

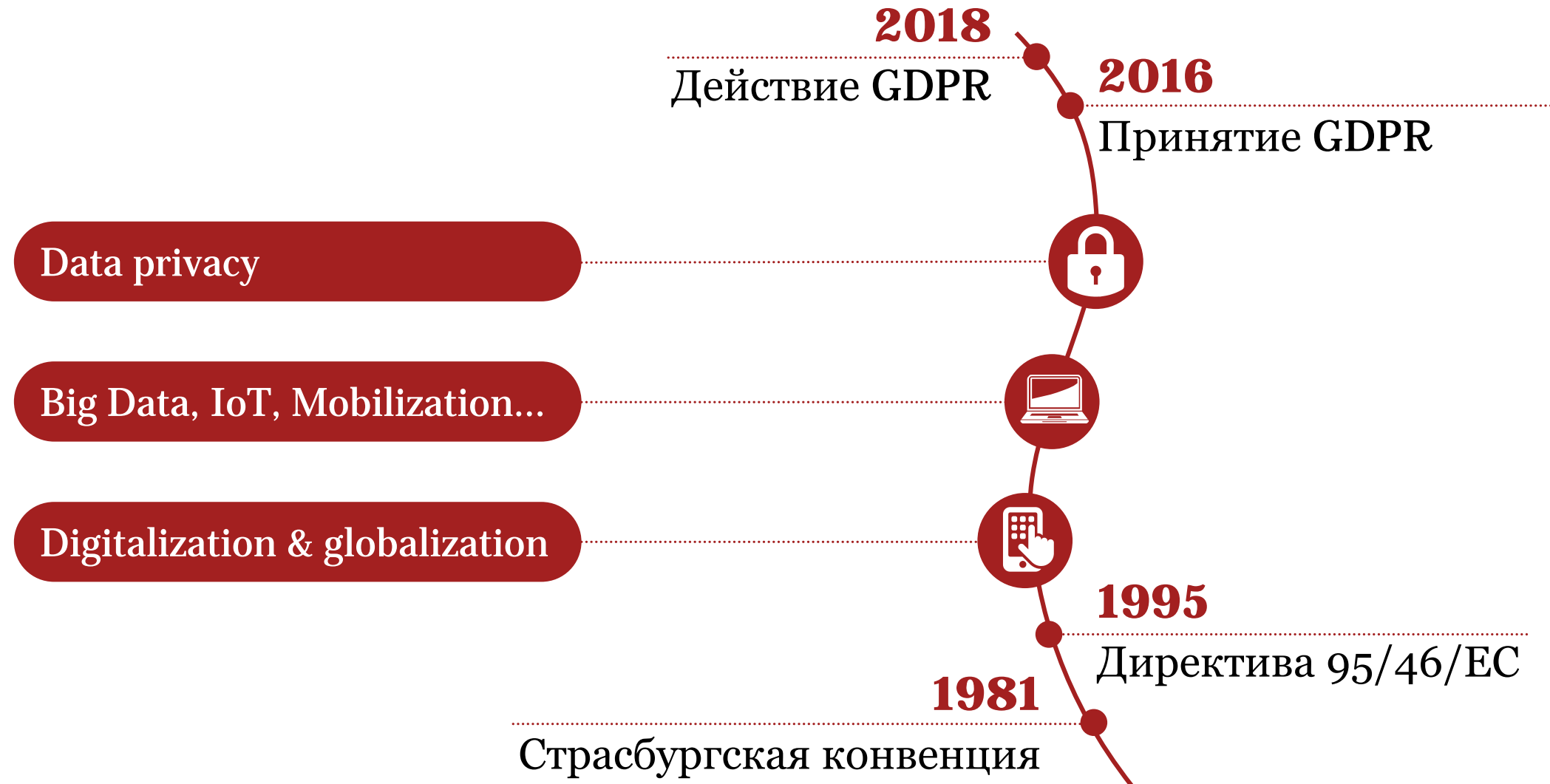
GDPR: практика реализации требований

General Data Protection Regulation

Июнь 2018



Причины появления *GDPR*



Значимость обеспечения конфиденциальности

1

Что с доверием?

