

GDPR: применение и основные требования

Алексей Мунтян
Генеральный директор Privacy Advocates

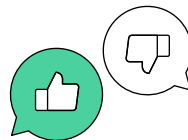


Проверка связи





Если у вас нет звука:

- убедитесь, что на вашем устройстве и на колонках включён звук
- обновите страницу вебинара (или закройте страницу и заново присоединитесь к вебинару)
- откройте вебинар в другом браузере
- перезагрузите компьютер (ноутбук) и заново попытайтесь зайти



Поставьте в чат:

-  если меня видно и слышно
-  если нет

Алексей Мунтян

О спикере:

- основатель и CEO в компании Privacy Advocates
- соучредитель «Сообщества профессионалов в области приватности» — RPPA.ru
- внешний data protection officer в нескольких транснациональных холдингах
- сопредседатель privacy & legal innovation кластера РАЭК
- участник центров компетенций «Информационная безопасность» и «Нормативное регулирование» при АНО «Цифровая экономика»
- участник комитета по безопасности данных партнёров и пользователей при Консультативном совете по развитию экосистемы Яндекса



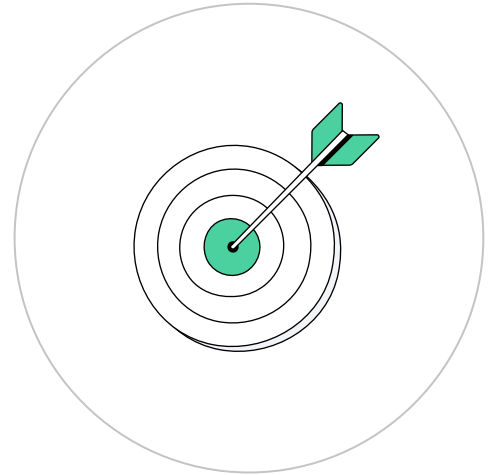
Правила участия

- 1 Приготовьте блокнот и ручку, чтобы записывать важные мысли и идеи
- 2 Продолжительность вебинара — 80 минут
- 3 Вы можете писать свои вопросы в чате
- 4 Запись вебинара будет доступна



Цели занятия

- Узнаем, зачем нужен GDPR и в чём заключается его специфика
- Поймём, как определять, попадает ли компания, конкретный сервис или процесс под регулирование GDPR
- Разберём основные требования и особенности GDPR



План занятия

- 1 Понятие и специфика GDPR
- 2 Применимость GDPR
- 3 Соответствие GDPR

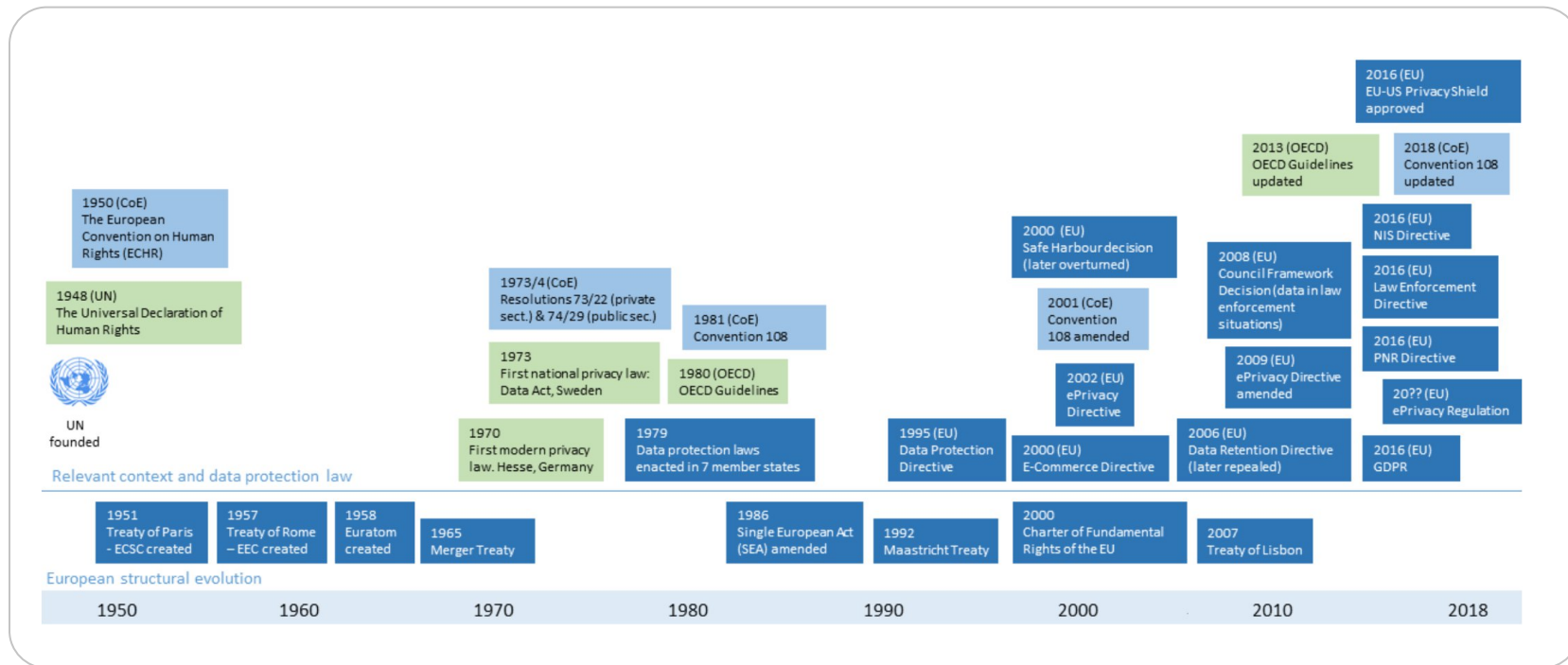


Понятие и специфика GDPR



1

Правовая традиция GDPR

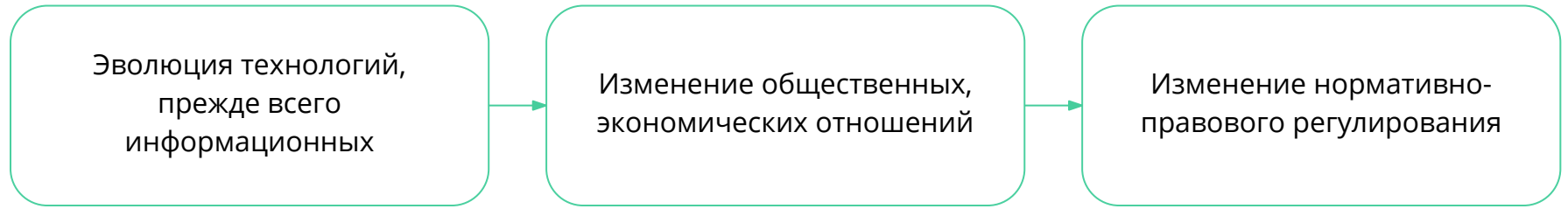


Правовая традиция GDPR.

