие технические стандарты для сертификационных механизмов, печатей и маркировочных знаков о защите данных, а также механизмы для содействия и признания указанных сертификационных механизмов, печатей и маркировочных знаков. Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки, указанной в Статье 93(2).

ГЛАВА V. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ СТРАНАМ ИЛИ МЕЖДУНАРОДНЫМ ОРГАНИЗАЦИЯМ

Статья 44

Общие принципы передачи

Любая передача персональных данных, которые уже обрабатываются или которые должны будут быть обработаны после передачи третьей стране или международной организации, должна осуществляться только, если контролер или обрабатывающее данные лицо соблюдают условия, установленные в настоящей Главе, а также иные положения настоящего Регламента, включая передачу персональных данных из третьей страны или международной организации в другую третью страну или другую международную организацию. Все положения настоящей Главы должны применяться для обеспечения того, что уровень защиты физических лиц, гарантированный настоящим Регламентом, остается неизменным.

Статья 45

Передача на основании решения о соответствии

1. Передача персональных данных третьей стране или международной организации может осуществляться, если Европейская Комиссия приняла решение о том, что третья страна, территория, или один или несколько специфических секторов в указанной третьей стране, или соответствующая международная организация гарантирует надлежащий уровень защиты. Указанная передача не требует специального разрешения.

2. При оценке соответствия уровня защиты Европейская Комиссия должна, в частности, принять во внимание следующие элементы:

(a) верховенство законодательства, уважение прав и основных свобод человека, соответствующее законодательство, как общего характера, так и отраслевое, в том числе в отношении общественной безопасности, обороны, внутренней безопасности и уголовного права и доступа органов государственной власти к персональным данным, а также имплементацию указанного законодательства, норм о защите данных, профессиональных правил и мер безопасности, включая правила передачи персональных данных другой третьей стране или международной организации, которые соблюдаются в указанной третьей стране или международной организации, прецедентное право, а также эффективные и защищенные права субъектов данных и эффективные административные и правовые средства защиты для субъектов данных, персональные данные которых передаются;

(b) существование и эффективное функционирование одного или нескольких независимых надзорных органов в третьей стране или органов, в ведении которых находится международная организация, обладающих компетенцией в отношении обеспечения и реализации соблюдения норм о защите данных, включая соответствующие правоприменительные полномочия, а также в отношении содействия и

консультирования субъектов данных при осуществлении ими своих прав и сотрудничества с надзорными органами государств-членов ЕС; и

(c) международные обязательства, которые взяли на себя третья страна или международная организация, или иные обязанности, вытекающие из юридически обязательных конвенций или нормативных документов, а также из участия в многосторонних или региональных системах, в частности, в отношении защиты персональных данных.

3. Европейская Комиссия, после оценки соответствия уровня защиты, может посредством имплементационного акта принять решение о том, что третья страна, территория, или один или несколько определенных секторов в указанной третьей стране, или соответствующая международная организация гарантирует соответствующий уровень защиты в значении параграфа 2 настоящей Статьи. Имплементационный акт должен предусматривать механизм периодической проверки, как минимум каждые четыре года, которая должна учесть все соответствующие изменения в третьей стране или международной организации. Имплементационный акт должен устанавливать территориальное или секторальное применение и, при необходимости, определять надзорный орган или органы, указанные в пункте (b) параграфа 2 настоящей Статьи. Имплементационный акт должен быть принят в соответствии с процедурой проверки, указанной в Статье 93(2).

4. Европейская Комиссия на постоянной основе должна контролировать изменения в третьих странах и международных организациях, которые могут повлиять на выполнение решений, принятых согласно параграфу 3 настоящей Статьи, и решений, принятых на основе Статьи 25(6) Директивы 95/46/ЕС.

5. Европейская Комиссия при обнаружении соответствующей информации, в частности, в результате проверки, указанной в параграфе 3 настоящей Статьи, о том, что третья страна, территория, или один или несколько определенных секторов в указанной третьей стране, или соответствующая международная организация более не гарантирует в той мере, в какой это необходимо, соответствующий уровень защиты в значении параграфа 2 настоящей Статьи, должна отменить, внести изменение или приостановить действие решения, указанного в параграфе 3 настоящей Статьи, посредством имплементационных актов без эффекта обратной силы. Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки, указанной в Статье 93(2). Исходя из соображений крайней необходимости, Европейская Комиссия должна незамедлительно принять имплементационные акты в соответствии с процедурой, указанной в Статье 93(3).

6. Европейская Комиссия должна начать консультации с третьей страной или международной организацией с тем, чтобы исправить ситуацию, которая привела к решению, принятому согласно параграфу 5.

7. Решение согласно параграфу 5 настоящей Статьи действует без ущерба передаче персональных данных третьей стране, территории, одному или нескольким специфическим секторам в указанной третьей стране или соответствующей международной организации согласно Статьям 46 - 49.

8. Европейская Комиссия должна опубликовать в Официальном Журнале Европейского Союза и на своем интернет-сайте перечень третьих стран, территорий и специфических секторов в третьей стране и международных организаций, в отношении которых она приняла решение о том, что они гарантируют или больше не гарантируют соответствующий уровень защиты.

9. Решения, принятые Европейской Комиссией на основании Статьи 25(6) Директивы 95/46/ЕС, остаются в силе до тех пор, пока они не будут изменены, заменены или отменены Решением Европейской Комиссии, принятым в соответствии с параграфом 3 или 5 настоящей Статьи.

Статья 46

Передача при условии соблюдения соответствующих гарантий

1. В случае отсутствия решения согласно Статье 45(3) контролер или обрабатывающее данные лицо могут передать персональные данные третьей стране или международной организации только, если контролер или обрабатывающее данные лицо предусмотрели соответствующие гарантии и если субъекты

данных обладают юридически защищенными правами и эффективными средствами правовой защиты.

2. Соответствующие гарантии, указанные в параграфе 1, могут быть предоставлены без особого разрешения надзорного органа посредством:

(a) имеющего обязательную юридическую силу документа между органами государственной власти или правительственными учреждениями;

(b) юридически обязывающих корпоративных правил в соответствии со Статьей 47;

(c) стандартных условий о защите данных, принятых Европейской Комиссией в соответствии с процедурой проверки, указанной в Статье 93(2);

(d) стандартных условий о защите данных, принятых надзорным органом и утвержденных Европейской Комиссией согласно процедуре проверки, указанной в Статье 93(2);

(e) утвержденной нормы поведения согласно Статье 40 совместно с юридически обязывающими и защищенными обязательствами контролера или обрабатывающего данные лица в третьей стране по применению соответствующих гарантий, в том числе в отношении прав субъектов данных; или

(f) утвержденного сертификационного механизма согласно Статье 42 совместно с юридически обязывающими и защищенными обязательствами контролера или обрабатывающего данные лица в третьей стране по применению соответствующих гарантий, в том числе в отношении прав субъектов данных.

3. При условии наличия разрешения компетентного надзорного органа соответствующие гарантии, указанные в параграфе 1, могут быть также предоставлены, в частности, посредством:

(a) статей договора, согласованных между контролером или обрабатывающим данные лицом и контролером, обрабатывающим данные лицом или получателем персональных данных в третьей стране или международной организации; или

(b) положений, которые должны быть внесены в административные договоренности между органами государственной власти или правительственными учреждениями и которые включают в себя защищенные и действующие права субъектов данных.

4. Надзорный орган должен применять механизм сопоставимости согласно Статье 63 в случаях, указанных в параграфе 3 настоящей Статьи.

5. Разрешения, выданные государством-членом ЕС или надзорным органом на основании Статьи 26(2) Директивы 95/46/EC, остаются в силе до тех пор, пока они не будут при необходимости изменены, заменены или отменены указанным надзорным органом. Решения, принятые Европейской Комиссией на основании Статьи 26(4) Директивы 95/46/EC, остаются в силе до тех пор, пока они не будут при необходимости изменены, заменены или отменены Решением Европейской Комиссии, принятым в соответствии с параграфом 2 настоящей Статьи.

Статья 47

Юридически обязывающие корпоративные правила

1. Компетентный надзорный орган в соответствии с механизмом сопоставимости, указанным в Статье 63, должен утвердить юридически обязывающие корпоративные правила при условии, что они:

(a) являются юридически обязательными и применяются в отношении каждого члена группы предприятий или группы компаний, занятых в совместной экономической деятельности, в том числе их сотрудников, а также обеспечиваются указанными лицами;

(b) прямо предоставляют юридически защищенные права субъектам данных в отношении обработки

их персональных данных;

(c) соблюдают требования, установленные в параграфе 2.

2. Юридически обязывающие корпоративные правила, указанные в параграфе 1, должны определять как минимум следующее:

(a) структуру и контактные данные группы предприятий или группы компаний, занятых в совместной экономической деятельности, а также контактные данные каждого из ее членов;

(b) передачу данных или ряд таких передач, включая категории персональных данных, тип обработки и ее цели, тип субъектов данных и идентификационную информацию относительно соответствующей третьей страны или стран;

(c) свой юридически обязательный характер, как внутренне, так и внешне;

(d) применение общих принципов защиты данных, в частности, целевое ограничение, минимизация данных, ограниченные сроки хранения, качество данных, защита данных, запланированная и по умолчанию, законное основание для обработки, обработка специальных категорий персональных данных, меры для обеспечения безопасности данных, требования относительно передачи данных органам, не связанным юридически обязывающими корпоративными правилами;

(e) права субъектов данных в отношении обработки и способы осуществления указанных прав, включая право не подчиняться решениям, основанным исключительно на автоматизированной обработке, включая формирование профиля, в соответствии со Статьей 22, а также право на подачу жалобы компетентному надзорному органу и в компетентные суды государств-членов ЕС в соответствии со Статьей 79, и право на возмещение и, в соответствующем случае, компенсацию за нарушение юридически обязывающих корпоративных правил;

(f) ответственность, которую контролер или обрабатывающее данные лицо, учрежденные на территории государства-члена ЕС, берут на себя за любое нарушение юридически обязывающих корпоративных правил любым членом группы предприятий, не учрежденным в Союзе; контролер или обрабатывающее данные лицо полностью или частично освобождаются от указанной обязанности только тогда, когда они докажут, что указанный член не несет ответственность за событие, послужившее причиной ущерба;

(g) способ предоставления субъектам данных информации о юридически обязывающих корпоративных правилах, в частности, о положениях, указанных в пунктах (d), (e) и (f) настоящего параграфа, в дополнение к Статьям 13 и 14;

(h) задачи любого инспектора по защите персональных данных, назначенного в соответствии со Статьей 37, или любого иного физического или юридического лица, отвечающего за контроль соблюдения юридически обязывающих корпоративных правил в рамках группы предприятий или группы компаний, занятых в совместной экономической деятельности, а также мониторинг обучения и рассмотрения жалоб;

(i) процедуры рассмотрения жалоб;

(j) механизмы в группе предприятий или группе компаний, занятых в совместной экономической деятельности, которые гарантируют проверку и подтверждение соблюдения юридически обязывающих корпоративных правил. Указанные механизмы должны включать в себя аудиторские проверки защиты данных и методы обеспечения корректирующих мер для защиты прав субъектов данных. Результаты указанной проверки должны быть представлены физическому или юридическому лицу, указанному в пункте (h), и совету, который осуществляет контроль предприятия в группе предприятий или группе компаний, занятых в совместной экономической деятельности, указанные результаты должны быть доступны компетентному надзорному органу по его запросу;

(k) механизмы для сообщения и учета изменений в правилах, а также механизмы информирования об указанных изменениях надзорного органа;

(l) механизм сотрудничества с надзорным органом в целях обеспечения соблюдения предписаний любым членом группы предприятий или группы компаний, задействованных в совместной экономической деятельности, в частности, посредством предоставления надзорному органу результатов проверок мер, указанных в пункте (j);

(m) механизм предоставления отчетов компетентному надзорному органу относительно любых законных требований, под действие которых подпадает член группы предприятий или группы компаний, задействованных в совместной экономической деятельности, в третьей стране, и которые могут оказать существенное негативное воздействие на гарантии, предоставленные юридически обязывающими корпоративными правилами; и

(n) соответствующее обучение защите данных для персонала, имеющего постоянный доступ к персональным данным.