Лояльность дает
примерно
+15% к обороту
и напрямую
зависит от доверия

69%

Клиентов полагают,
что компании
уязвимы к атакам

25%

Клиентов верят,
что компании заботятся
о их данных должным
образом

*Реальность в том, что
сейчас клиенты доверяют
компаниям меньше, чем в
прошлом. Всего 12%
отвечивших доверяют
больше, чем год назад.*

85%

Покупателей не станут
приобретать у компании,
если они думают, что она
недостаточно безопасна.

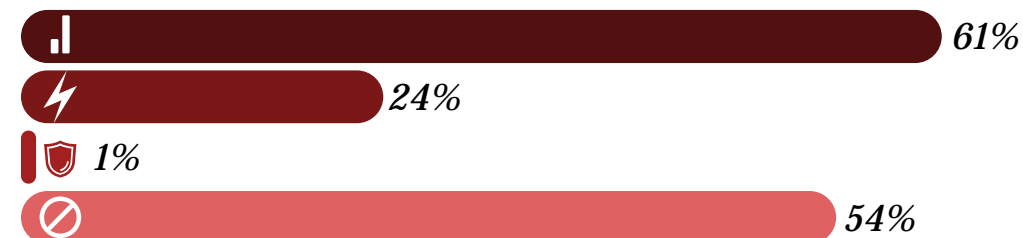
Отказ клиентов от покупок при сомнениях в обеспечении конфиденциальности их данных



Обычно читают политику безопасности данных до выполнения транзакций



Могут отказаться от транзакций из-за положений политики безопасности



*По данным опроса Forrester Data Consumer Technographics Online Benchmark Survey 2017

В чем же проблемы?

Цифровые
личности —
новая валюта
на черном
рынке

Количество данных, скомпрометированных
в первой половине 2017

1,901,866,611

10,507,550

Потери в
день



437,815

Потери в
час



7,297

Потери в
минуту



122

Потери в
секунду



Количество инцидентов по типу

74%

Кража
цифровой
личности
680 инцидентов



<http://breachlevelindex.com/>

Бизнес вынужден оперировать в атмосфере нулевого доверия

Цена решения проблемы?

Клиенты склонны прощать, но только в случае, когда компании смогут продемонстрировать реальные изменения по защите данных клиентов.

Потребители, у которых был позитивный опыт взаимодействия с компанией, на 15% вероятнее останутся лояльными к бренду. Однако, если у клиента был негативный опыт, его лояльность падает сразу на 25%.

Предпочтения клиентов о том, как компании могут вернуть их доверие после взлома



Source: PwC US Protect.me Survey, 2017

*Что такое **GDPR** и сравнение с 152ФЗ*

2

Применение *GDPR*



- Старые согласия действуют, если соответствуют GDPR
- Постепенное внедрение карательных механизмов
- Последующий тюнинг регулирования



- Любые персональные данные (ПД)
- Любые способы обработки включая картотеки
- Тест: «reasonable likely to be used» контролером / 3м лицом



- Страны ЕС
- Субъекты ПД – лица, находящиеся в ЕС
- Контролёры и процессоры – экстерриториально

Применение *GDPR*



- Старые согласия действуют, если соответствуют GDPR
- Постепенное внедрение карательных механизмов
- Последующий тюнинг регулирования



- Любые персональные данные (ПД)
- Любые способы обработки включая картотеки
- Тест: «reasonable likely to be used» контролером / зм лицом



- Страны ЕС
- Субъекты ПД – лица, находящиеся в ЕС
- Контролёры и процессоры – экстерриториально

Применение *GDPR*



- Старые согласия действуют, если соответствуют GDPR
- Постепенное внедрение карательных механизмов
- Последующий тюнинг регулирования



- Любые персональные данные (ПД)
- Любые способы обработки включая картотеки
- Тест: «reasonable likely to be used» контролером / 3м лицом



- Страны ЕС
- Субъекты ПД – лица, находящиеся в ЕС
- Контролёры и процессоры – экстерриториально

Область регулирования *GDPR*

GDPR применяется ...



с **25 мая 2018 г.** согласия физических лиц на обработку ПДн, полученные ранее, могут использоваться, если они соответствуют GDPR. Карательные механизмы будут внедряться постепенно, так как многие правила определены в GDPR лишь на уровне принципов. Регулирование будет в последующем конкретизировано в разъяснениях регулирующих органов и правоприменительной практике.