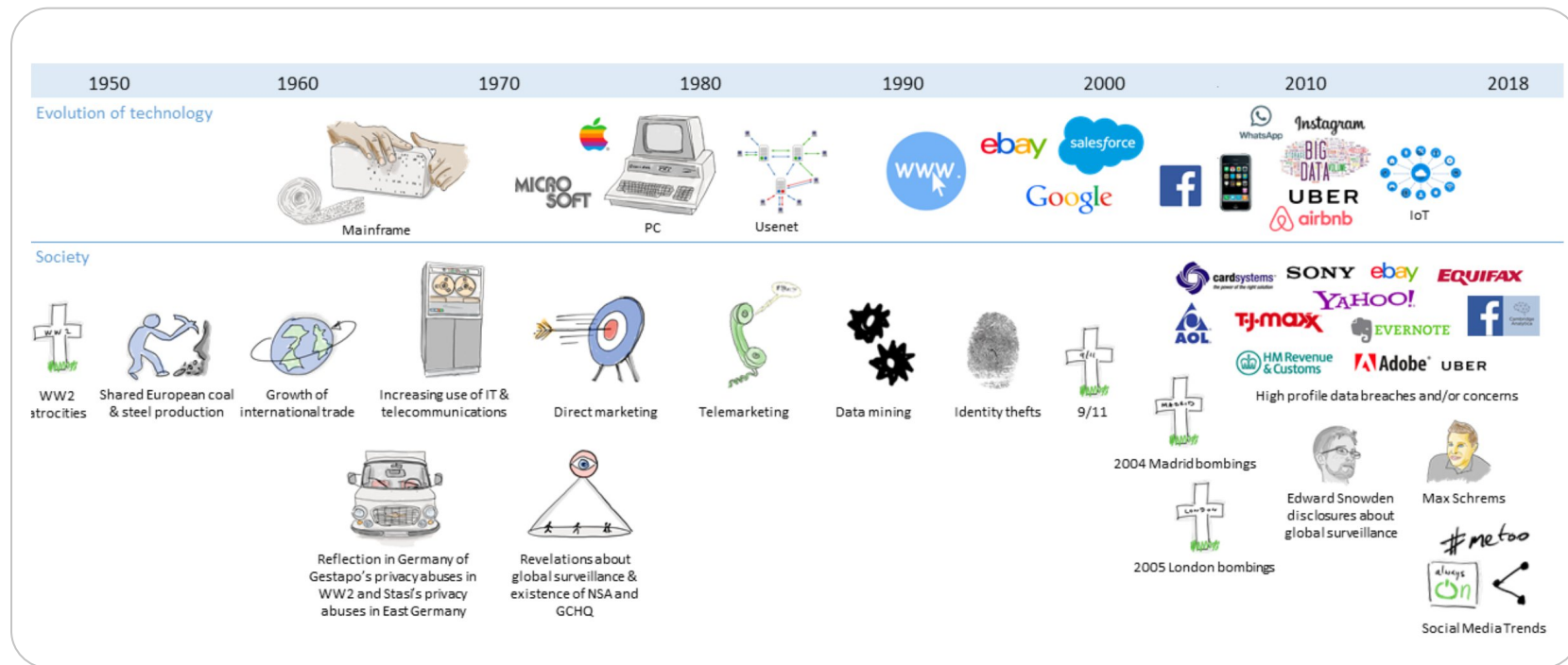
Ключевые моменты

- GDPR — квинтэссенция пятидесятилетнего опыта европейской традиции регулирования вопросов, связанных с обработкой и защитой персональных данных
- Конвенция Совета Европы 108 о защите персональных данных (1981 г.) — первый международный правовой акт, посвящённый вопросам защиты персональных данных
- Директива ЕС о защите данных 1995 года — документ-предшественник GDPR
- GDPR приняли в 2018 г. как новый регламент, который учитывает современные технологии и проблемы, связанные с защитой данных

Факторы, определившие появление GDPR



Факторы, определившие появление GDPR



Чем регулируется обработка и защита данных



General data protection regulation (GDPR)

Общий регламент о защите персональных данных

Регламент Европейского союза, который определяет порядок обработки персональных данных организациями



Что важно знать о GDPR

GDPR вступил в силу
25 мая 2018 года



Основная задача стандарта —
вернуть управление данными
людям и повысить
прозрачность обработки



Все страны стали
равняться на GDPR при
обновлении национального
законодательства



За 5,5 лет (май 2018 – октябрь
2023 г.) вынесли 1 800+
штрафов на общую сумму
в 4,5 млрд €

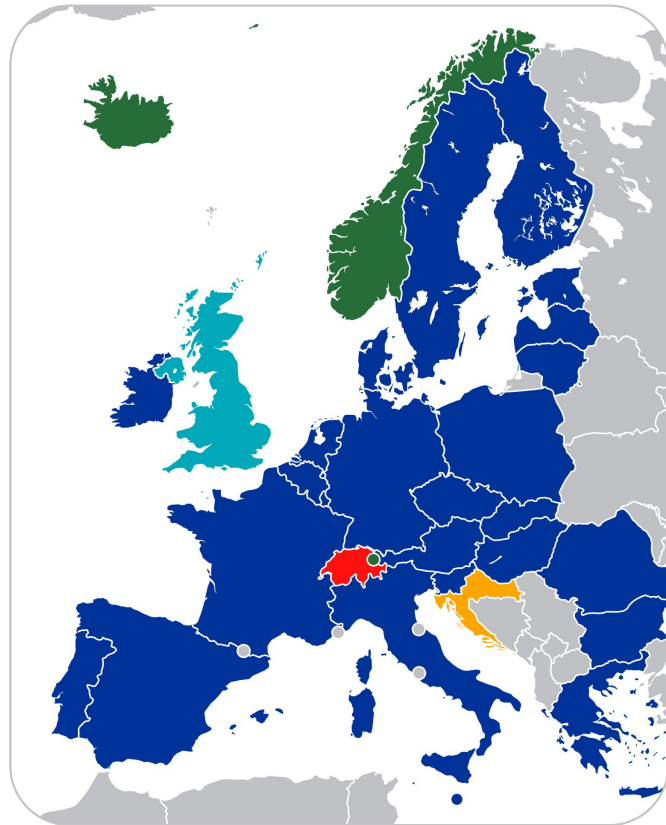


Международный бизнес берёт
GDPR за основу
при построении privacy-
программ



Особенности

GDPR распространяется на страны
Европейского союза (ЕС) и Европейской
экономической зоны (ЕЭЗ)



Законодательство ЕС, ЕЭЗ и требования GDPR

Страны-члены ЕС и ЕЭЗ принимают и изменяют свои законы, чтобы они соответствовали требованиям GDPR.