3. Европейская Комиссия может установить формат и процедуры для обмена информацией относительно юридически обязывающих корпоративных правил в значении настоящей Статьи между контролерами, обрабатывающими данные лицами и надзорными органами. Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки, указанной в Статье 93(2).

Статья 48

Передача или раскрытие данных,
не разрешенное законодательством Союза

Любое решение суда или трибунала и любое решение административного органа третьей страны, требующее от контролера или обрабатывающего данные лица передать или раскрыть персональные данные, может быть признано или может подлежать исполнению, если оно основано на действующем международном соглашении, например, на договоре о взаимной юридической помощи между запрашивающей третьей страной и Союзом или государством-членом ЕС, без ущерба иным основаниям для передачи согласно настоящей Главе.

Статья 49

Частичное отступление для определенных случаев

1. В случае отсутствия решения о соответствии согласно Статье 45(3) или соответствующих гарантий согласно Статье 46, включая юридически обязывающие корпоративные правила, передача или ряд передач персональных данных третьей стране или международной организации должна осуществляться только при соблюдении одного из следующих условий:

(a) субъект данных дал прямое согласие на соответствующую передачу данных после того, как он был проинформирован о возможных рисках указанной передачи данных вследствие отсутствия решения о соответствии и надлежащих гарантий;

(b) передача необходима для выполнения договора между субъектом данных и контролером или для имплементации преддоговорных мер, принятых по запросу субъекта данных;

(c) передача необходима для заключения договора или для исполнения договора, заключенного в интересах субъекта данных между контролером и другим физическим или юридическим лицом;

(d) передача необходима по причинам общественного интереса;

(e) передача необходима для обоснования, осуществления или оспаривания судебного иска;

(f) передача необходима для защиты жизненно важных интересов субъекта данных или других лиц, если субъект данных физически или юридически не может дать свое согласие;

(g) передача осуществляется из реестра, целью которого согласно законодательству Союза или

государства-члена ЕС является предоставление информации общественности и который открыт для ознакомления широкой общественности или любому лицу, которое может доказать наличие законного интереса, но только в той мере, в какой соблюдаются условия, установленные законодательством Союза или государства-члена ЕС, для ознакомления в отдельном случае.

В случае если передача не может основываться на положении Статьи 45 или 46, в том числе на положениях о юридически обязывающих корпоративных правилах, и если не применяются частичные отступления для определенных случаев согласно первому подпараграфу настоящего параграфа, передача данных третьей стране или международной организации может осуществляться только, если передача не носит повторяющийся характер, касается ограниченного количества субъектов данных, необходима в целях защиты законных интересов контролера, при условии, что интересы или права и свободы субъекта данных не превалируют над ними, и контролер оценил все обстоятельства, связанные с передачей данных, и на основании указанной оценки предусмотрел надлежащие гарантии относительно защиты персональных данных. Контролер должен проинформировать о передаче надзорный орган. В дополнение к предоставлению информации, указанной в Статьях 13 и 14, контролер должен проинформировать субъекта данных о передаче данных и о своих законных интересах.

2. Передача согласно пункту (g) первого подпараграфа параграфа 1 не должна включать в себя все персональные данные или все категории персональных данных, содержащихся в реестре. Если целью реестра является ознакомление лиц, имеющих законный интерес, передача должна осуществляться только по запросу указанных лиц или если указанные лица являются получателями данных.

3. Пункты (a), (b) и (c) первого подпараграфа параграфа 1, а также второй подпараграф параграфа 1 не должны применяться в отношении деятельности, осуществляемой органами государственной власти при выполнении ими своих полномочий.

4. Общественный интерес в значении пункта (d) первого подпараграфа параграфа 1 должен быть признан в законодательстве Союза или в законодательстве государства-члена ЕС, под действие которого подпадает контролер.

5. В случае отсутствия решения о соответствии в законодательстве Союза или государства-члена ЕС может быть по причинам общественного интереса предусмотрено ограничение передачи определенных категорий персональных данных третьей стране или международной организации. Государства-члены ЕС должны уведомить об указанных положениях Европейскую Комиссию.

6. Контролер или обрабатывающее данные лицо должно зафиксировать в учетных сведениях, указанных в Статье 30, оценку и надлежащие гарантии, указанные во втором подпараграфе параграфа 1 настоящей Статьи.

Статья 50

Международное сотрудничество для защиты персональных данных

В том, что касается третьих стран и международных организаций, Европейская Комиссия и надзорные органы должны принять соответствующие меры:

(a) для совершенствования механизмов международного сотрудничества в целях содействия эффективной реализации законодательства о защите персональных данных;

(b) для оказания международного взаимного содействия при реализации законодательства о защите персональных данных, в том числе посредством уведомления, передачи жалоб на рассмотрение, помощи в расследовании и обмена информацией, при наличии соответствующих гарантий для защиты персональных данных и других основных прав и свобод;

(c) для привлечения соответствующих заинтересованных лиц к участию в обсуждениях и деятельности, направленной на содействие международному сотрудничеству при реализации законодательства о защите персональных данных;

(d) для содействия обмену и документальному оформлению законодательства и установившейся практики в области защиты персональных данных, включая судебные конфликты с третьими странами.

ГЛАВА VI. НЕЗАВИСИМЫЕ НАДЗОРНЫЕ ОРГАНЫ

Раздел 1

НЕЗАВИСИМЫЙ СТАТУС

Статья 51

Надзорный орган

1. Каждое государство-член ЕС должно предусмотреть один или несколько независимых органов государственной власти, ответственных за мониторинг применения настоящего Регламента, для защиты основных прав и свобод физических лиц при обработке данных и для содействия свободному движению персональных данных в Союзе ("надзорный орган").

2. Каждый надзорный орган должен способствовать согласованному применению настоящего Регламента на территории всего Союза. Для указанной цели надзорные органы должны сотрудничать друг с другом и с Европейской Комиссией в соответствии с Главой VII.

3. В случае если в государстве-члене ЕС учреждено более одного надзорного органа, указанное государство-член ЕС должно определить надзорный орган, который должен будет представлять указанные органы в Совете, и установить механизм обеспечения соблюдения другими органами правил, связанных с механизмом сопоставимости согласно Статье 63.

4. Каждое государство-член ЕС не позднее 25 мая 2018 г. должно уведомить Европейскую Комиссию о положениях своего законодательства, которые оно принимает согласно настоящей Главе, а также незамедлительно о любых последующих изменениях указанных положений.

Статья 52

Независимость

1. Каждый надзорный орган должен быть полностью независим при выполнении своих задач и осуществлении своих полномочий в соответствии с настоящим Регламентом.

2. Член или члены каждого надзорного органа при выполнении своих задач и осуществлении своих полномочий в соответствии с настоящим Регламентом не должны подвергаться прямому или косвенному воздействию внешних факторов, а также не должны ни стремиться получить, ни получать указания от кого бы то ни было.

3. Член или члены каждого надзорного органа должны воздерживаться от любых действий, несовместимых с их обязанностями, и в течение срока действия полномочий не должны участвовать в любой другой несовместимой с их полномочиями оплачиваемой или неоплачиваемой деятельности.

4. Каждое государство-член ЕС должно гарантировать, что каждый надзорный орган обеспечен кадровыми, техническими или финансовыми ресурсами, помещениями и инфраструктурой, необходимой ему для эффективного выполнения задач и осуществления полномочий, в том числе в рамках взаимной помощи, сотрудничества и участия в Совете.

5. Каждое государство-член ЕС должно гарантировать, что каждый надзорный орган выбирает и располагает собственным персоналом, который находится в непосредственном подчинении члена или членов соответствующего надзорного органа.

6. Каждое государство-член ЕС должно гарантировать, что каждый надзорный орган подлежит финансовому контролю, который не влияет на его независимость, и что он имеет отдельные,

государственные, годовые бюджетные сметы, которые могут являться частью всего государственного или национального бюджета.

Статья 53

Общие условия для членов надзорного органа

1. Государства-члены ЕС должны гарантировать, что каждый член их надзорных органов утверждается посредством прозрачной процедуры:

- парламентом;

- правительством;

- главой государства; или

- независимым органом, на который возлагаются обязанности по назначению согласно законодательству государства-члена ЕС.

2. Каждый член должен обладать необходимыми для выполнения своих обязанностей и осуществления своих полномочий квалификациями, опытом и навыками, в частности, в области защиты персональных данных.

3. Обязанности члена должны заканчиваться с истечением срока действия его полномочий, с увольнением или обязательным выходом на пенсию в соответствии с законодательством государства-члена ЕС.

4. Член должен быть освобожден от должности только в случае серьезного нарушения дисциплины или если он больше не соблюдает условия, необходимые для выполнения обязанностей.

Статья 54

Правила учреждения надзорного органа

1. Каждое государство-член ЕС законодательно должно предусмотреть следующее:

(a) учреждение каждого надзорного органа;

(b) необходимые квалификации и условия для назначения члена каждого надзорного органа;

(c) правила и процедуры для назначения члена или членов каждого надзорного органа;

(d) срок полномочий члена или членов каждого надзорного органа не менее четырех лет; это не относится к первому назначению после 24 мая 2016 г., срок которого для части членов может быть меньше, если для защиты независимости надзорного органа необходима процедура дифференцированного назначения;

(e) вопрос о том, могут ли, и если да, как часто, член или члены каждого надзорного органа назначаться на новый срок;

(f) условия, регулирующие обязательства члена или членов и персонала каждого надзорного органа, запреты на несовместимые с указанными обязательствами действия, профессиональную деятельность и выплаты в течение и по окончании срока полномочий, а также правила, регулирующие прекращение службы.

2. Член или члены и персонал каждого надзорного органа в соответствии с законодательством Союза или государства-члена ЕС должны, как в течение, так и по окончании срока их полномочий, соблюдать профессиональную тайну относительно любой конфиденциальной информации, которая стала известна им

в ходе выполнения задач или осуществления полномочий. В течение срока их полномочий указанная обязанность по соблюдению профессиональной тайны должна, в частности, применяться в отношении нарушений настоящего Регламента, о которых сообщили физические лица.

Раздел 2

КОМПЕТЕНЦИЯ, ЗАДАЧИ И ПОЛНОМОЧИЯ

Статья 55

Компетенция

1. Каждый надзорный орган отвечает за выполнение поставленных задач и осуществление предоставленных ему полномочий в соответствии с настоящим Регламентом на территории его собственного государства-члена ЕС.

2. Если обработка осуществляется органами государственной власти или частными организациями, действующими на основе пункта (c) или (e) Статьи 6(1), ответственным является надзорный орган соответствующего государства-члена ЕС. В указанном случае Статья 56 не применяется.

3. Надзорные органы не должны отвечать за контроль над обработкой данных, осуществляемой судами в рамках их судейской дееспособности.