к **любым типам персональных данных** без исключений и к **любым способам обработки** ПДн. ПДн включают в себя **любую** информацию, относящуюся прямо или **косвенно** к определенному или определяемому лицу (т.е. ФИО, паспортные данные, заработная плата, местонахождение, адрес проживания, контактные данные e-mail, телефон), IP-адрес используемых устройств и т.п.).



к обработке ПДн **лиц, находящихся в ЕС**. В GDPR отсутствует привязка к гражданству субъектов ПДн. Вероятно правила GDPR будут применяться ко всем лицам, находящимся на территории ЕС, и/или к лицам чьи данные обрабатываются на территории ЕС, не зависимо от гражданства этих лиц.

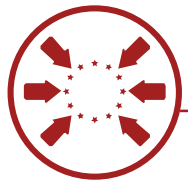


к контроллерам (операторам ПДн) и обработчикам, если они обрабатывают ПДн лиц, находящихся в ЕС, **независимо от места осуществления обработки**. Применение ответственности к операторам и обработчикам ПДн, находящимся за пределами ЕС. Распространено мнение, что в первую очередь европейские регуляторы проверят на соответствие GDPR компании из США, Китая и России.

Периметр применимости *GDPR*

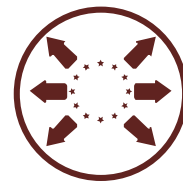


Место нахождения контролёра/процессора



в ЕС

- Постоянные структуры, расположенные в ЕС, вне зависимости от организационно-правовой формы / типа обособленного подразделения






вне ЕС

- Осуществление реальной деятельности через постоянную структуру в ЕС
- Направленность деятельности на ЕС
- Совместный контроль ПД с постоянными компаниями, расположенными в ЕС




GDPR vs 152-ФЗ: принципы обработки данных

	152-ФЗ
Законность процессов обработки ПД	
Справедливость процессов обработки ПД	
Понятность процессов гражданину	
Точность и актуальность данных	
Обработка только для заявленных целей	
Отсутствие избыточных данных	
Ограниченный срок хранения	
Сохранность и конфиденциальность	

 соответствует  частично соответствует  не соответствует

GDPR vs 152-ФЗ: права субъектов

	152-ФЗ
Доступ к данным и информации об обработке	
Получение копии данных (raw data)	
Корректировка и дополнение данных	
Уничтожение данных (право на забвение)	
Блокировка обработки данных	
Возражение против обработки данных	
Перенос данных (data portability right)	
Отзыв согласия	

 соответствует  частично соответствует  не соответствует

GDPR vs 152-ФЗ: обязанности контролера

152-ФЗ

Доказать соблюдение принципов обработки (accountability)



Принимать технические и организационные меры (privacy by design / default)



Документировать деятельность по обработке данных (recording)



Оценивать риски (data protection impact assessment)



Обеспечивать безопасность данных



Внедрить политики по обработке данных



Извещать регулятора и граждан о проблемах с данными






Уведомлять граждан о получении их данных от третьих лиц












Назначать ответственного за защиту данных



 соответствует  частично соответствует  не соответствует

GDPR vs 152-ФЗ: ключевые требования к согласию

	152-ФЗ
Свободное, конкретное, информированное, непротиворечивое	
Форма согласия и отзыва: заявление или утвердительное действие	
Простой и понятный язык	
Отдельное от каких-либо других вопросов	
Отдельное согласие для каждой цели обработки	
Родительское согласие на обработку данных детей до 16 лет для онлайн услуг	
Отозвать также просто, как и получить	
Контролер должен доказать получение согласия	

 соответствует  частично соответствует  не соответствует

Требования *GDPR* – на что обратить внимание?



Требования *GDPR* – на что обратить внимание?

Согласно

Право на забвение Штрафы

Переносимость данных Извещение о проблемах с данными

Представитель в ЕС *Privacy by design and default*

Полномочия регуляторов

Принятие решений на основании автоматической обработки

Переносимость данных (*data portability right*)

«Субъект персональных данных имеет право получить относящиеся к нему персональные данные, предоставленные им контролёру, в структурированном, широко используемом и машиночитаемом формате и передать эти данные другому контролёру без препятствий со стороны контролёра, которому эти данные были предоставлены».