Локальные законы стран сами определяют возраст совершеннолетия, общественные интересы и законодательные требования к процессорам.

Общий надзор осуществляет Европейский совет по защите данных (European data protection board), а в отдельных странах местные надзорные органы

Специфика ЕС. GDPR Tracker

Дети онлайн (Children online) —————>

Назначение уполномоченного по защите данных
(Designation a data protection officer) —————>

Персональные данные умерших лиц
(Personal data of deceased persons) —————>

Трудоустройство (Employment) —————>

Генетические, биометрические данные или данные о здоровье
(Genetic, biometric of health data) —————>

Национальные идентификационные номера / любой другой идентификатор общего применения
(National identification numbers / any other identifier of general application)

Специфика ЕС. GDPR Tracker

Любые другие области на обсуждении (Any other areas under discussion) —————>

Подход к реализации (Approach to implementation) —————>

Персональные данные и свобода выражения мнений
(Personal data and freedom of expression) —————>

Срок реализации (Timescale for implementation) —————>

Штрафы (Penalties) —————>

Профессиональная тайна (Professional secrecy) —————>

Научные, исторические или статистические цели (Scientific , historical or statistical purposes) —————>

Особые правила для особых категорий данных (Special rules for special categories of data) —————>

Стадия законодательного прогресса (GDPR Tracker — stage of legislative progress)

Принципы обработки персональных данных

Конвенция Совета Европы	GDPR	152-ФЗ
Законность	Законность, справедливость, прозрачность	Законность, справедливость
Справедливость, прозрачность		
Ограниченность целей	Ограниченность целей	Ограниченность целей
Адекватность и избыточность по отношению к целям	Минимизация данных	Неизбыточность по отношению к целям
Точность и актуальность	Точность и актуальность	Точность, актуальность, достаточность
Ограниченность времени хранения	Ограниченность времени хранения	Ограниченность времени хранения
-	Подотчётность	-
-	Безопасность обработки	-

Принципы обработки персональных данных



Прозрачность обработки

App privacy labels

App privacy details

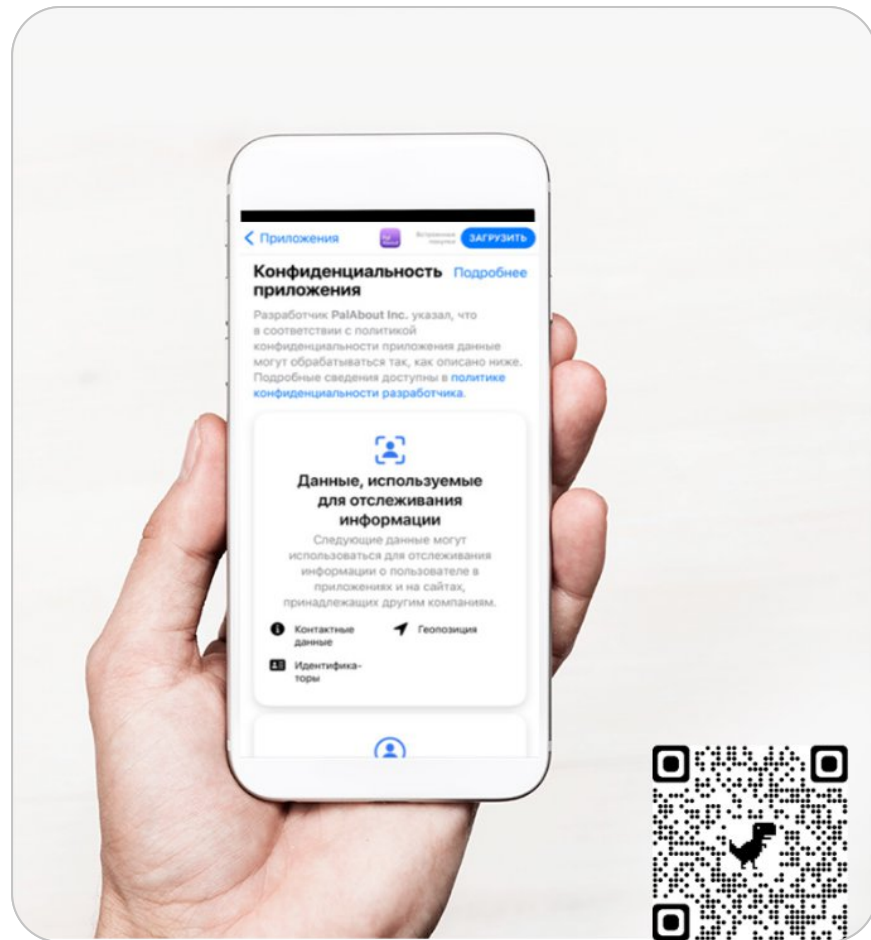
Describing Data Usage

Privacy information

«Этикетка с составом» для приложения, связанная со сбором данных: ярлык показывает, какие данные собираются приложением и для какой цели

Eric Benjamin Seufert

[Источник](#)



Регламент GDPR.

Права субъектов данных

- Право на защиту данных (Rec. 1, Art. 1)
- Право распоряжаться своими данными (Rec. 7)
- Право в любое время отозвать согласие на обработку данных (Art. 7)
- Право на информацию и транспарентность в отношении обработки данных (Art. 12–14, 19, 23)
- Право на доступ к данным (Art. 15)
- Право на внесение исправлений в данные (Art. 16)
- Право на удаление данных (Art. 17)
- Право на ограничение обработки данных (Art. 18)
- Право на переносимость данных (Art. 20)
- Право на возражение против обработки данных (Art. 21)

Регламент GDPR.