Статья 56

Компетенция главного надзорного органа

1. Без ущерба действию Статьи 55 надзорный орган центрального учреждения или единственного учреждения контролера или обрабатывающего данные лица должен выступать в качестве компетентного главного надзорного органа для трансграничной обработки, осуществляемой указанным контролером или обрабатывающим данные лицом в соответствии с процедурой, предусмотренной в Статье 60.

2. Путем частичного отступления от параграфа 1 каждый надзорный орган должен отвечать за рассмотрение поданных ему жалоб или возможных нарушений настоящего Регламента, если предмет относится только к учреждению в его государстве-члене ЕС или существенно влияет на субъекты данных только в его государстве-члене ЕС.

3. В случаях, указанных в параграфе 2 настоящей Статьи, надзорный орган должен незамедлительно проинформировать главный надзорный орган об указанном обстоятельстве. В течение трех недель после получения соответствующей информации главный надзорный орган должен принять решение о рассмотрении указанного дела в соответствии с процедурой, предусмотренной в Статье 60, принимая во внимание тот факт, находится ли учреждение контролера или обрабатывающего данные лица в государстве-члене ЕС, надзорный орган которого проинформировал его.

4. В случае если главный надзорный орган принимает решение о рассмотрении дела, должна применяться процедура согласно Статье 60. Надзорный орган, который проинформировал главный надзорный орган, может предоставить ему проект решения. Главный надзорный орган должен уделить внимание указанному проекту при подготовке проекта решения, указанного в Статье 60(3).

5. Если главный надзорный орган принимает решение не рассматривать дело, надзорный орган, который проинформировал главный надзорный орган, должен рассмотреть его согласно Статьям 61 и 62.

6. Главный надзорный орган должен являться единственным посредником контролера или обрабатывающего данные лица по вопросам, связанным с трансграничной обработкой, осуществляемой указанным контролером или обрабатывающим данные лицом.

Статья 57

Задачи

1. Без ущерба другим задачам, установленным в настоящем Регламенте, каждый надзорный орган на своей территории должен:

(a) контролировать и обеспечивать применение настоящего Регламента;

(b) содействовать информированности общества и пониманию рисков, норм, гарантий и прав в отношении обработки. Особое внимание необходимо уделять деятельности, касающейся детей;

(c) консультировать в соответствии с законодательством государства-члена ЕС, национальный парламент, правительство и другие институты и органы о законодательных и административных мерах, связанных с защитой прав и свобод физических лиц при обработке их данных;

(d) содействовать информированности контролеров и обрабатывающих данные лиц относительно их обязанностей согласно настоящему Регламенту;

(e) по запросу предоставить информацию любому субъекту данных относительно осуществления его прав согласно настоящему Регламенту и, в соответствующих случаях, сотрудничать в связи с этим с надзорными органами других государств-членов ЕС;

(f) рассматривать жалобы, поданные субъектом данных или органом, организацией или объединением в соответствии со Статьей 80, расследовать, в соответствующих случаях, предмет жалобы и в приемлемый срок проинформировать заявителя о ходе и результатах расследования, в частности, если необходимо дальнейшее расследование или сотрудничество с другим надзорным органом;

(g) сотрудничать с другими надзорными органами, включая обмен информацией и предоставление взаимной помощи, с тем, чтобы гарантировать согласованное применение и исполнение настоящего Регламента;

(h) проводить расследования относительно применения настоящего Регламента, в том числе на основании информации, предоставленной другим надзорным органом или органом государственной власти;

(i) контролировать соответствующие изменения, если они влияют на защиту персональных данных, в частности, разработку информационных и коммуникационных технологий и деловых практик;

(j) принимать стандартные договорные условия, указанные в Статье 28(8) и в пункте (d) Статьи 46(2);

(k) составить и вести список в отношении требования об оценке воздействия на защиту данных согласно Статье 35(4);

(l) консультировать относительно обработки данных, указанной в Статье 36(2);

(m) способствовать разработке норм поведения согласно Статье 40(1), давать заключение и утверждать указанные нормы поведения, которые обеспечивают соответствующие гарантии согласно Статье 40(5);

(n) способствовать установлению сертификационных механизмов защиты данных, а также печатей и маркировочных знаков для защиты данных согласно Статье 42(1) и утверждать критерии сертификации согласно Статье 42(5);

(o) в соответствующих случаях, проводить периодическую проверку выданных в соответствии со Статьей 42(7) сертификаций;

(p) составить и опубликовать критерии аккредитации органа по контролю за соблюдением норм поведения согласно Статье 41 и критерии аккредитации сертификационного органа согласно Статье 43;

(q) провести аккредитацию органа по контролю за соблюдением норм поведения согласно Статье 41 и

аккредитацию сертификационного органа согласно Статье 43;

(r) утвердить условия договора и положения, указанные в Статье 46(3);

(s) утвердить юридически обязывающие корпоративные правила согласно Статье 47;

(t) содействовать деятельности Совета;

(u) вести внутренний учет нарушений настоящего Регламента и мер, принятых в соответствии со Статьей 58(2); и

(v) выполнять иные задачи, связанные с защитой персональных данных.

2. Каждый надзорный орган должен облегчить подачу жалоб, указанных в пункте (f) параграфа 1, посредством таких мер, как предоставление формы для подачи жалобы, которая может заполняться электронным образом, не исключая других способов взаимодействия.

3. Выполнение задач каждого надзорного органа осуществляется на бесплатной основе для субъекта данных и, в соответствующих случаях, для инспектора по защите персональных данных.

4. В случае если запросы явно не обоснованы или чрезмерны, в частности, вследствие их повторяющегося характера, надзорный орган может взимать приемлемую плату на основе административных расходов или отказаться действовать на основании запроса. Надзорный орган должен нести бремя доказывания необоснованного или чрезмерного характера запроса.

Статья 58

Полномочия

1. Каждый надзорный орган должен располагать следующими следственными полномочиями:

(a) поручать контролеру и обрабатывающему данные лицу и, в соответствующих случаях, их представителю предоставить любую информацию, необходимую ему для выполнения его задач;

(b) проводить расследования в форме аудиторских проверок защиты данных;

(c) проводить проверку сертификаций, предоставленных согласно Статье 42(7);

(d) уведомить контролера или обрабатывающее данные лицо о предполагаемом нарушении настоящего Регламента;

(e) от контролера или обрабатывающего данные лица получить доступ ко всем персональным данным и всей информации, необходимой ему для выполнения его задач;

(f) получить доступ к любым помещениям контролера или обрабатывающего данные лица, включая оборудование и средства для обработки данных, в соответствии с процессуальным законодательством Союза или государства-члена ЕС.

2. Каждый надзорный орган должен располагать следующими корректирующими полномочиями:

(a) выдавать предупреждения контролеру или обрабатывающему данные лицу о том, что запланированная обработка данных может нарушать положения настоящего Регламента;

(b) делать предупреждения контролеру или обрабатывающему данные лицу, если обработка данных нарушила положения настоящего Регламента;

(c) требовать от контролера или обрабатывающего данные лица соблюдать запросы субъекта данных относительно осуществления его прав согласно настоящему Регламенту;

(d) потребовать от контролера или обрабатывающего данные лица привести процесс обработки данных в соответствие положениям настоящего Регламента, при необходимости, в установленном порядке и в установленный срок;

(e) потребовать от контролера сообщить субъекту данных об утечке персональных данных;

(f) наложить временное или окончательное ограничение на обработку данных, включая запрет;

(g) потребовать исправить или уничтожить персональные данные или ограничить обработку согласно Статьям 16, 17 и 18, а также уведомить об указанных мерах получателей, которым были раскрыты персональные данные согласно Статье 17(2) и Статье 19;

(h) отменить сертификацию, или потребовать от сертификационного органа отменить сертификацию, предоставленную согласно Статьям 42 и 43, или потребовать от сертификационного органа не предоставлять сертификацию, если не соблюдаются требования для сертификации;

(i) наложить административный штраф в соответствии со Статьей 83 в дополнение к или вместо мер, указанных в настоящем параграфе, в зависимости от обстоятельств каждого отдельного случая;

(j) потребовать приостановить передачу данных получателю в третьей стране или международной организации.

3. Каждый надзорный орган должен располагать следующими разрешительными и консультативными полномочиями:

(a) консультировать контролера в соответствии с процедурой предварительной консультации, указанной в Статье 36;

(b) по собственной инициативе или по запросу выдавать национальному парламенту, правительству государства-члена ЕС или в соответствии с законодательством государства-члена ЕС другим институтам или органам, а также общественности заключения по любому вопросу, связанному с защитой персональных данных;

(c) разрешать обработку, указанную в Статье 36(5), если в соответствии с законодательством государства-члена ЕС требуется указанное предварительное разрешение;

(d) выдавать заключение и утверждать проект норм поведения согласно Статье 40(5);

(e) аккредитовывать сертификационные органы согласно Статье 43;

(f) выдавать сертификации и утверждать критерии сертификации в соответствии со Статьей 42(5);

(g) принимать стандартные условия по защите данных, указанные в Статье 28(8) и в пункте (d) Статьи 46(2);

(h) утверждать договорные условия, указанные в пункте (a) Статьи 46(3);

(i) разрешать административные договоренности, указанные в пункте (b) Статьи 46(3);

(j) утверждать юридически обязывающие корпоративные правила согласно Статье 47.

4. Полномочия, предоставленные надзорному органу согласно настоящей Статье, осуществляются при условии наличия соответствующих гарантий, включая эффективные средства судебной защиты и должную процедуру, установленную в законодательстве Союза или государства-члена ЕС в соответствии с Хартией.

5. Каждое государство-член ЕС должно законодательно предусмотреть, что его надзорный орган вправе довести до сведения органов судебной власти факт нарушения настоящего Регламента и, в соответствующих случаях, вправе начать или иным образом участвовать в судебном процессе в целях

обеспечения исполнения положений настоящего Регламента.

6. Каждое государство-член ЕС может законодательно предусмотреть, что его надзорный орган должен обладать полномочиями, дополнительными к полномочиям, указанным в параграфах 1, 2 и 3. Выполнение указанных полномочий не влияет на эффективное осуществление Главы VII.

Статья 59

Отчеты о проделанной работе

Каждый надзорный орган подготавливает ежегодный отчет о проделанной работе, который может включать в себя перечень типов выявленных нарушений и принятых мер в соответствии со Статьей 58(2). Указанные отчеты должны передаваться национальному парламенту, правительству и другим органам, определенным законодательством государства-члена ЕС. Они должны быть доведены до сведения общественности, Европейской Комиссии и Совета.

ГЛАВА VII. СОТРУДНИЧЕСТВО И СОПОСТАВИМОСТЬ

Раздел 1

СОТРУДНИЧЕСТВО

Статья 60

Сотрудничество между главным надзорным органом
и другими соответствующими надзорными органами

1. В стремлении достичь консенсуса главный надзорный орган должен сотрудничать с другими надзорными органами в соответствии с настоящей Статьей. Главный надзорный орган и соответствующие надзорные органы должны обмениваться друг с другом всей существенной информацией.

2. Главный надзорный орган всегда может запросить соответствующие другие надзорные органы о предоставлении взаимной помощи согласно Статье 61 и может проводить совместные действия согласно Статье 62, в частности, для осуществления расследований или мониторинга имплементации меры относительно контролера или обрабатывающего данные лица, учрежденных в другом государстве-члене ЕС.

3. Главный надзорный орган должен незамедлительно передать соответствующую информацию по делу другим надзорным органам. Он без промедления должен представить проект решения другим надзорным органам для их заключения и принять во внимание их мнение.