Важные детали:

- Получение **своих** персональных данных, предоставленных контролёру.
- Машиночитаемый **формат**.
- Передача **другому контролёру**.
- **Отсутствие препятствий**.
- **Применимо** только для **автоматизированной** обработки.
- **Информирование** о наличии права.

Принципы «*Privacy by default*» и «*Privacy by design*»

«Privacy by default»



- Суть принципа – минимизация объема обрабатываемых данных и сроков их обработки.
- Минимизация обрабатываемых данных сузит область проекта по трансформации либо полностью выведет компанию из-под действия GDPR.
- Задайте вопрос: «Для чего нам нужны эти данные?»
- Задайте вопрос: «Что произойдет, если мы не будем обрабатывать эти данные, через один год, через три года, через пять лет?»
- Уничтожение данных, утративших свою актуальность – это довольно сложный проект, который требует вовлечения юристов, бизнес-подразделений и ИТ-специалистов.
- Принцип Privacy by default обязывает контроллеров знать в каких процессах и ИТ-системах обрабатываются данные, в каком объеме, с какой целью и как долго. Выявить это можно путем ручного или автоматизированного анализа (например, с помощью специальных GDPR модулей SAP).

GDPR требует, чтобы компании обрабатывали минимально необходимый объем данных в минимально возможные сроки. Регулятор имеет право оценить заявленные объемы и сроки.



Принципы «*Privacy by default*» и «*Privacy by design*»

«Privacy by design»



- Принцип призван решить проблему «недальновидности» организаций в начале сбора персональных данных.
- Следуя этому принципу, организации должны продумывать механизмы защиты информации на этапе планирования процедур обработки данных.
- Если внедряется новая система или процесс, рабочая группа должна оценить, отвечает ли это изменение требованиям GDPR? Например, возможно ли будет реализовать право субъекта на забвение или право на перенос его данных из системы? Как будет реализовано управление доступом к данным? И другие подобные вопросы.
- Принцип должен быть внедрен в процессы SDLC (разработки ПО), управления изменениями, а так же в процессы проектного управления.

Европейские регуляторы будут просить предъявить свидетельства того, что при внедрении изменений принцип «Privacy by design» соблюдается как контролером, так и обработчиком.



Оценка воздействия на защищенность персональных данных

Data protection impact assessment (DPIA)



- Обязательно нужно проводить при скоринге, мониторинге, обработке больших объемов специальных категорий данных и при других аналогичных операциях с высоким риском для субъекта (*передача данных за пределы ЕС, применение технических новшеств, обработка данных слабозащищённых лиц*).
- Контроллер так же должен провести процедуры оценки рисков, для выявления критичных процессов, для которых DPIA нужно провести дополнительно.
- Основная цель – понять последствия, которые могут наступить для субъекта и для контролёра/обработчика в случае, если что-то пойдет не так.
- GDPR ставит задачи, обязательно решаемые в ходе DPIA. Структуру, форму и методологию контролёр/обработчик определяет самостоятельно.
- Вопрос необходимости проведения DPIA рекомендуется внедрить в процессы Privacy by Design.

Европейские регуляторы разъясняют, что важным аспектом для принятия решения о необходимости DPIA является качественная оценка рисков в процессах обработки персональных данных.



Сообщение о проблемах с данными



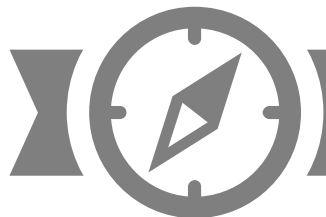
Содержание сообщения:

- Описание проблемы, влекущей *неправомерное уничтожение, утрату, изменение, раскрытие, доступ к ПД*
- Число и категория затронутых лиц и записей (*можно не сообщать гражданину*)
- Последствия
- Принятые/предлагаемые меры для решения проблемы (*например, рекомендации гражданину*)
- Контактное лицо

Законопроект № 416052-6

- обязанность уведомлять Роскомнадзор в случае неправомерного раскрытия персональных данных неограниченному кругу лиц

Сообщение о проблемах с данными



Когда можно не сообщать?