Права субъектов данных

- Право не подчиняться решению, основанному на автоматизированной обработке данных (Art. 22)
- Право быть уведомленным об утечке данных (Art. 34)
- Право на обращение к data protection officer (Art. 38)
- Право на обращение (подачу жалобы) к надзорному органу (Art. 77)
- Право на эффективные средства судебной защиты против надзорного органа (Art. 78)
- Право на эффективные средства судебной защиты в отношении контролёра или обработчика (Art. 79)
- Право на представительство, т. е. передачу полномочий (Art. 79)
- Право на компенсацию материального или нематериального ущерба (Art. 82)

Права субъектов данных

Права субъектов ПД

Информирование и доступ к ПД — позволяет получать сведения о цели, источниках, правовых основаниях, участниках, способе и сроках обработки ПД, а также уведомления о передаче ПД третьим лицам и об утечках ПД

Переносимость ПД — позволяет получать копию ПД в формате, дающем возможность повторно использовать копию ПД в других сервисах/компаниях

Возражение против обработки ПД — позволяет ограничивать прямые маркетинговые/рекламные контакты и возражать против решений, основанных на исключительно автоматизированной обработке ПД

Прекращение обработки ПД (право быть забытым) — позволяет прекратить любую обработку ПД, которую нельзя обосновать договором с субъектом ПД или требованием закона

Исправление, блокирование, уничтожение ПД — позволяет требовать уточнения, блокирования или уничтожения неполных, устаревших, неточных, избыточных или незаконно полученных ПД

Стороны взаимоотношений

- 1 Субъект данных и его представитель
 - 2 Контролёр, совместный контролёр
 - 3 Процессор, subprocessor
 - 4 Получатель
 - 5 Представитель контролёра или процессора
- Роли по GDPR практически во всём похожи на зафиксированные в 152-ФЗ
 - По GDPR более внимательно нужно относиться к выбору роли, иначе надзорные органы могут её оспорить

Основания обработки («меню»)

Согласие субъекта



Заключение
и исполнение договора
с субъектом



Защита жизненно
важных интересов
субъекта



Законный интерес
оператора



Исполнение обязан-
ностей в соответствии
с законом



Публичные интересы,
государственные
функции



Вред от обработки

Человек ведёт себя по-разному в зависимости от контекста, в котором находится:
у каждого разные «я» для работы, друзей, родных.

Если данные из разных контекстов объединяются, человек не может больше разделять роли, предназначенные для разных контекстов





Ваши вопросы

Выводы

- GDPR — регламент Европейского союза, определяющий порядок обработки персональных данных организациями
- GDPR устанавливает строгие требования по обработке и защите персональных данных
- GDPR предусматривает значительные штрафы за нарушение его положений
- GDPR распространяется на организации, работающие с данными граждан ЕС, независимо от места их нахождения

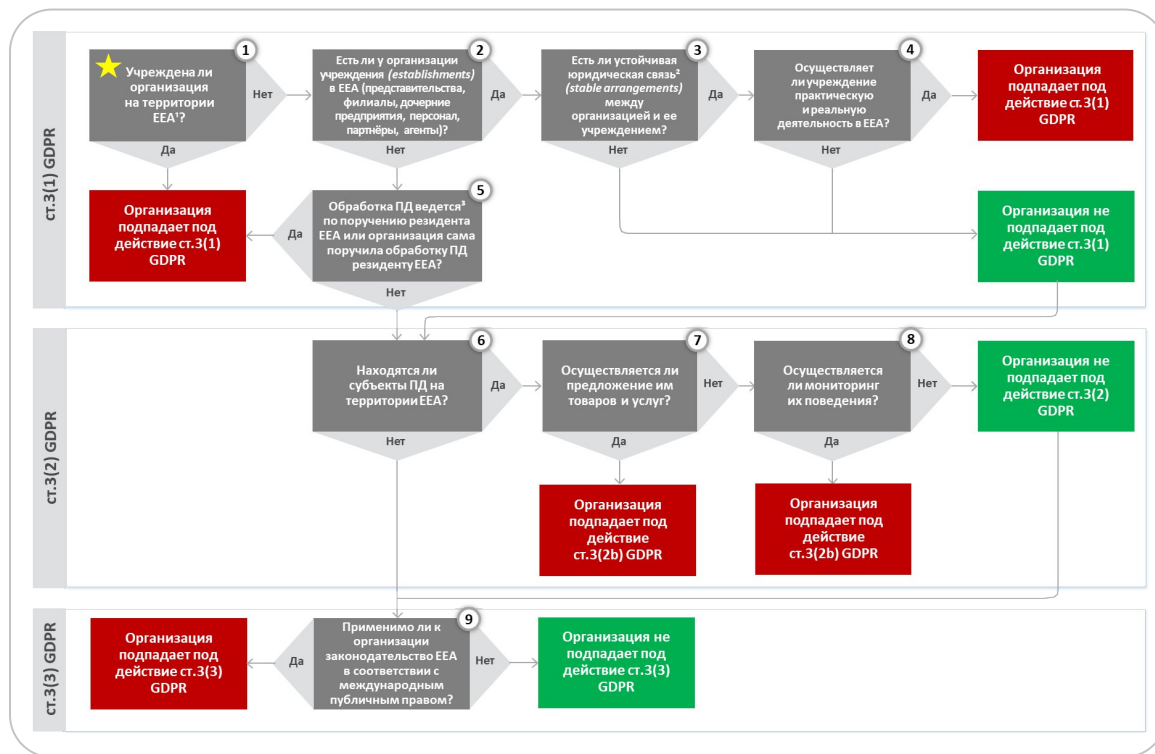


Применимость GDPR



2

Применимость GDPR к процессам обработки ПД



Критерии применимости GDPR

¹ Наличие правоотношений вне зависимости от их формы: соглашения, контракты, участие в уставном капитале и т. д.

² Обработка ПД, выполняемая на основании и для исполнения договора между оператором и обработчиком (controller-to-processor agreement), ведётся в контексте практической и реальной деятельности организации, находящейся в статусе оператора или обработчика на территории ЕС. Применимость GDPR определяется отдельно для каждого факта поручения обработки ПД и **не зависит от места фактического осуществления обработки ПД (на территории ЕС или вне её)**

№	Вопрос	Ответ	GDPR	3/2018 ³	5/2021 ⁴
1	Учреждена ли организация на территории ЕС	Да — GDPR применим Нет — см. вопрос 2	ст. 3 (1) гс. 22	п. 1(a) exp. 1	п. 13, 16, 18 exp. 3–4, 6–7
2	Есть ли у организации учреждения (establishments) в ЕС: представительства, филиалы, дочерние предприятия, персонал, партнёры, агенты	Да — см. вопрос 3 Нет — см. вопрос 5			
3	Есть ли устойчивая юридическая связь ¹ (stable arrangements) между организацией и её учреждением	Да — см. вопрос 4 Нет — см. вопрос 6			
4	Осуществляет ли учреждение практическую и реальную деятельность в ЕС	Да — GDPR применим Нет — см. вопрос 6		п. 1 (b) exp. 2–3	
5	Обработка ПД ведётся ² по поручению резидента ЕС или организация сама поручила обработку ПД резиденту ЕС	Да — GDPR применим Нет — см. вопрос 6		п. 1 (c), (d) exp. 4–7	