4. В случае если один из соответствующих надзорных органов в течение четырех недель после проведения консультации в соответствии с параграфом 3 настоящей Статьи высказывает существенное и мотивированное возражение против проекта решения, главный надзорный орган, если он не согласен с существенным и мотивированным возражением или считает, что возражение не существенно и не мотивировано, должен инициировать в отношении данного вопроса механизм сопоставимости, указанный в Статье 63.

5. В случае если главный надзорный орган соглашается с существенным и мотивированным возражением, он должен передать другим надзорным органам доработанный проект решения для их заключения. Указанный доработанный проект решения должен подлежать процедуре, указанной в параграфе 4, в течение двух недель.

6. Если ни один из других надзорных органов не возражает против проекта решения, который был представлен главным надзорным органом в течение срока, указанного в параграфах 4 и 5, главный надзорный орган и соответствующие надзорные органы считаются согласными с указанным проектом решения и должны быть им связаны.

7. Главный надзорный орган должен принять решение и уведомить о нем основное учреждение или единственное учреждение контролера или обрабатывающего данные лица, в соответствующих случаях, и проинформировать другие надзорные органы и Совет об указанном решении, включая краткое изложение фактов и оснований. Надзорный орган, которому была подана жалоба, должен проинформировать заявителя о решении.

8. Путем частичного отступления от параграфа 7, если жалоба отклонена или признана несостоятельной, надзорный орган, которому она была подана, должен утвердить решение и уведомить о нем заявителя и проинформировать контролера.

9. В случае если главный надзорный орган и соответствующие надзорные органы отклоняют или признают несостоятельной только часть жалобы и действуют в соответствии с другой ее частью, по каждой части дела необходимо принять отдельное решение. Главный надзорный орган должен вынести решение по части, касающейся действий в отношении контролера, должен уведомить о нем основное учреждение или единственное учреждение контролера или обрабатывающего данные лица на территории своего государства-члена ЕС, а также должен проинформировать о нем заявителя; при этом надзорный орган заявителя должен вынести решение по части, касающейся отклонения жалобы или признания ее несостоятельной, и должен уведомить об этом заявителя и проинформировать контролера или обрабатывающее данные лицо.

10. После уведомления о решении главного надзорного органа согласно параграфам 7 и 9 контролер или обрабатывающее данные лицо должно принять необходимые меры, чтобы гарантировать соблюдение решения в отношении обработки данных во всех его учреждениях в Союзе. Контролер или обрабатывающее данные лицо должно уведомить о мерах, принятых в целях соблюдения решения, главный надзорный орган, который должен проинформировать другие соответствующие надзорные органы.

11. Если в исключительных обстоятельствах соответствующий надзорный орган имеет основания полагать, что существует острая необходимость действовать в целях защиты интересов субъектов данных, должна применяться неотложная процедура, указанная в Статье 66.

12. Главный надзорный орган и другие надзорные органы должны предоставлять друг другу информацию, необходимую согласно настоящей Статье, электронным способом, с использованием стандартизованного формата.

Статья 61

Взаимная помощь

1. Надзорные органы должны предоставлять друг другу соответствующую информацию и оказывать взаимную помощь в целях единообразной имплементации и применения настоящего Регламента; они должны принимать меры для эффективного сотрудничества друг с другом. Взаимная помощь, в частности, распространяется на информационные запросы и меры надзора, например, на запросы относительно предварительных консультаций и разрешений, а также относительно проведения проверок и расследований.

2. Каждый надзорный орган должен принять все соответствующие меры, чтобы незамедлительно и не позднее одного месяца после получения запроса дать на него ответ другому надзорному органу. Указанные меры могут включать в себя, в частности, передачу соответствующей информации о проведении расследования.

3. Запросы об оказании помощи должны содержать в себе всю необходимую информацию, включая цели и причины запроса. Переданная информация должна использоваться исключительно для цели, указанной в запросе.

4. Запрашиваемый надзорный орган должен отклонить запрос только в случае, если:

(a) он не обладает компетенцией относительно предмета запроса или относительно мер, которые он согласно запросу должен выполнить; или

(b) выполнение запроса может нарушить положения настоящего Регламента или законодательства Союза или государства-члена ЕС, под действие которого подпадает надзорный орган, получивший запрос.

5. Запрашиваемый надзорный орган должен проинформировать запрашивающий надзорный орган о результатах или, в соответствующих случаях, о ходе выполнения мер, принятых в ответ на запрос. Запрашиваемый надзорный орган должен предоставить причины отказа в выполнении запроса в соответствии с параграфом 4.

6. Запрашиваемый надзорный орган должен предоставлять информацию, требуемую другими надзорными органами, как правило, электронным способом, с использованием стандартизованного формата.

7. Запрашиваемый надзорный орган не должен взимать плату за действия, предпринятые им в соответствии с запросом о взаимной помощи. Надзорные органы могут согласовать правила по возмещению друг другу в исключительных случаях особых затрат, возникших в результате предоставления взаимной помощи.

8. В случае если надзорный орган не предоставляет информацию, указанную в параграфе 5 настоящей Статьи, в течение месяца после получения запроса от другого надзорного органа, запрашивающий надзорный орган может принять временную меру на территории своего государства-члена ЕС в соответствии со Статьей 55(1). В указанном случае острая необходимость действия согласно Статье 66(1) требует срочного обязывающего решения Совета согласно Статье 66(2).

9. Европейская Комиссия посредством имплементационных актов может определить формат и процедуры взаимной помощи, указанной в настоящей Статье, а также формы электронного обмена информацией между надзорными органами и между надзорными органами и Советом, в частности, установить стандартизованный формат, указанный в параграфе 6 настоящей Статьи. Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки, указанной в Статье 93(2).

Статья 62

Совместные действия надзорных органов

1. Надзорные органы должны в соответствующих случаях проводить совместные действия, включая совместные расследования и совместные принудительные меры, в которых участвуют члены и персонал надзорных органов других государств-членов ЕС.

2. Если учреждения контролера или обрабатывающего данные лица находятся в нескольких государствах-членах ЕС или если обработка данных может существенно повлиять на значительное количество субъектов данных более чем в одном государстве-члене ЕС, надзорный орган каждого из указанных государств-членов ЕС вправе участвовать в совместных действиях. Надзорный орган, компетентный согласно Статье 56(1) или (4), должен пригласить надзорный орган каждого из указанных государств-членов ЕС принять участие в совместных действиях и должен незамедлительно дать ответ на запрос надзорного органа об участии.

3. Надзорный орган в соответствии с законодательством государства-члена ЕС и с разрешения оказывающего поддержку надзорного органа может наделить полномочиями, в том числе следственными полномочиями, участвующих в совместных действиях членов или персонал оказывающего поддержку надзорного органа, или постольку, поскольку это допустимо согласно законодательству государства-члена ЕС основного надзорного органа, может позволить членам или персоналу оказывающего поддержку надзорного органа осуществлять их следственные полномочия в соответствии с законодательством государства-члена ЕС оказывающего поддержку надзорного органа. Указанные следственные полномочия могут осуществляться только под руководством и в присутствии членов или персонала основного надзорного органа. Члены или персонал оказывающего поддержку надзорного органа подпадают под действие законодательства государства-члена ЕС основного надзорного органа.

4. Если в соответствии с параграфом 1 персонал оказывающего поддержку надзорного органа

осуществляет свою деятельность в другом государстве-члене ЕС, государство-член ЕС основного надзорного органа должно взять на себя ответственность за их действия, в том числе финансовые обязательства за любой ущерб, причиненный в результате их деятельности, в соответствии с законодательством государства-члена ЕС, на территории которого они осуществляют свою деятельность.

5. Государство-член ЕС, на территории которого был причинен ущерб, должно устранить причиненный ущерб согласно условиям, применимым в отношении ущерба, причиненного его собственным персоналом. Государство-член ЕС оказывающего поддержку надзорного органа, персонал которого причинил ущерб любому лицу на территории другого государства-члена ЕС, должно возместить указанному другому государству-члену ЕС в полном размере любую сумму, которую оно заплатило лицам, управомоченным от их имени.

6. Без ущерба осуществлению прав по отношению к третьим сторонам и за исключением параграфа 5 каждое государство-член ЕС в случае, предусмотренном в параграфе 1, должно отказаться от запрашиваемого возмещения от другого государства-члена ЕС относительно ущерба, указанного в параграфе 4.

7. В случае если совместные действия запланированы и надзорный орган в течение одного месяца не выполняет обязательство, установленное во втором предложении параграфа 2 настоящей Статьи, другие надзорные органы могут утвердить временную меру на территории своего государства-члена ЕС в соответствии со Статьей 55. В указанном случае острая необходимость действия согласно Статье 66(1) требует заключения или срочного обязывающего решения Совета согласно Статье 66(2).

Раздел 2

СОПОСТАВИМОСТЬ

Статья 63

Механизм сопоставимости

В целях содействия единообразному применению настоящего Регламента в Союзе надзорные органы должны сотрудничать друг с другом и в соответствующих случаях с Европейской Комиссией в рамках указанного в настоящем Разделе механизма сопоставимости.

Статья 64

Заключение Совета

1. Совет должен дать свое заключение, если компетентный надзорный орган намерен утвердить одну из нижеследующих мер. В этой связи компетентный надзорный орган должен передать Совету проект решения, если он:

(a) направлен на утверждение перечня процессов обработки данных в соответствии с требованием об оценке воздействия на защиту данных согласно Статье 35(4);

(b) касается обстоятельства согласно Статье 40(7), а также вопроса относительно того, соответствует ли проект нормы поведения или ее изменение или расширение настоящему Регламенту;

(c) направлен на утверждение критериев для аккредитации органа согласно Статье 41(3) или сертификационного органа согласно Статье 43(3);

(d) направлен на определение стандартных условий защиты данных, указанных в пункте (d) Статьи 46(2) и в Статье 28(8);

(e) направлен на утверждение договорных условий согласно пункту (a) Статьи 46(3); или

(f) направлен на утверждение юридически обязывающих корпоративных правил в значении Статьи 47.

2. Любой надзорный орган, президиум Совета или Европейская Комиссия могут потребовать, чтобы любое дело общего применения или оказывающее воздействие в нескольких государствах-членах ЕС было изучено Советом в целях получения заключения, в частности, если компетентный надзорный орган не выполняет обязательства по оказанию взаимной помощи в соответствии со Статьей 61 или в отношении совместных действий в соответствии со Статьей 62.

3. В случаях, указанных в параграфах 1 и 2, Совет должен дать заключение по представленному ему на рассмотрение делу при условии, что он уже не дал своего заключения по тому же самому делу. Указанное заключение должно быть принято в течение восьми недель простым большинством голосов членов Совета. Указанный срок может быть продлен еще на шесть недель с учетом сложности предмета рассмотрения. В отношении указанного в параграфе 1 проекта решения, направленного членам Совета в соответствии с параграфом 5, предполагается, что член, который не высказывает возражений в приемлемый срок, установленный Президиумом, согласен с проектом решения.

4. Надзорные органы и Европейская Комиссия незамедлительно должны передать Совету электронным способом, с использованием стандартизированного формата любую соответствующую информацию, в том числе в соответствующих случаях краткое изложение фактов, проект решения, основания для принятия необходимой меры, а также мнения других соответствующих надзорных органов.

5. Президиум Совета незамедлительно должен электронным способом проинформировать:

(a) членов Совета и Европейскую Комиссию о любой направленной ему соответствующей информации с использованием стандартизированного формата. Секретариат Совета при необходимости должен обеспечить перевод соответствующей информации; и

(b) надзорный орган, указанный в соответствующих случаях в параграфах 1 и 2, и Европейскую Комиссию о своем заключении и опубликовать его.