Регулятору

- **Возникновение рисков** для прав и свобод гражданина **маловероятно**



Гражданину

- Проблема **не приведёт к высоким рискам** для его прав и свобод

Например, данные защищены так, что не могут быть прочтены посторонним лицом или приняты меры, не дающие риску материализоваться

- Было публичное сообщение о проблеме, т.к. рассылка индивидуальных сообщений требует неадекватных усилий.

Когда необходимо назначать ответственного за защиту персональных данных (DPO)?

1

Обработка органом власти, субъектом властных полномочий (public body)



Когда необходимо назначать ответственного за защиту персональных данных (DPO)?

2

Регулярное систематическое наблюдение в больших объёмах

Мониторинг через
«умные» устройства



Трекинг
местонахождения



Видеомониторинг



Программы лояльности



Поведенческая
реклама



Создание профилей
и скоринг для оценки
рисков



Когда необходимо назначать ответственного за защиту персональных данных (DPO)?

3

Обработка больших объёмов специальных категорий ПД

Медицинские
данные



Данные о сексуальной
ориентации



Генетические данные



Данные о политических
и религиозных взглядах



Данные об этническом
происхождении



Данные о членстве в
профсоюзе



Биометрические
данные для
идентификации



Когда необходимо назначать ответственного за защиту персональных данных (DPO)?

4

Обработка больших объемов данных о судимости и правонарушениях

Данные о
правонарушениях



Данные об уголовных
приговорах



Данные о нарушении
правил безопасности



Как назначить ответственного за защиту персональных данных (DPO)?

Может находиться
не в ЕС

Подчинение
первому лицу

Может быть
внешним
сотрудником

Один на несколько
компаний

Защищен от
конфликтов
интересов и
влияния

Специальные
знания GDPR

Назначение представителя в ЕС



Для кого обязательно?

Для контролера или обработчика, не осуществляющего в ЕС реальную деятельность через постоянную структуру, но предлагающего товары/услуги для ЕС или ведущего мониторинг поведения в ЕС

Исключения минимальны

Нерегулярная обработка ПД, при которой:

- Не обрабатываются большие объёмы специальных данных и данных о судимости и правонарушениях и
- Маловероятны риски нарушения прав и свобод человека

Представитель

- В одной из стран ЕС, чьи данные обрабатываются
- От имени контролёра/ обработчика (вместо них или в дополнение) взаимодействует с властями ЕС и гражданами
- **Привлекается к ответственности за нарушения контролёра/ обработчика**

Широкие полномочия регулятора



GDPR, Статья 58

- **Истребовать информацию** у контролёра и обработчика;
- **Получать** от контролёра и обработчика **доступ** к информации и ПД, в помещения/на территорию, к оборудованию и средствам обработки данных;
- **Проводить** проверку (**аудит**) защиты ПД;
- Требовать выполнения запроса гражданина;
- Требовать корректировки, уничтожения, блокировки ПД;
- Требовать **сообщить гражданину о проблемах с ПД**;
- Требовать приведения обработки ПД в соответствие с GDPR;
- **Накладывать** временные и постоянные **ограничения**, в том числе запрещать обработку;
- **Приостанавливать передачу ПД** за пределы ЕС;
- Выносить предупреждения, объявлять замечания и **накладывать штрафы**.

Штрафы

До 10 миллионов Евро или до 2% выручки*

Сферы нарушения обязательств контролёра и обработчика

- Получение согласия на обработку ПД детей
- **Privacy by design and by default**
- Совместный контроль ПД
- **Неназначение представителя в ЕС**
- Обязанности обработчика и действия согласно указаниям контролёра
- Документирование обработки ПД
- Сотрудничество с надзорным органом
- Требования к безопасности ПД
- **Сообщение о проблемах с ПД надзорному органу и субъекту ПД**
- **Оценка влияния на защищённость ПД (DPIA)**
- Назначение ответственного за защиту ПД и его задачи

До 20 миллионов Евро или до 4% выручки*

Нарушения основополагающих правил

- Принципы обработки ПД
- Правомерность обработки ПД
- Правила согласия на обработку ПД
- Обработка спец. категорий ПД

Сферы нарушения прав субъектов ПД

- Уведомление субъекта ПД
- Право доступа к ПД
- Корректировка ПД
- Уничтожение ПД
- Перенос данных
- Ограничение обработки
- Право возражать против обработки ПД
- Принятие решений на основе автоматической обработки

Нарушения при передаче данных из ЕС

Отказ в доступе к информации, ПД, в помещения/ на территорию, невыполнение предписания, ограничивающего обработку или приостанавливающего передачу ПД, невыполнение требований

*Выручка по всему миру за предшествующий финансовый год

Как применяются штрафы?