Критерии применимости GDPR

№	Вопрос	Ответ	GDPR	3/2018 ³	5/2021 ⁴
6	Находятся ли субъекты ПД на территории ЕС	Да — см. вопрос 7 Нет — см. вопрос 9	ст. 3 (2) rc. 14	п. 2 (a) exp. 8–12	п. 18 exp. 7
7	Осуществляется ли предложение товаров и услуг субъектам ПД на территории ЕС	Да — GDPR применим Нет — см. вопрос 8	ст. 3 (2a) rc. 23	п. 2 (b) exp. 13–16	
8	Осуществляется ли мониторинг поведения субъектов ПД на территории ЕС	Да — GDPR применим Нет — см. вопрос 9	ст. 3 (2b) rc. 24	п. 2 (c), (d) exp. 17–21	
9	Применимо ли к организации законодательство ЕС согласно международному публичному праву	Да — GDPR применим Нет — GDPR неприменим	ст. 3 (3) rc. 25	п. 3 exp. 22–23	–

³ EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)

⁴ EDPB Guidelines 5/2021 on the Interplay between the application of Article 3 and the provisions of Chapter V of the GDPR

Сокращения: ст. — статья, п. — пункт, rc. — пункт преамбулы (recital), exp. — пример (example)

Критерии применимости GDPR

→ Требования к учреждениям (establishments) из ЕС:

- наличие филиала, представительства, дочерней организации на территории ЕС
- наличие работников и офисов на территории ЕС
- наличие компаний, на которых имеете влияние: мажоритарный акционер, инвестор
- наличие устойчивой юридической связи между российской компанией и европейским учреждением

Критерии применимости GDPR

→ Требования к продвижению товаров и услуг:

- наличие веб-сайта в доменной зоне одной из стран-членов ЕС: .de, .fr, .eu и др.
- наличие телефонных номеров на сайте с кодами стран-членов ЕС
- реклама товаров и услуг на территории ЕС
- наличие информации на сайте о доставке на территории стран-членов ЕС
- локализация на языки стран-членов ЕС
- приём платежей в валюте стран-членов ЕС
- наличие партнёров (например, партнёрских сервисных центров) на территориях стран-членов ЕС
- международный характер деятельности: страховые компании, авиакомпании, туризм, банки, телеком

Критерии применимости GDPR

→ Мониторинг поведения физических лиц в ЕС:

- осуществление таргетированной рекламы
- профилирование на основании анализа данных пользователя: IP, cookie
- мониторинг поведения пользователей через носимые устройства
- отслеживание геолокации

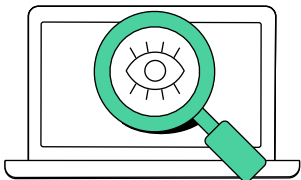
Представитель в ЕС

Назначать представителя в ЕС обязательно для контролёра или процессора, которые не осуществляют в ЕС реальную деятельность через постоянную структуру, но предлагают товары/услуги для ЕС или ведут мониторинг поведения в ЕС



Исключения минимальны — нерегулярная обработка данных, при которой:

1. Не обрабатывают большие объёмы специальных данных и данных о судимости и правонарушениях
2. Маловероятны риски нарушения прав и свобод человека



Представитель в ЕС:

1. Назначается в одной из стран ЕС, где обрабатывают данные
2. От имени контролёра/процессора (вместо них или в дополнение) взаимодействует с властями ЕС и субъектами
3. Привлекается к ответственности за нарушения контролёра/процессора



Ваши вопросы

Кейс



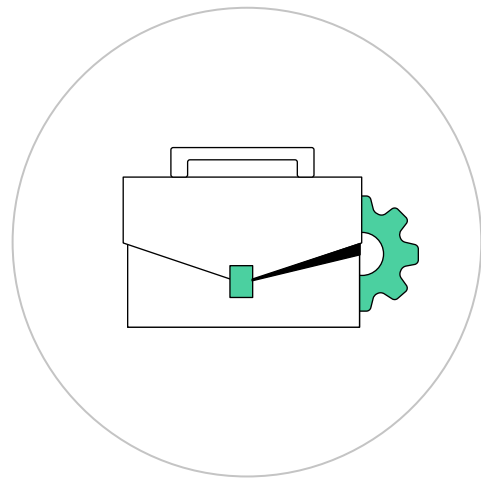
Кейс

У организации из России есть сайт на английском языке.

Организация реализует на сайте сервис для учёта личных финансов.

Оплату принимают в том числе в евро.

Попадает ли организация под действие GDPR?





Ваши вопросы

Выводы

- GDPR применяют, если организация по подряду обрабатывает персональные данные, полученные от европейской компании
- Если в Европейском союзе у организации нет представительства или филиала, но GDPR применим, нужно назначить представителя на территории ЕС



Перерыв

5 минут



Соответствие GDPR



3

Этапы подготовки к применению GDPR

- 1 Оценить применимость GDPR
- 2 Провести GAP-анализ* соответствия
- 3 Выполнить аудит обработки персональных данных (data mapping)
- 4 Оценить соответствия GDPR (GDPR assessment)
- 5 Составить план приведения в соответствие
- 6 Подписать договор с представителем

* **GAP-анализ, или анализ разрывов** — метод стратегического анализа, с помощью которого ищут шаги для достижения заданной цели