6. Компетентный надзорный орган не должен принимать проект решения, указанный в параграфе 1, в течение срока, указанного в параграфе 3.

7. Надзорный орган, указанный в параграфе 1, должен принять во внимание заключение Совета и в течение двух недель после получения заключения электронным способом, с использованием стандартизированного формата сообщить Президиуму Совета о том, оставит ли он проект решения без изменений или внесет в него изменения; в соответствующих случаях он должен передать измененный проект решения.

8. В случае если соответствующий надзорный орган в течение срока, указанного в параграфе 7 настоящей Статьи, информирует Президиум Совета о том, что он не намерен частично или полностью следовать заключению Совета, и указывает соответствующие причины, должна применяться Статья 65(1)

Статья 65

Решение Советом спорных вопросов

1. Для того чтобы в отдельных случаях гарантировать правильное и единообразное применение настоящего Регламента, Совет должен принять обязательное для исполнения решение в следующих случаях:

(a) если в случае, указанном в Статье 60(4), соответствующий надзорный орган высказал соответствующее и обоснованное возражение против проекта решения главного органа или главный орган отклонил указанное возражение по причине его несоответствия или необоснованности. Обязательное для исполнения решение должно касаться всех обстоятельств, которые являются предметом соответствующего и обоснованного возражения, в частности, вопросов относительно наличия нарушения настоящего Регламента;

(b) если имеются противоречивые точки зрения относительно того, какой из соответствующих надзорных органов отвечает за основное учреждение;

(c) если компетентный надзорный орган не требует заключения Совета в случаях, указанных в Статье 64(1), или не следует заключению Совета, предоставленному согласно Статье 64. В указанном случае любой соответствующий надзорный орган или Европейская Комиссия могут передать дело Совету.

2. Решение, указанное в параграфе 1, должно быть принято в течение одного месяца после передачи предмета дела на рассмотрение большинством в две трети голосов членов Совета. Указанный срок может быть продлен еще на один месяц исходя из сложности предмета рассмотрения. Решение, указанное в параграфе 1, должно быть мотивированным и направлено в главный надзорный орган и всем соответствующим надзорным органам; оно должно быть обязательным для их исполнения.

3. Если Совет не смог принять решение в течение срока, указанного в параграфе 1, он должен принять свое решение в течение двух недель после истечения второго месяца, указанного в параграфе 2, простым большинством голосов членов Совета. При равенстве голосов членов Совета правом решающего голоса при принятии решения обладает его Президиум.

4. Соответствующие надзорные органы не должны принимать решение по существу вопроса, направленного в Совет согласно параграфу 1, в течение сроков, указанных в параграфах 2 и 3.

5. Президиум Совета должен незамедлительно уведомить о решении, указанном в параграфе 1, соответствующие надзорные органы. Он должен проинформировать о нем Европейскую Комиссию. Решение должно быть опубликовано на интернет-сайте Совета сразу после того, как надзорный орган уведомит об окончательном решении, указанном в параграфе 6.

6. Главный надзорный орган или, в соответствующих случаях, надзорный орган, которому была подана жалоба, должен принять свое окончательное решение на основании решения, указанного в параграфе 1 настоящей Статьи, незамедлительно и не позднее одного месяца, после того как Совет уведомил о своем решении. Главный надзорный орган или, в соответствующих случаях, надзорный орган, которому была подана жалоба, должен проинформировать Совет о дате, когда контролер или обрабатывающее данные лицо и субъект данных будут уведомлены о его окончательном решении. Окончательное решение надзорных органов должно быть принято согласно Статье 60(7), (8) и (9). Окончательное решение должно соотноситься с решением, указанным в параграфе 1 настоящей Статьи, и должно устанавливать, что решение, указанное в данном параграфе, будет опубликовано на интернет-сайте Совета в соответствии с параграфом 5 настоящей Статьи. К окончательному решению должно прилагаться решение, указанное в параграфе 1 настоящей Статьи.

Статья 66

Неотложная процедура

1. В исключительных обстоятельствах, если соответствующий надзорный орган считает, что существует острая необходимость в защите прав и свобод субъектов данных, он может, путем частичного отступления от механизма сопоставимости, указанного в Статьях 63, 64 и 65, или от процедуры, указанной в Статье 60, незамедлительно принять временные меры, порождающие юридические последствия на его собственной территории, с определенным сроком действия, который не должен превышать трех месяцев. Надзорный орган незамедлительно должен сообщить об указанных мерах и причинах для их принятия другим соответствующим надзорным органам, Совету и Европейской Комиссии.

2. В случае если надзорный орган принял меру согласно параграфу 1 и считает, что необходимо срочно принять окончательные меры, он может запросить неотложного заключения Совета или срочного обязательного решения Совета и указать причины запроса такого заключения или решения.

3. Любой надзорный орган может запросить Совет предоставить неотложное заключение или, в соответствующем случае, срочное обязательное решение, если компетентный надзорный орган не принял соответствующую меру, несмотря на то, что имелась острая необходимость в защите прав и свобод субъектов данных, и указать причины для запроса такого заключения или решения, в том числе в отношении указанной острой необходимости.

4. Путем частичного отступления от Статьи 64(3) и от Статьи 65(2) неотложное заключение или

срочное обязательное решение согласно параграфам 2 и 3 настоящей Статьи должно быть принято в течение двух недель простым большинством голосов членов Совета.

Статья 67

Обмен информацией

Европейская Комиссия может принимать имплементационные акты общего действия для того, чтобы определить порядок электронного обмена информацией между надзорными органами, а также между надзорными органами и Советом, в частности, стандартизированный формат, указанный в Статье 64.

Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки согласно Статье 93(2).

Раздел 3

ЕВРОПЕЙСКИЙ СОВЕТ ПО ЗАЩИТЕ ДАННЫХ

Статья 68

Европейский совет по защите данных

1. Европейский совет по защите данных ("Совет") настоящим учреждается в качестве органа Союза и обладает правоспособностью.

2. Совет представлен его Президиумом.

3. В состав Совета входят глава одного надзорного органа каждого государства-члена ЕС и Европейский инспектор по защите персональных данных или их представители.

4. В случае если в государстве-члене ЕС более одного надзорного органа отвечают за мониторинг применения положений настоящего Регламента, в соответствии с законодательством указанного государства-члена ЕС должен быть назначен совместный представитель.

5. Европейская Комиссия вправе принимать участие в деятельности и заседаниях Совета без права голоса. Европейская Комиссия должна назначить представителя. Президиум Совета должен сообщать Европейской Комиссии о деятельности Совета.

6. В случаях, указанных в Статье 65, Европейский инспектор по защите персональных данных имеет право голоса только в отношении решений, которые касаются принципов и правил, применяемых к институтам, органам, ведомствам и агентствам Союза, и которые по существу соответствуют принципам и правилам настоящего Регламента.

Статья 69

Независимость

1. Совет должен действовать независимо при выполнении своих задач и осуществлении своих полномочий согласно Статьям 70 и 71.

2. Без ущерба требованиям Европейской Комиссии, указанным в пункте (b) Статьи 70(1) и в Статье 70(2), Совет при выполнении своих задач и осуществлении своих полномочий не должен ни стремиться получить, ни получать указания от кого бы то ни было.

Статья 70

Задачи Совета

1. Совет должен гарантировать единообразное применение настоящего Регламента. В этой связи Совет должен по собственной инициативе или, в соответствующих случаях, по требованию Европейской Комиссии, в частности:

(a) контролировать и гарантировать правильное применение настоящего Регламента в случаях, предусмотренных в Статьях 64 и 65, без ущерба задачам национальных надзорных органов;

(b) консультировать Европейскую Комиссию по любому вопросу, связанному с защитой персональных данных в Союзе, включая любые предполагаемые изменения настоящего Регламента;

(c) консультировать Европейскую Комиссию относительно формата и процедур обмена информацией между контролерами, обрабатывающими данные лицами и надзорными органами в отношении юридически обязывающих корпоративных правил;

(d) издавать руководящие указания, рекомендации и стандарты передовой практики относительно процедур удаления ссылок на персональные данные, копий или реплик указанных данных с общедоступных служб связи согласно Статье 17(2);

(e) по собственной инициативе, по запросу одного из своих членов или по требованию Европейской Комиссии рассматривать любые вопросы, связанные с применением настоящего Регламента, и издавать руководящие указания, рекомендации и стандарты передовой практики в целях содействия единообразному применению настоящего Регламента;

(f) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа для дальнейшего определения критериев и условий для решений, основанных на формировании профиля, согласно Статье 22(2);

(g) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа для установления утечек персональных данных и определения неоправданной задержки в значении Статьи 33(1) и (2), а также в отношении особых обстоятельств, при которых контролер или обрабатывающее данные лицо должны уведомить об утечке персональных данных;

(h) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа относительно обстоятельств, при которых утечка персональных данных может привести к высокой степени риска для прав и свобод физических лиц согласно Статье 34(1);

(i) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа в целях дальнейшего определения критериев и требований для передачи персональных данных, основанной на юридически обязывающих корпоративных правилах контролера или обрабатывающего данные лица, а также на необходимых требованиях, гарантирующих защиту персональных данных субъектов данных согласно Статье 47;

(j) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа в целях дальнейшего определения критериев и требований относительно передачи персональных данных на основании Статьи 49(1);

(k) разрабатывать руководящие указания для надзорных органов относительно применения мер, указанных в Статье 58(1), (2) и (3), и установить административные штрафы согласно Статье 83;

(l) проверять практическое применение руководящих указаний, рекомендаций и стандартов передовой практики согласно пунктам (e) и (f);

(m) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа в отношении установления общих процедур для сообщений физических лиц о нарушениях настоящего Регламента согласно Статье 54(2);

(n) содействовать разработке норм поведения и установлению сертификационных механизмов защиты данных, печатей и маркировочных знаков для защиты данных согласно Статьям 40 и 42;

(o) осуществлять аккредитацию сертификационных органов и их регулярную проверку согласно Статье 43, а также вести открытый реестр аккредитованных органов согласно Статье 43(6) и аккредитованных контролеров и обрабатывающих данные лиц, учрежденных в третьих странах согласно Статье 42(7);

(p) определить требования, указанные в Статье 43(3), в целях аккредитации сертификационных органов согласно Статье 42;

(q) представить Европейской Комиссии заключение относительно сертификационных требований, указанных в Статье 43(8);

(r) представить Европейской Комиссии заключение относительно графических обозначений, указанных в Статье 12(7);

(s) представить Европейской Комиссии заключение относительно оценки соответствия уровня защиты в третьей стране или в международной организации, включая оценку вопроса относительно того, что третья страна, территория, или один или несколько специфических секторов в указанной третьей стране, или международная организация больше не гарантирует соответствующий уровень безопасности. В этой связи Европейская Комиссия должна представить Совету всю необходимую документацию, в том числе переписку с правительством третьей страны, в отношении указанной третьей страны, территории или специфического сектора, или с международной организацией.

(t) выдавать заключения относительно проектов решений надзорных органов согласно механизму сопоставимости, указанному в Статье 64(1), относительно вопросов, переданных на рассмотрение согласно Статье 64(2), а также выдавать обязательные для исполнения решения согласно Статье 65, в том числе в случаях, указанных в Статье 66;

(u) содействовать сотрудничеству, а также эффективному двустороннему и многостороннему обмену информацией и стандартами передовой практики между надзорными органами;

(v) содействовать общим программам обучения и способствовать обмену персоналом между надзорными органами и, при необходимости, с надзорными органами третьих стран или с международными организациями;

(w) содействовать обмену знаниями и документацией относительно законодательства и практики по защите данных с органами по надзору за соблюдением законодательства о защите персональных данных по всему миру;

(x) выдавать заключения относительно норм поведения, разработанных на уровне Союза, согласно Статье 40(9); и

(y) вести общедоступный электронный реестр решений, принятых надзорными органами и судами по вопросам, обработанным в рамках механизма сопоставимости.