Основные правила

- 1 Единообразие vs. **индивидуальный подход**
- 2 Штраф **может не применяться** при незначительных нарушениях
- 3 Штраф должен быть **действенным, соразмерным и вразумляющим**
- 4 Может быть наложен **в дополнение или вместо** других мер
- 5 За нарушение нескольких положений GDPR по одной или связанным операциям размер штрафа не должен превышать максимального для самого тяжёлого нарушения.

Как применяются штрафы?



Что будет учтено при определении размера?

Природа, тяжесть и
продолжительность
нарушения

Число затронутых
лиц и масштаб
причинённого им
вреда

Совершено
нарушение
умышленно или по
неосторожности

Принятие мер по
снижению
последствий
нарушения

Предшествующие
схожие нарушения

Ранее выданные
требования по тому
же вопросу

Уровень сотрудничества
с регулятором для
устранения нарушения и
снижения негативного
эффекта

Доходы (снижение
убытков), полученные
от нарушения

Примеры применимости требований к организациям

3

Торговая площадка в Интернет (*Digital market place*)

Описание бизнеса компании

- Представление товаров от продавцов из Китая покупателям в России, ЕС и США через web-сайт
- Организация продажи представленных товаров, их оплаты, доставки и обработки претензий покупателей
- ЦОД расположен в ЕС и/или РФ
- Группа поддержки ИТ и разработчики сайта находятся в России
- Деятельность ведется от имени нескольких юр. лиц в разных юрисдикциях

Анализ процессов обработки ПДн, подпадающих под требования GDPR

- Сбор и обработка данных граждан ЕС
- Таргетирование рекламы и индивидуальных предложений для граждан ЕС
- Передача данных граждан ЕС продавцам и логистическим компаниям
- Обработка платежей от граждан ЕС
- Обработка претензий от граждан ЕС

Заключение о применимости Требования GDPR применимы



Интернет-магазин программного обеспечения

Описание бизнеса компании

- Технологическая платформа для организации взаимодействия покупателей ПО и производителей ПО
- Организация продажи ключей активации для ПО, получения оплаты от покупателей (физических лиц), доставки им ключей активации и передачи платежей производителям ПО (физическим и юридическим лицам)
- Охват территории и месторасположение контрагентов – весь мир, в т.ч. ЕС
- Наличие адресных коммуникаций для лиц, находящихся в ЕС
- ЦОД расположен в РФ
- Группа поддержки ИТ и разработчики сайта находятся в России
- Деятельность ведется от имени нескольких юр. лиц в разных юрисдикциях

Анализ процессов обработки ПДн, подпадающих под требования GDPR

- Сбор и обработка данных граждан ЕС
- Таргетирование рекламы и индивидуальных предложений для граждан ЕС
- Передача данных граждан ЕС производителям ПО
- Обработка платежей от граждан ЕС
- Обработка претензий от граждан ЕС

Заключение о применимости Требования GDPR применимы



Российская часть глобальной розничной торговой сети

Описание бизнеса компании

- Штаб-квартира на территории ЕС
- Продажа товаров через сеть собственных магазинов на территории РФ
- Направление покупателям персонифицированных предложений по различным каналам коммуникаций, вне зависимости от их фактического местонахождения в момент получения информации (e-mail, SMS)
- Целевая аудитория – лица, находящиеся на территории РФ и посещающие магазины на территории РФ

Анализ процессов обработки ПДн, потенциально подпадающих под требования GDPR

- Ориентированность деятельности на граждан ЕС и лиц, находящихся в ЕС отсутствует (деятельность направлена только на лиц, находящихся в РФ)

Заключение о применимости Требования GDPR **не применимы**



Логистическая компания – автомобильные перевозки РФ-ЕС

Описание бизнеса компании

- Автомобильные грузоперевозки между РФ и ЕС
- Собственный парк автомобилей
- Водители и экспедиторы граждане РФ и СНГ, в штате компании
- Мониторинг движения транспортных средств
- Мониторинг времени водителя, проведенного за рулем
- Деятельность ведется от имени нескольких юр. лиц в различных юрисдикциях