Этапы подготовки к применению GDPR

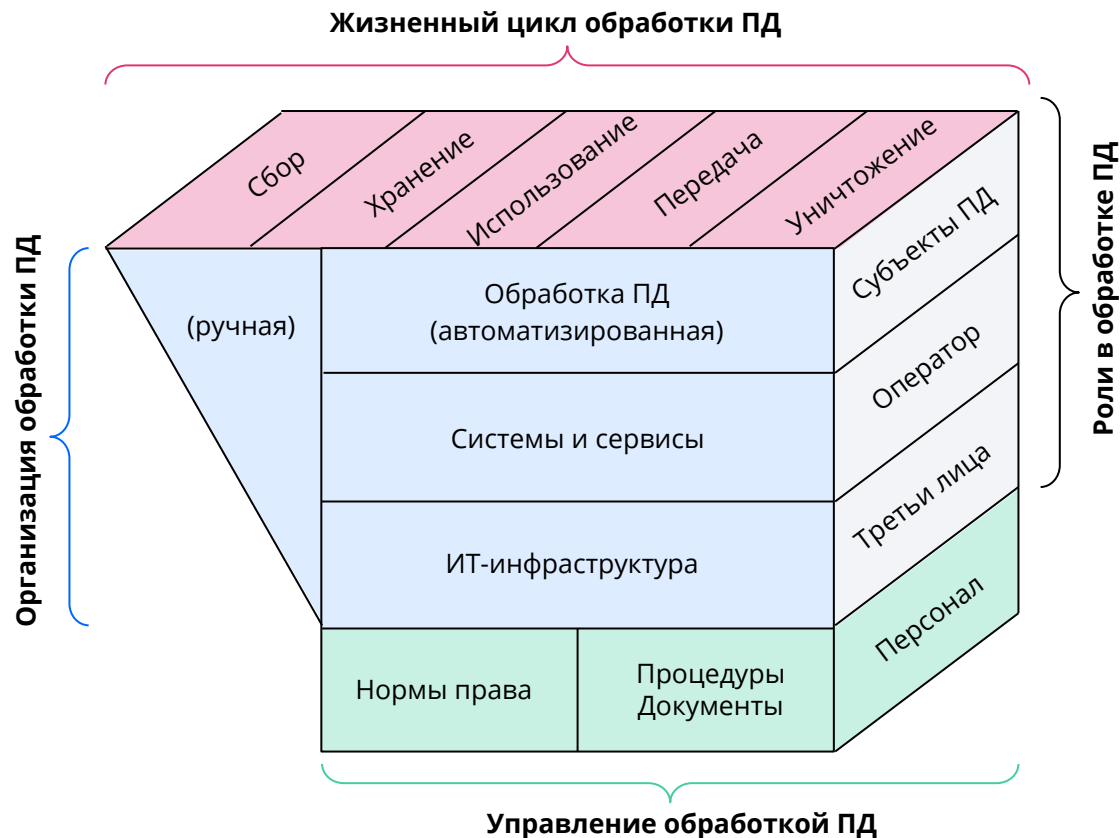
- 7 Привести в соответствие обработку данных
- 8 Удалить избыточные данные
- 9 Разработать и внедрить документы
- 10 Привести в соответствие обмен данными с контрагентами
- 11 Внедрить процессы соответствия

Этапы подготовки к применению GDPR

- 12 Провести DPIA**
- 13 Внедрить меры технической защиты
- 14 Зарегистрироваться в надзорном органе
- 15 Обучить персонал

* **DPIA (data protection impact assessment)** — оценка воздействия на защиту персональных данных (процедура, предусмотренная ст. 35 GDPR)

Учёт обработки данных (RoPA)

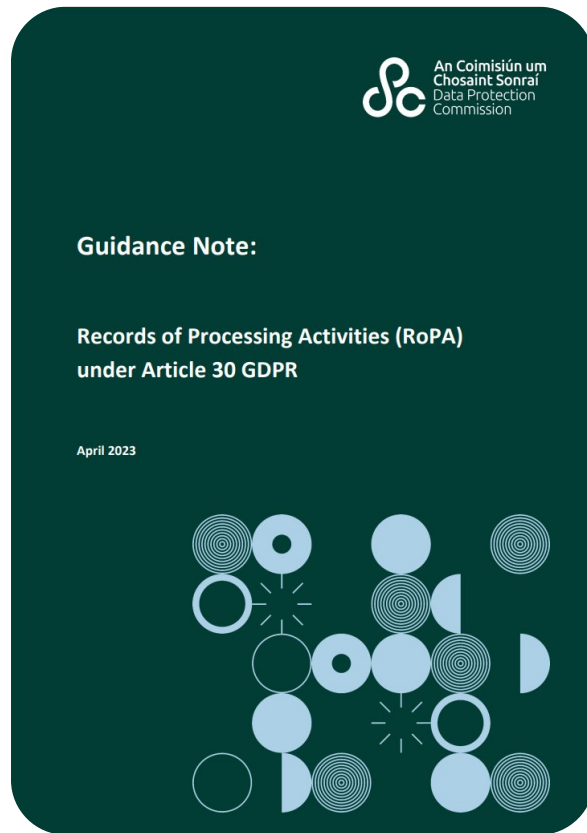


Учёт обработки данных (RoPA)

Ирландская комиссия по защите данных (DPC) 19.04.2023 опубликовала **руководство по ведению записей о деятельности по обработке данных (RoPA)** в соответствии со ст. 30 GDPR. RoPA.

Как мера демонстрации соответствия RoPA — одно из средств, с помощью которых контролёры данных реализуют принцип подотчётности, изложенный в ст. 5(2) GDPR

[Источник](#)

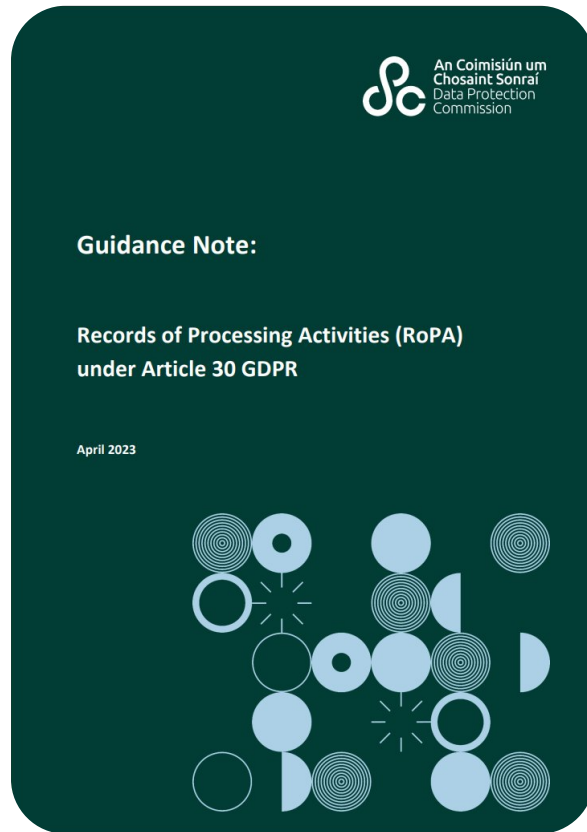


Учёт обработки данных (RoPA)

В руководстве есть примеры надлежащей практики **RoPA**.

Примеры:

- использование реляционной системы баз данных для группировки деятельности по обработке данных по подразделениям и командам, включая два возможных варианта макета RoPA с применением электронных таблиц
- примеры рекомендуемых и недостаточно подробных описаний процессов обработки данных



Чек-лист по GDPR от Gartner

Gartner.

GDPR Audit Checklist

The Gartner GDPR Audit Checklist helps organizations prepare for internal and external audits of GDPR compliance.

Instructions:

1. Track the status of all checklist items until fully compliant.
2. Use the notes page as needed for comments on progress.

For each requirement we have noted the relevant GDPR article for easy reference.