2. В случае если Европейской Комиссии требуется консультация Совета, она может указать предельно допустимый срок, с учетом срочности обстоятельства дела.

3. Совет должен передать свои заключения, руководящие указания, рекомендации и стандарты передовой практики Европейской Комиссии и комитету, указанному в Статье 93, а также опубликовать их.

4. В соответствующих случаях Совет должен проконсультировать заинтересованные стороны и дать им возможность в приемлемый срок сделать свои замечания. Без ущерба Статьи 76 Совет должен довести результаты консультации до всеобщего сведения.

Статья 71

Представление отчетов

1. Совет должен составить ежегодный отчет относительно защиты физических лиц при обработке данных в Союзе и, в соответствующих случаях, в третьих странах и международных организациях. Отчет должен быть обнародован и передан Европейскому Парламенту, Совету ЕС и Европейской Комиссии.

2. Ежегодный отчет должен включать в себя проверку практического применения руководящих указаний, рекомендаций и стандартов передовой практики, указанных в пункте (l) Статьи 70(1), а также обязательных для исполнения решений, указанных в Статье 65.

Статья 72

Процедура

1. Если иное не установлено в настоящем Регламенте, Совет должен принимать решения простым большинством голосов своих членов.

2. Совет принимает свои правила процедуры большинством в две трети голосов своих членов и устанавливает свой собственный режим работы.

Статья 73

Президиум

1. Совет из числа своих членов простым большинством голосов должен выбрать председателя и двух заместителей председателя.

2. Срок полномочий председателя и двух его заместителей должен составлять пять лет; допускается их однократное переизбрание.

Статья 74

Задачи президиума

1. Президиум должен выполнять следующие задачи:

(a) созывать совещания Совета и подготавливать их повестку дня;

(b) уведомить о решениях, принятых Советом согласно Статье 65, главный надзорный орган и соответствующие надзорные органы;

(c) гарантировать своевременное выполнение задач Совета, в частности, в отношении механизма сопоставимости согласно Статье 63.

2. Совет должен установить распределение задач между председателем и двумя его заместителями в правилах процедуры.

Статья 75

Секретариат

1. Совет должен располагать секретариатом, который обеспечивается Европейским инспектором по защите персональных данных.

2. Секретариат должен выполнять задачи только на основании указаний Президиума Совета.

3. Персонал Европейского инспектора по защите персональных данных, который участвует в осуществлении задач, возложенных на Совет настоящим Регламентом, подпадает под действие других обязанностей по представлению отчетов в качестве персонала, участвующего в выполнении задач, возложенных на Европейского инспектора по защите персональных данных.

4. В соответствующих случаях Совет и Европейский инспектор по защите персональных данных должны составить и опубликовать Протокол о взаимопонимании, имплементирующий настоящую Статью, определяющий условия их сотрудничества и применимый к персоналу Европейского инспектора по защите персональных данных, участвующему в осуществлении задач, возложенных на Совет настоящим Регламентом.

5. Секретариат должен предоставить Совету аналитическую, административную и логистическую поддержку.

6. Секретариат несет ответственность, в частности:

(a) за повседневную деятельность Совета;

(b) за общение между членами Совета, его Президиумом и Европейской Комиссией;

(c) за общение с другими институтами и общественностью;

(d) за использование электронных средств для внутренней и внешней связи;

(e) за перевод существенной информации;

(f) за подготовку и анализ результатов заседаний Совета;

(g) за подготовку, составление и публикацию заключений, решений об урегулировании спорных вопросов между надзорными органами и других документов, принятых Советом.

Статья 76

Конфиденциальность

1. Обсуждения Совета согласно его правилам процедуры должны носить конфиденциальный характер, если Совет сочтет это необходимым.

2. Доступ к документам, представленным на рассмотрение членам Совета, экспертам и представителям третьих сторон, должен регулироваться Регламентом (ЕС) 1049/2001 Европейского Парламента и Совета ЕС <*>.

<*> Регламент (ЕС) 1049/2001 Европейского Парламента и Совета ЕС от 30 мая 2001 г. о доступе общественности к документам Европейского Парламента, Совета ЕС и Европейской Комиссии (ОЖ N L 145, 31.05.2001, стр. 43).

ГЛАВА VIII. ПРАВОВЫЕ СРЕДСТВА ЗАЩИТЫ, ОТВЕТСТВЕННОСТЬ И САНКЦИИ

Статья 77

Право на подачу жалобы в надзорный орган

1. Без ущерба любому другому административному или судебному средству защиты каждый субъект данных должен обладать правом подачи жалобы в надзорный орган, в частности, в государстве-члене ЕС места его проживания, места работы или места предполагаемого нарушения, если субъект данных считает, что обработка относящихся к нему персональных данных нарушает настоящий Регламент.

2. Надзорный орган, в который была подана жалоба, должен проинформировать заявителя о ходе и результатах рассмотрения жалобы, в том числе о возможности судебной защиты согласно Статье 78.

Статья 78

Право на эффективное средство судебной защиты в отношении надзорного органа

1. Без ущерба любым другим административным или несудебным средствам защиты каждое физическое или юридическое лицо должно иметь право на эффективное средство судебной защиты в отношении касающегося его юридически обязательного решения надзорного органа.

2. Без ущерба любым другим административным или несудебным средствам защиты каждый субъект данных имеет право на эффективное средство судебной защиты, если надзорный орган, компетентный согласно Статьям 55 и 56, не рассматривает жалобу или не информирует субъекта данных в течение трех месяцев о ходе или результатах рассмотрения жалобы, поданной согласно Статье 77.

3. Производство в отношении надзорного органа должно быть передано в суд государства-члена ЕС, в котором учрежден надзорный орган.

4. Если производство инициировано в отношении решения надзорного органа, которому предшествовало заключение или решение Совета в рамках механизма сопоставимости, надзорный орган должен направить указанное заключение или решение в суд.

Статья 79

Право на эффективное средство судебной защиты в отношении контролера или обрабатывающего данные лица

1. Без ущерба любым другим применимым административным или несудебным средствам защиты, в том числе праву на подачу жалобы в надзорный орган согласно Статье 77, каждый субъект данных должен иметь право на эффективное средство судебной защиты, если он считает, что его права согласно настоящему Регламенту были нарушены в результате обработки его персональных данных с нарушением требований настоящего Регламента.

2. Производство в отношении контролера или обрабатывающего данные лица должно быть передано в суд государства-члена ЕС, в котором находится учреждение контролера или обрабатывающего данные лица. Другая возможность предусматривает, что указанное производство может быть передано в суд государства-члена ЕС, в котором постоянно проживает субъект данных, за исключением случаев, когда контролер или обрабатывающее данные лицо является органом государственной власти государства-члена ЕС, действующим при осуществлении общественных полномочий.

Статья 80

Представительство субъектов данных

1. Субъект данных вправе передать некоммерческому органу, организации или объединению, которые были основаны в соответствии с законодательством государства-члена ЕС, имеют уставные задачи в сфере общественного интереса, а также осуществляют деятельность в области защиты прав и свобод субъектов данных в отношении защиты их персональных данных, право подавать жалобу от его имени, осуществлять права, указанные в Статьях 77, 78 и 79, от его имени и осуществлять право на получение компенсации согласно Статье 82 от его имени в случаях, предусмотренных законодательством государства-члена ЕС.

2. Государства-члены ЕС могут предусмотреть, что любой орган, организация или объединение, указанные в параграфе 1 настоящей Статьи, независимо от поручения субъекта данных, имеет право подавать в указанном государстве-члене ЕС жалобу в надзорный орган, компетентный в соответствии со Статьей 77, и осуществлять права, указанные в Статьях 78 и 79, если он считает, что права субъектов данных согласно настоящему Регламенту были нарушены в результате обработки данных.

Статья 81

Приостановление производства по делу

1. В случае если суд соответствующей инстанции государства-члена ЕС обладает информацией относительно производства, касающегося того же самого предмета в отношении обработки тем же самым контролером или обрабатывающим данные лицом и находящегося на рассмотрении в суде другого государства-члена ЕС, он должен связаться с указанным судом в другом государстве-члене ЕС, для того чтобы подтвердить наличие указанного производства.

2. В случае, если производство, касающееся того же самого предмета в отношении обработки тем же самым контролером или обрабатывающим данные лицом находится на рассмотрении в суде другого государства-члена ЕС, любой суд соответствующей инстанции, рассматривающий дело позже, может приостановить его производство.

3. В случае если дело находится в производстве суда первой инстанции, любой суд, рассматривающий дело позже, может также по заявлению одной из сторон отказаться от юрисдикции, если суд, рассматривающий дело первым, уполномочен рассматривать указанные дела и его законодательство разрешает объединение исков.

Статья 82

Право на компенсацию и ответственность

1. Любое лицо, которое понесло материальный или нематериальный ущерб в результате нарушения положений настоящего Регламента, должно иметь право на получение компенсации от контролера или обрабатывающего данные лица за понесенный ущерб.

2. Любой контролер, участвующий в обработке, несет ответственность за ущерб, причиненный не соответствующей настоящему Регламенту обработкой. Обрабатывающее данные лицо несет ответственность за ущерб, причиненный обработкой, только если она не соответствовала обязательствам обрабатывающего данные лица согласно настоящему Регламенту или если он действовал, выходя за рамки законных инструкций контролера, или вопреки им.

3. Контролер или обрабатывающее данные лицо освобождается от ответственности согласно параграфу 2, если он докажет, что он никоим образом не несет ответственность за событие, которое явилось причиной причинения ущерба.

4. Если более одного контролера или обрабатывающего данные лица, или и контролер и обрабатывающее данные лицо участвуют в одной и той же обработке данных и если они согласно параграфам 2 и 3 несут ответственность за любой ущерб, причиненный обработкой, каждый контролер или каждое обрабатывающее данные лицо несет ответственность за весь ущерб, для того чтобы гарантировать эффективную компенсацию субъекту данных.

5. Если контролер или обрабатывающее данные лицо полностью компенсировало в соответствии с параграфом 4 причиненный ущерб, указанный контролер или обрабатывающее данные лицо вправе требовать от других контролеров или обрабатывающих данные лиц, участвовавших в той же самой обработке, возврата части компенсации, соответствующей их части ответственности за ущерб в соответствии с условиями параграфа 2.

6. Судебное производство в отношении осуществления права на получение компенсации должно быть передано в суд, компетентный согласно законодательству государства-члена ЕС, указанному в Статье 79(2).

Статья 83

Общие условия для наложения административных штрафов

1. Каждый надзорный орган должен гарантировать, что наложение административных штрафов согласно настоящей Статье в отношении нарушений положений настоящего Регламента, указанных в параграфах 4, 5 и 6, в каждом отдельном случае должно быть эффективным, пропорциональным и должно оказывать сдерживающее воздействие.

2. В зависимости от обстоятельств каждого отдельного случая административные штрафы должны налагаться в дополнение к мерам или вместо мер, указанных в пунктах (a) - (h) и (j) Статьи 58(2). При решении вопроса относительно наложения административного штрафа и о его размере в каждом отдельном случае необходимо учитывать следующее:

(a) характер, тяжесть и продолжительность нарушения, принимая во внимание характер, объем и цели обработки, а также количество субъектов данных, интересы которых были затронуты указанной обработкой, и размер причиненного им ущерба;

(b) преднамеренный или неосторожный характер нарушения;

(c) любые меры, принятые контролером или обрабатывающим данные лицом, для смягчения ущерба, причиненного субъектам данных;

(d) степень ответственности контролера или обрабатывающего данные лица, принимая во внимание технические и организационные меры, имплементированные согласно Статьям 25 и 32;

(e) любые существенные нарушения, ранее совершенные контролером или обрабатывающим данные лицом;

(f) степень сотрудничества с надзорным органом для устранения нарушения и смягчения возможных негативных последствий;

(g) категории персональных данных, затронутых нарушением;

(h) способ, посредством которого надзорному органу стало известно о нарушении, в частности, уведомил ли контролер или обрабатывающее данные лицо о нарушении, и если да, то в какой степени;

(i) в случае если ранее были предписаны указанные в Статье 58(2) меры в отношении контролера или обрабатывающего данные лица относительно того же самого предмета рассмотрения, соблюдение указанных мер;

(j) соблюдение утвержденных норм поведения согласно Статье 40 или утвержденных сертификационных механизмов согласно Статье 42; и

(k) любые другие отягчающие или смягчающие обстоятельства в деле, например, полученную материальную выгоду или предотвращенные убытки, прямо или косвенно возникшие в результате нарушения.

3. Если контролер или обрабатывающее данные лицо нарушают положения настоящего Регламента намеренно или по неосторожности в рамках одного и того же процесса обработки или в рамках взаимосвязанных процессов обработки, общий размер административного штрафа не должен превышать размер, установленный для самого тяжкого нарушения.

4. За нарушения следующих положений в соответствии с параграфом 2 должны налагаться административные штрафы в размере не более 10 000 000 Евро или в случае предприятия, в размере не более 2% от общего годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше:

(a) обязанностей контролера и обрабатывающего данные лица согласно Статьям 8, 11, 25 - 39 и 42 и 43;

(b) обязанностей сертификационного органа согласно Статьям 42 и 43;

(c) обязанностей контролирующего органа согласно Статье 41(4).

5. За нарушения следующих положений в соответствии с параграфом 2 должны налагаться административные штрафы в размере не более 20 000 000 Евро или в случае предприятия, в размере не более 4% от общего годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше:

(a) основных принципов обработки, в том числе условий для согласия в соответствии со Статьями 5, 6, 7 и 9;

(b) прав субъектов данных согласно Статьям 12 - 22;

(c) передачи персональных данных получателю в третьей стране или международной организации согласно Статьям 44 - 49;

(d) любых обязанностей согласно законодательству государства-члена ЕС, принятому в рамках Главы IX;

(e) несоблюдения требования или временного или окончательного ограничения на обработку или приостановление передачи данных надзорным органом согласно Статье 58(2) или отказ в предоставлении доступа в нарушение Статьи 58(1).

6. За невыполнение требования надзорного органа согласно Статье 58(2) должны в соответствии с параграфом 2 налагаться административные штрафы в размере не более 20 000 000 Евро или, в случае предприятия, в размере не более 4% от общего годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

7. Без ущерба корректирующим полномочиям надзорных органов согласно Статье 58(2) каждое государство-член ЕС может установить правила относительно того, могут ли и в какой степени административные штрафы налагаться на органы государственной власти и другие государственные органы, учрежденные в указанном государстве-члене ЕС.

8. На осуществление надзорным органом своих полномочий согласно настоящей Статье распространяются соответствующие процессуальные гарантии в соответствии с законодательством Союза и государства-члена ЕС, включая эффективные средства судебной защиты и надлежащую правовую процедуру.

9. В случае если правовая система государства-члена ЕС не предусматривает административные штрафы, настоящая Статья может применяться таким образом, что наложение штрафа инициируется компетентным надзорным органом, а штраф накладывается компетентными национальными судами, при этом гарантируется, что указанные средства правовой защиты являются эффективными и имеют воздействие, эквивалентное воздействию административных штрафов, налагаемых надзорными органами. В любом случае, налагаемые штрафы должны быть эффективными, пропорциональными и должны оказывать сдерживающее воздействие. Указанные государства-члены ЕС должны уведомить Европейскую Комиссию о положениях своего законодательства, которые они принимают согласно настоящему параграфу, до 25 мая 2018 г. и незамедлительно о любых последующих законодательных актах, о поправках или любых изменениях, затрагивающих указанные положения.

Статья 84

Санкции

1. Государства-члены ЕС могут установить правила об иных санкциях, применимых к нарушениям настоящего Регламента, в частности, к нарушениям, которые не подпадают под административные штрафы согласно Статье 83, и принять все меры, необходимые для обеспечения их имплементации. Указанные санкции должны быть эффективными, пропорциональными и должны оказывать сдерживающее воздействие.

2. Каждое государство-член ЕС должно уведомить Европейскую Комиссию о положениях своего законодательства, которые оно принимает согласно параграфу 1, до 25 мая 2018 г. и незамедлительно о любых изменениях, затрагивающих указанные положения.

ГЛАВА IX. ПОЛОЖЕНИЯ В ОТНОШЕНИИ ОСОБЫХ СИТУАЦИЙ ОБРАБОТКИ

Статья 85

Обработка и свобода выражения мнений и информации

1. Государства-члены ЕС законодательно должны согласовать право на защиту персональных данных в соответствии с настоящим Регламентом с правом на свободу выражения мнений и информации, включая обработку в журналистских целях, а также в научных, художественных и литературных целях.

2. Для обработки, осуществляемой в журналистских, научных, художественных и литературных целях, государства-члены ЕС должны предусмотреть исключения и частичные отступления от Главы II (принципы), Главы III (права субъекта данных), Главы IV (контролер и обрабатывающее данные лицо), Главы V (передача персональных данных третьим странам и международным организациям), Главы VI (независимые надзорные органы), Главы VII (сотрудничество и сопоставимость) и Главы IX (особые ситуации обработки данных), если они необходимы для того, чтобы согласовать право на защиту персональных данных со свободой выражения мнений и информации.

3. Каждое государство-член ЕС должно уведомить Европейскую Комиссию о положениях своего законодательства, которые оно приняло согласно параграфу 2, и незамедлительно о любых последующих законодательных актах, о поправках или любых изменениях, затрагивающих указанные положения.

Статья 86

Обработка и доступ общественности к официальным документам

Персональные данные в официальных документах, находящихся в органах государственной власти, или правительственных учреждениях, или частных организациях для осуществления задачи в рамках общественного интереса, могут быть раскрыты органом или учреждением в соответствии с законодательством Союза или государства-члена ЕС, под действие которого подпадает орган государственной власти или учреждение, для того чтобы согласовать доступ общественности к официальным документам с правом на защиту персональных данных согласно настоящему Регламенту.

Статья 87

Обработка национального идентификационного номера

Государства-члены ЕС могут определить особые условия для обработки национального идентификационного номера или любого другого идентификатора общего назначения. В указанном случае национальный идентификационный номер или любой другой идентификатор общего назначения должен использоваться только при обеспечении соответствующих гарантий для прав и свобод субъекта данных согласно настоящему Регламенту.

Статья 88

Обработка в контексте занятости

1. Государства-члены ЕС могут законодательно или посредством коллективных договоров предусмотреть более специфичные правила для того, чтобы гарантировать защиту прав и свобод в отношении обработки персональных данных работников при выполнении должностных обязанностей, в частности в целях приема на работу, выполнения трудового договора, включая исполнение обязательств, установленных в соответствии с законодательством или коллективным договором, в целях управления, планирования и организации работы, равноправия и многообразия на рабочем месте, охраны труда и

производственной безопасности, защиты собственности работодателя или клиента, а также в целях осуществления связанных с занятостью индивидуальных или коллективных прав и гарантий и в целях прекращения трудовых отношений.

2. Указанные правила должны включать в себя приемлемые и конкретные меры, для того чтобы гарантировать человеческое достоинство, законные интересы и основные права субъекта данных, особенно в отношении прозрачности обработки, передачи персональных данных в рамках группы предприятий или группы компаний, задействованных в совместной экономической деятельности, а также в отношении мониторинга систем на рабочем месте.

3. Каждое государство-член ЕС должно уведомить Европейскую Комиссию об указанных положениях своего законодательства, которые оно приняло согласно параграфу 1, до 25 мая 2018 г. и незамедлительно о любых последующих изменениях, затрагивающих указанные положения.

Статья 89

Гарантии и частичные отступления в отношении обработки
в целях архивирования в интересах общества, в целях научного
или исторического исследования или в статистических целях

1. На обработку в целях архивирования в интересах общества, в научных целях, в целях исторического исследования или в статистических целях должны распространяться соответствующие гарантии в отношении прав и свобод субъекта данных согласно настоящему Регламенту. Указанные гарантии должны обеспечивать наличие технических и организационных мер, в частности, для соблюдения принципа минимизации данных. Указанные меры могут включать в себя псевдонимизацию при условии, что указанные цели могут быть достигнуты таким образом. Если указанные цели могут быть достигнуты при дальнейшей обработке, которая не допускает или больше не допускает идентификацию субъектов данных, указанные цели должны достигаться таким образом.

2. В случае если персональные данные обрабатываются в научных целях, в целях исторического исследования или в статистических целях, в законодательстве Союза или государства-члена ЕС могут быть предусмотрены частичные отступления от прав, указанных в Статьях 15, 16, 18 и 21, в соответствии с условиями и гарантиями, указанными в параграфе 1 настоящей Статьи, постольку, поскольку указанные права могут сделать невозможным или серьезно сказаться на достижении особых целей, и указанные частичные отступления необходимы для достижения указанных целей.

3. В случае если персональные данные обрабатываются в целях архивирования в интересах общества, в законодательстве Союза или государства-члена ЕС могут быть предусмотрены частичные отступления от прав, указанных в Статьях 15, 16, 18, 19, 20 и 21, в соответствии с условиями и гарантиями, указанными в параграфе 1 настоящей Статьи, постольку, поскольку указанные права могут сделать невозможным или серьезно сказаться на достижении особых целей, и указанные частичные отступления необходимы для достижения указанных целей.

4. В случае если обработка, указанная в параграфах 2 и 3, служит в одно и то же время для другой цели, частичные отступления должны применяться только в отношении обработки для целей, предусмотренных в указанных параграфах.

Статья 90

Обязанность неразглашения тайны

1. Государства-члены ЕС могут принять особые правила для утверждения полномочий надзорных органов в значении пунктов (e) и (f) Статьи 58(1) в отношении контролеров и обрабатывающих данные лиц, которые согласно законодательству Союза или государства-члена ЕС или согласно правилам, установленным национальными компетентными органами, подлежат обязанности соблюдать профессиональную тайну или иным эквивалентным обязанностям неразглашения тайны, если это необходимо и пропорционально для согласования права на защиту персональных данных с обязанностью

неразглашения тайны. Указанные положения должны применяться только в отношении персональных данных, которые контролер или обрабатывающее данные лицо получило в результате деятельности, которая подпадает под указанную обязанность неразглашения тайны.

2. Каждое государство-член ЕС должно уведомить Европейскую Комиссию о положениях, принятых согласно параграфу 1, до 25 мая 2018 г. и незамедлительно о любых последующих изменениях, затрагивающих указанные положения.