Get Started

Status key						
FC - Fully compliant IP - In progress NC - Not compliant NA - Not applicable						
	Audit question	Reference article	Status			
Accountability Governance	Do you maintain an overarching data protection policy that demonstrates compliance with requirements including processing, privacy by design and record keeping?	5(2)	FC	IP	NC	NA
	Do you train all employees on GDPR requirements and principles – including processing activities, controls, privacy impact assessments, audits, data subject rights, reporting lines and privacy by design – and the potential impact of non-compliance?	5(2)	FC	IP	NC	NA
	Do you regularly test, retrain and maintain records of training for employees who handle personal data on their understanding of GDPR requirements?	5(2)	FC	IP	NC	NA
	If you require a data protection officer (DPO), does he or she have reporting authority to the highest level of management, necessary resources, independence, and authority to ensure compliance with the GDPR and other data protection laws?	39(1) 38(1,4,6)	FC	IP	NC	NA
	Is the DPO bound by secrecy or confidentiality concerning the performance of his or her tasks?	38(5)	FC	IP	NC	NA
	If the DPO has other responsibilities, have they been assessed to avoid conflicts of interest?	38(6)	FC	IP	NC	NA
	Does the DPO have the knowledge and ability to fulfil tasks outlined in Article 39?	37(5) 39(1,2)	FC	IP	NC	NA
	Have you shared the DPO's contact information internally, publicly and with the relevant supervisory authority?	37(7)	FC	IP	NC	NA
	Do you maintain records management and data retention policies?	24(2,3)	FC	IP	NC	NA
	Have you documented principles to justify retention periods?	5(1)	FC	IP	NC	NA
Processing Principles	Is personal data processed lawfully, fairly and in a transparent manner?	5(1) 6(1,2,3,4)	FC	IP	NC	NA
	Is personal data collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes?	5(1)	FC	IP	NC	NA
	Is personal data relevant, limited and minimized to what is necessary in relation to the purposes for which they are processed?	5(1)	FC	IP	NC	NA
	Is personal data accurate and kept up to date – and is every reasonable step taken to ensure inaccurate personal data is erased and rectified without delay?	5(1)	FC	IP	NC	NA
	Is personal data kept only for as long as is necessary for the purposes for which it is processed?	5(1)	FC	IP	NC	NA
	Is personal data processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures?	5(1)	FC	IP	NC	NA
	Have you clearly identified, detailed, documented and kept up to date the purpose(s) of processing personal data?	5(1)	FC	IP	NC	NA
	Have you implemented appropriate technical or organizational measures to ensure security of personal data, including protection against unauthorized processing, accidental loss, destruction or damage?	5(1) 24(1,2)	FC	IP	NC	NA
	If you process special categories of sensitive data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), are you in compliance with Article 9(2) conditions?	9(1,2)	FC	IP	NC	NA
	If you process personal data relating to criminal convictions and offences or related security measures based on Article 6(1), is this carried out under the control of official authority or authorized by union or member state law?	10	FC	IP	NC	NA

ICO Accountability Framework

Согласно **ст. 5(2)** GDPR контролёр несёт ответственность за соблюдение принципов обработки ПД, зафиксированных в **ст. 5(1)** GDPR, и должен быть в состоянии продемонстрировать его соблюдение (принцип подотчётности).

В **п. 82** преамбулы GDPR указано, что для демонстрации соответствия GDPR контролёр или процессор должен вести учёт деятельности по обработке, за которую он отвечает.

Каждый контролёр и процессор обязан сотрудничать с надзорным органом и по запросу предоставлять в его распоряжение указанные учётные сведения, чтобы контролировать процесс обработки

Структурное описание принципа подотчётности в GDPR на основе ICO Accountability Framework

v.1.0 2022.01.10 © Алексей Мунтян | Alexey Muntyan

muntyan.alexey@gmail.com



Согласно ст.5(2) GDPR контролёр несет ответственность за соблюдение принципов обработки ПД, зафиксированных в ст.5(1) GDPR, и должен быть в состоянии продемонстрировать его соблюдение («Принцип подотчётности»). В п.82 Преамбулы GDPR указано, что для демонстрации соответствия GDPR контролёр или процессор должен вести учёт деятельности по обработке, за которую он отвечает. Каждый контролёр и процессор обязан сотрудничать с надзорным органом и по запросу предоставлять в его распоряжение указанные учётные сведения в целях мониторинга процесса обработки.

Одним из наиболее проработанных и признаваемых в экспертной среде инструментов по созданию и поддержанию комплексной программы управления защитой ПД (Comprehensive Privacy Management Programme), а также по соблюдению принципа подотчётности, является Accountability Framework¹, разработанный Офисом Уполномоченного по информации в Соединённом Королевстве (Information Commissioner's Office). На основе структуры и содержания указанного документа ниже описано **78** контролей (включающие в себя около 360 элементов) подотчётности, **группированных в 10 категорий**, где каждый из контролей направлен на обеспечение организацией возможности демонстрации соблюдения требований GDPR.

Данное описание не является дословным переводом на русский язык Accountability Framework, включает в себя несколько дополнительных контролей, а также содержит краткие ссылки и указания. Отдельным перечнем приведена документированная информация, позволяющая объективно продемонстрировать соблюдение требований GDPR.

Навигация:

1. Руководство и надзор	1
2. Политики и процедуры	2
3. Обучение и осведомлённость	3
4. Права субъектов данных	4
5. Прозрачность	6
6. VoPA и законное основание	8
7. Соглашения и обмен данными	10
8. Оценка рисков и DPIA	13
9. Управление записями и безопасность	15
10. Реализование на нарушениях и мониторинг	18
Документированная информация, позволяющая объективно продемонстрировать соблюдение требований GDPR	20
Перечень сокращений и их расшифровки	21

Описание контролей демонстрации соблюдения требований GDPR

1. Руководство и надзор

Основным элементом является эффективное руководство и надзор. Это включает в себя обеспечение четкой ответственности персонала за деятельность, связанную с обработкой и защитой данных, на стратегическом и функциональном уровне. В некоторых организациях по закону требуется должность DPO, но каждая организация должна выделять достаточно ресурсов и следить за тем, чтобы защита данных была общей ответственностью, а не задачей отдельного человека, непосредственно выполняющего функции по защите данных. Руководство организации должно нести свою долю ответственности за защиту данных, и оно должно подавать пример организованного, активного и конструктивного подхода к защите данных, который лежит в основе всего остального.