Статья 91

Существующие положения о защите данных
церквей и религиозных организаций

1. В случае если церкви и религиозные организации или общины в государстве-члене ЕС в момент вступления в силу настоящего Регламента применяют исчерпывающие правила в отношении защиты физических лиц при обработке их данных, указанные правила могут применяться в дальнейшем, при условии их соответствия настоящему Регламенту.

2. Церкви и религиозные организации, которые применяют исчерпывающие правила в соответствии с параграфом 1 настоящей Статьи, подлежат надзору со стороны независимого надзорного органа, который может иметь специфический характер, при условии, что он соблюдает условия, установленные в Главе VI настоящего Регламента.

ГЛАВА X. ДЕЛЕГИРОВАННЫЕ АКТЫ И ИМПЛЕМЕНТАЦИОННЫЕ АКТЫ

Статья 92

Осуществление делегирования

1. Полномочие на принятие делегированных актов предоставляется Европейской Комиссии согласно условиям, установленным в настоящей Статье.

2. Делегирование полномочий, указанных в Статье 12(8) и в Статье 43(8), предоставляется Европейской Комиссии на неопределенный срок, начиная с 24 мая 2016 г.

3. Делегирование полномочий, указанных в Статье 12(8) и в Статье 43(8), может быть отменено в любое время Европейским Парламентом или Советом ЕС. Решение об отмене прекращает делегирование полномочий, определенных в указанном решении. Оно вступает в силу на следующий день после публикации решения в Официальном Журнале Европейского Союза или в более поздний срок, определенный в решении. Оно не влияет на действительность делегированных актов, которые уже вступили в силу.

4. Сразу же после принятия делегированного акта Европейская Комиссия должна уведомить об этом Европейский Парламент и Совет ЕС.

5. Делегированный акт, принятый согласно Статье 12(8) и Статье 43(8), должен вступать в силу только в случае, если ни Европейский Парламент, ни Совет ЕС не представили возражения в течение трех месяцев с момента уведомления об указанном акте или если до истечения указанного срока Европейский Парламент и Совет ЕС проинформировали Европейскую Комиссию о том, что они не будут представлять возражения. Указанный срок должен быть продлен на три месяца по инициативе Европейского Парламента или Совета ЕС.

Статья 93

Процедура Комитета

1. Европейской Комиссии должен оказывать содействие Комитет. Указанный Комитет должен

являться комитетом в значении Регламента (ЕС) 182/2011.

2. В случае если делается ссылка на настоящий параграф, применяется Статья 5 Регламента (ЕС) 182/2011.

3. В случае если делается ссылка на настоящий параграф, применяется Статья 8 Регламента (ЕС) 182/2011 совместно со Статьей 5 указанного Регламента.

ГЛАВА XI. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 94

Отмена Директивы 95/46/ЕС

1. Директива 95/46/ЕС отменяется с 25 мая 2018 г.

2. Ссылки на отмененную Директиву должны рассматриваться как ссылки на настоящий Регламент. Ссылки на Рабочую группу по защите физических лиц при обработке персональных данных, учрежденную Статьей 29 Директивы 95/46/ЕС, должны рассматриваться как ссылки на Европейский совет по защите данных, учрежденный настоящим Регламентом.

Статья 95

Соотношение с Директивой 2002/58/ЕС

Настоящий Регламент не должен налагать дополнительные обязательства на физических и юридических лиц при обработке в сочетании с положением об общедоступных электронных услугах связи в сетях связи общего пользования в Союзе по вопросам, в отношении которых они подлежат специфическим обязанностям, установленным в Директиве 2002/58/ЕС и преследующим одну и ту же цель.

Статья 96

Соотношение с уже заключенными соглашениями

Международные соглашения, касающиеся передачи персональных данных третьим странам или международным организациям, которые государства-члены ЕС заключили до 24 мая 2016 г. и которые соответствуют законодательству Союза, применявшемуся до указанной даты, должны сохранять свою силу до тех пор, пока они не будут изменены, заменены или отменены.

Статья 97

Отчеты Европейской Комиссии

1. До 25 мая 2020 г. и каждые четыре года впоследствии Европейская Комиссия должна направлять отчет об оценке и пересмотре настоящего Регламента в Европейский Парламент и Совет ЕС. Отчет должен быть опубликован.

2. В рамках оценки и пересмотра согласно параграфу 1 Европейская Комиссия должна проверить, в частности, применение и действие:

(a) Главы V о передаче персональных данных третьим странам или международным организациям, в особенности, с учетом решений, принятых согласно Статье 45(3) настоящего Регламента, и решений, принятых на основе Статьи 25(6) Решения 95/46/ЕС;

(b) Главы VII о сотрудничестве и сопоставимости.

3. Для цели параграфа 1 Европейская Комиссия может запрашивать информацию у государств-членов ЕС и надзорных органов.

4. При выполнении оценки и пересмотра согласно параграфам 1 и 2 Европейская Комиссия должна учесть позиции и выводы Европейского Парламента, Совета ЕС и других соответствующих органов или источников.

5. Европейская Комиссия, при необходимости, должна внести соответствующие предложения по изменению настоящего Регламента, в частности, с учетом развития информационных технологий и в свете прогресса в информационном обществе.

Статья 98

Пересмотр других правовых актов о защите данных

Европейская Комиссия, при необходимости, должна внести законодательные предложения по изменению других правовых актов о защите персональных данных, для того чтобы гарантировать единообразную и последовательную защиту физических лиц при обработке данных. В частности, это касается норм о защите физических лиц при обработке данных институтами, органами, службами и агентствами Союза, а также норм о свободном обращении указанных данных.

Статья 99

Вступление в силу и применение

1. Настоящий Регламент вступает в силу на двадцатый день после своего опубликования в Официальном Журнале Европейского Союза.

2. Он должен применяться с 25 мая 2018 г.

Настоящий Регламент является обязательным в полном объеме и подлежит прямому применению в государствах-членах ЕС.

Совершено в Брюсселе 27 апреля 2016 г.

(Подписи)

REGULATION (EU) No. 2016/679
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
ON THE PROTECTION OF NATURAL PERSONS WITH REGARD
TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT
OF SUCH DATA, AND REPEALING DIRECTIVE 95/46/EC
(GENERAL DATA PROTECTION REGULATION)

(Brussels, 27.IV.2016)

(Text with EEA relevance)

The European Parliament and the Council of the European Union,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee <1>,

---

<1> OJ C 229, 31.7.2012, p. 90.

Having regard to the opinion of the Committee of the Regions <2>,

---

<2> OJ C 391, 18.12.2012, p. 127.

Acting in accordance with the ordinary legislative procedure <3>,

---

<3> Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the "Charter") and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council <4> seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

<4> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology

allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ("sensitive data"). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of

the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC <1>.

<1> Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council <2> applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

<2> Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council <1>. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the

scope of this Regulation.

<1> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council <2>, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

<2> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") (OJ L 178, 17.7.2000, p. 1).

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of

a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of "pseudonymisation" in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council <1> to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

<1> Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of

undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the "Court of Justice") and the European Court of Human Rights.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC <1> a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

<1> Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of

personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping "denial of service" attacks and damage to computer and electronic communication systems.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term "racial origin" in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs

in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, "public health" should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council <1>, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

<1> Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take

additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on

profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(65) A data subject should have the right to have personal data concerning him or her rectified and a "right to be forgotten" where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data

subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes "profiling" that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the "Board") should be able to issue guidance in that context.

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for

regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a

clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a

data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data

subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing

operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities,

and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council <1> as established under this Regulation, to the European Parliament and to the Council.

<1> Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another

processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include

judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This

should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ("one-stop-shop mechanism"), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-a-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency

mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority,

exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of

the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council <1> should not prejudice the application of such specific rules.

<1> Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice.

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council <1> leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

<1> Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

(155) Member State law or collective agreements, including "works agreements", may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on

an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the

relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council <1> should apply.

<1> Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council <2> provides further specifications on statistical confidentiality for European statistics.

<2> Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 <1>.

<1> OJ C 192, 30.6.2012, p. 7.

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council <2>, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

---

<2> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

Have adopted this Regulation:

CHAPTER I. GENERAL PROVISIONS

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) "restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

(4) "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) "filing system" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) "recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) "third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) "genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) "biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) "data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) "main establishment" means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) "representative" means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) "enterprise" means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) "group of undertakings" means a controlling undertaking and its controlled undertakings;

(20) "binding corporate rules" means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) "supervisory authority" means an independent public authority which is established by a Member State pursuant to Article 51;

(22) "supervisory authority concerned" means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) "cross-border processing" means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) "relevant and reasoned objection" means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) "information society service" means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council <1>;

<1> Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(26) "international organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II. PRINCIPLES

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability").

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation
to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process

additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III. RIGHTS OF THE DATA SUBJECT

Section 1

TRANSPARENCY AND MODALITIES

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2

INFORMATION AND ACCESS TO PERSONAL DATA

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and

of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data
have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their

source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3

RECTIFICATION AND ERASURE

Article 16

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17

Right to erasure ("right to be forgotten")

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that

the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING

Article 21

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5

RESTRICTIONS

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV. CONTROLLER AND PROCESSOR

Section 1

GENERAL OBLIGATIONS

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by

default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26

Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis–à–vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27

Representatives of controllers or processors
not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29

Processing under the authority of
the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data

protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Section 2

SECURITY OF PERSONAL DATA

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the

requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

Notification of a personal data breach to
the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the

purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36

Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4

DATA PROTECTION OFFICER

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5

CODES OF CONDUCT AND CERTIFICATION

Article 40

Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as

with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension

complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42

Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43

Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council <1> in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

<1> Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in

accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection
of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI. INDEPENDENT SUPERVISORY AUTHORITIES

Section 1

INDEPENDENT STATUS

Article 51

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ("supervisory authority").

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 52

Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53

General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

- their parliament;

- their government;

- their head of State; or

- an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

(a) the establishment of each supervisory authority;

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Section 2

COMPETENCE, TASKS AND POWERS

Article 55

Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56

Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive

character of the request.

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State

government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59

Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

CHAPTER VII. COOPERATION AND CONSISTENCY

Section 1

COOPERATION

Article 60

Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for

carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61

Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective

cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62

Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory

authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights vis – à – vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2

CONSISTENCY

Article 63

Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64

Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

(b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

(c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);

(d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);

(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

(f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

(a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred

to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66

Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Article 67

Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Section 3

EUROPEAN DATA PROTECTION BOARD

Article 68

European Data Protection Board

1. The European Data Protection Board (the "Board") is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69

Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 70

Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);

(e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

(l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the icons referred to in Article 12(7);

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a

third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71

Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72

Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Article 73

Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 74

Tasks of the Chair

1. The Chair shall have the following tasks:

(a) to convene the meetings of the Board and prepare its agenda;

(b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;

(c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75

Secretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

5. The secretariat shall provide analytical, administrative and logistical support to the Board.

6. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the Board;

(b) communication between the members of the Board, its Chair and the Commission;

(c) communication with other institutions and the public;

(d) the use of electronic means for the internal and external communication;

(e) the translation of relevant information;

(f) the preparation and follow-up of the meetings of the Board;

(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76

Confidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council <1>.

<1> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

CHAPTER VIII. REMEDIES, LIABILITY AND PENALTIES

Article 77

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78

Right to an effective judicial remedy against
a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79

Right to an effective judicial remedy against
a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a

result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81

Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective

compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

CHAPTER IX. PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

Article 85

Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86

Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87

Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88

Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90

Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X. DELEGATED ACTS AND IMPLEMENTING ACTS

Article 92

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI. FINAL PROVISIONS

Article 94

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95

Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication

networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 96

Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Article 97

Commission reports

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

(b) Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Article 98

Review of other Union legal acts on data protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 April 2016.