Описание	Организационная структура
Ожидания	<ul style="list-style-type: none">Руководство организации несет общую ответственность за управление и практическую реализацию защиты данных.Лица, принимающие решения, поддают пример и поощряют активную, конструктивную культуру соблюдения требований по защите данных.Существует четкий порядок коммуникаций между соответствующими группами.Политики и процедуры четко определяют организационную структуру управления и практической реализации защиты данных.В должностных инструкциях четко прописаны обязанности и порядок предоставления отчетности руководству.Должностные инструкции являются актуальными, соответствуют поставленной цели и регулярно пересматриваются.Персонал, обеспечивающий защиту данных, понимает организационную структуру и свои обязанности.
Ссылки	<ul style="list-style-type: none">GDPR: ст.24, ст.74GDPR Guidelines 07/2020 on the concepts of controller and processor in the GDPREDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020)
1.2 Контроль	Назначение DPO

¹ См. <https://ico.org.uk/for-organisations/accountability-framework/>

² Под «персоналом» понимается совокупность всех сотрудников организации, а также иные физические лица, осуществляющие производственные, управленческие или иные функции в интересах организации на основании трудового договора или договора гражданско-правового характера.

ICO Accountability Framework

Accountability Framework, разработанный офисом уполномоченного по информации в Соединенном Королевстве (Information commissioner's office), — один из признаваемых в экспертной среде инструментов, которые помогают создать и поддерживать комплексную программу управления защитой ПД (Comprehensive privacy management programme), а также соблюдать принцип подотчётности.

На его основе описано **78 контролей (включают около 360 элементов) подотчётности, которые сгруппированы в 10 категорий**, где каждый из контролей направлен на обеспечение организацией возможности продемонстрировать соблюдение требований GDPR

Структурное описание принципа подотчётности в GDPR на основе ICO Accountability Framework

v.1.0 2022.01.10 © Алексей Мунтян | Alexey Muntyan
muntyan.alexey@gmail.com



Согласно ст.5(2) GDPR контролёр несет ответственность за соблюдение принципов обработки ПД, зафиксированных в ст.5(1) GDPR, и должен быть в состоянии продемонстрировать его соблюдение («Принцип подотчётности»). В п.82 Преамбулы GDPR указано, что для демонстрации соответствия GDPR контролёр или процессор должны вести учет деятельности по обработке, за которую они отвечают. Каждый контролёр и процессор обязан сотрудничать с надзорным органом и по запросу предоставлять в его распоряжение указанные учетные сведения в целях мониторинга процесса обработки.

Одним из наиболее проработанных и признаваемых в экспертной среде инструментов по созданию и поддержанию комплексной программы управления защитой ПД (Comprehensive Privacy Management Programme), а также по соблюдению принципа подотчётности, является Accountability Framework¹, разработанный Офисом Уполномоченного по информации в Соединенном Королевстве (Information Commissioner's Office). На основе структуры и содержания указанного документа ниже описано **78 контролей (включающие в себя около 360 элементов) подотчётности, сгруппированных в 10 категорий**, где каждый из контролей направлен на обеспечение организацией возможности демонстрации соблюдения требований GDPR.

Данное описание не является дословным переводом на русский язык Accountability Framework, включает в себя несколько дополнительных контролей, а также содержит краткие ссылки и указания. Отдельным перечнем приведена документированная информация, позволяющая объективно продемонстрировать соблюдение требований GDPR.

Навигация:

1. Руководство и надзор	1
2. Политики и процедуры	2
3. Обучение и осведомленность	3
4. Права субъектов данных	4
5. Прозрачность	6
6. ВРА и законное основание	8
7. Соглашения и обмен данными	10
8. Оценка рисков и DPIA	13
9. Управление записями и безопасность	15
10. Реагирование на нарушения и мониторинг	18
Документированная информация, позволяющая объективно продемонстрировать соблюдение требований GDPR	20
Перечень сокращений и их расшифровки	21

Описание контролей демонстрации соблюдения требований GDPR

1. Руководство и надзор

Основополагающим элементом является эффективное руководство и надзор. Это включает в себя обеспечение четкой ответственности персонала² за деятельность, связанную с обработкой и защитой данных, на стратегическом и функциональном уровне. В некоторых организациях по закону требуется должность DPO, но каждая организация должна выделять достаточно ресурсов и следить за тем, чтобы защита данных была общей ответственностью, а не задачей отдельного человека, непосредственно выполняющего функции по защите данных. Руководство организации должно нести свою долю ответственности за защиту данных, и оно должно подавать пример организованного, активного и конструктивного подхода к защите данных, который лежит в основе всего остального.



Описание	Организационная структура
Ожидания	<ul style="list-style-type: none">Существует организационная структура для управления и практической реализации защиты данных, которая обеспечивает эффективное руководство и надзор, четкий порядок и обязанности, а также эффективные коммуникации.Руководство организации несет общую ответственность за управление и практическую реализацию защиты данных.Лица, принимающие решения, подают пример и поощряют активную, конструктивную культуру соблюдения требований по защите данных.Существует четкий порядок коммуникаций между соответствующими группами.Политики и процедуры четко определяют организационную структуру управления и практической реализации защиты данных.В должностных инструкциях четко прописаны обязанности и порядок предоставления отчетности руководством.Должностные инструкции являются актуальными, соответствуют поставленной цели и регулярно пересматриваются.Персонал, обеспечивающий защиту данных, понимает организационную структуру и свои обязанности.
Ссылки	<ul style="list-style-type: none">GDPR: ст.24, ст.74EDPS Guidelines 07/2020 on the concepts of controller and processor in the GDPREDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020)

1.2 Контроль Назначение DPO

¹ См. <https://ico.org.uk/for-organisations/accountability-framework/>

² Под «персоналом» понимается совокупность всех сотрудников организации, а также иные физические лица, осуществляющие производственные, управленческие или иные функции в интересах организации на основании трудового договора или договора гражданско-правового характера.

ICO Accountability Framework

- 1 Руководство и надзор
- 2 Политики и процедуры
- 3 Обучение и осведомлённость
- 4 Права субъектов данных
- 5 Прозрачность обработки
- 6 RoPA и законное основание
- 7 Соглашения и обмен данными
- 8 Оценка рисков и DPIA
- 9 Управление записями и безопасность
- 10 Реагирование на нарушения и мониторинг

Выводы

- Требования GDPR похожи на те, что содержатся в российском законодательстве, но есть новые подходы к защите данных и прав физических лиц в части обработки их данных
- В GDPR, согласно принципу accountability, требуется подтверждать выполнение каждого требования регламента





Ваши вопросы

Итоги занятия

- Узнали, зачем нужен GDPR и в чём заключается его специфика
- Поняли, как определять, попадает ли компания, конкретный сервис или процесс под регулирование GDPR
- Разобрались в основных требованиях и особенностях GDPR



Дополнительные материалы

- [GDPR](#) на русском языке
- [Разъяснения](#) EDPB по применимости GDPR
- [Разъяснения](#) EDPB по определению контролёра и процессора



GDPR: применение и основные требования

Алексей Мунтян
Генеральный директор Privacy Advocates