Анализ процессов обработки ПДн, подпадающих под требования GDPR

- Сбор и обработка данных лиц (водителей и экспедиторов), находящихся на территории ЕС

Заключение о применимости Требования GDPR применимы



Разработчики и издатели компьютерных игр

Описание бизнеса компании

- Технологическая платформа для организации взаимодействия покупателей компьютерных игр и различных игровых артефактов и производителей
- Организация продажи компьютерных игр и различных игровых артефактов, получения оплаты от покупателей (физических лиц), доставки им ключей активации и передачи платежей производителям ПО (физическим и юридическим лицам)
- Охват территории и месторасположение контрагентов – весь мир, в т.ч. ЕС
- Наличие адресных коммуникаций для лиц, находящихся в ЕС
- ЦОДы расположены в различных юрисдикциях
- Деятельность ведется от имени нескольких юр. лиц в различных юрисдикциях

Анализ процессов обработки ПДн, подпадающих под требования GDPR

- Сбор и обработка данных граждан ЕС
- Таргетирование рекламы и индивидуальных предложений для граждан ЕС
- Передача данных граждан ЕС компьютерных игр и различных игровых артефактов
- Обработка платежей от граждан ЕС
- Обработка претензий от граждан ЕС

Заключение о применимости Требования GDPR применимы



Оператор аренды автомобилей (*rent-a-car*) с возможностью выезда на арендованном автомобиле в ЕС

Описание бизнеса компании

- Предоставление услуги аренды автомобилей с возможностью выезда в ЕС
- Собственный парк автомобилей
- Клиенты – физические и юридические лица
- Мониторинг движения автомобилей и отслеживание текущего местоположения
- Применение разных тарифов в зависимости от возможности выезда за пределы РФ и разрешенного пробега

Анализ процессов обработки ПДн, подпадающих под требования GDPR

- Сбор и обработка данных лиц (арендаторов автомобилей), находящихся на территории ЕС
- Сбор и обработка данных об административных правонарушениях лиц, находящихся на территории ЕС

Заключение о применимости Требования GDPR применимы



Пассажирско-транспортная компания

Описание бизнеса компании

- Продажа билетов на маршруты из ЕС в РФ
- Идентификация пассажиров
- Организация пассажирских перевозок
- Организация туров по РФ на сайте, для лиц, находящихся за границей

Анализ процессов обработки ПДн, потенциально подпадающих под требования GDPR

- Продажа билетов лицам, находящимся в ЕС
- Продажа и организация туров для лиц, находящихся в ЕС
- Работа представительств компании, находящихся в странах ЕС

Заключение о применимости Требования GDPR применимы



Туристическая компания

Описание бизнеса компании

- Организация туров для клиентов в РФ и за границей
- Бронирование гостиниц
- Бронирование авиа и железнодорожных билетов

Анализ процессов обработки ПДн, потенциально подпадающих под требования GDPR

- Организация туров по РФ для клиентов из ЕС
- Бронирование билетов и гостиниц для клиентов из ЕС

Заключение о применимости Требования GDPR применимы



Практика внедрения требований в организации

4

Ответственность за реализацию требований **GDPR**



Крупные компании

(Оборот > \$500M)

- Технический директор\ИТ-директор
- Директор по соответствию требованиям
- Генеральный директор
- Директор по защите данных

Небольшие компании

(Оборот < \$500M)

- Технический директор\ИТ-директор
- Совет директоров
- Директор по соответствию требованиям
- Генеральный директор

*По данным опроса PwC *Pulse Survey: CEO involvement helps boost GDPR preparations*

- <https://www.pwc.com/us/en/cybersecurity/general-data-protection-regulation/pulse-survey-ceo-involvement.html>

Влияние поддержки высшего менеджмента на успех внедрения GDPR

Поддержка высшего руководства имеет решающее значение для внедрения требований GDPR. По данным исследования PwC, **компаниях, в которых ответственным за реализацию требований GDPR является первое лицо (CEO), в 44% процентах случаев уже завершили реализацию требований GDPR.** *

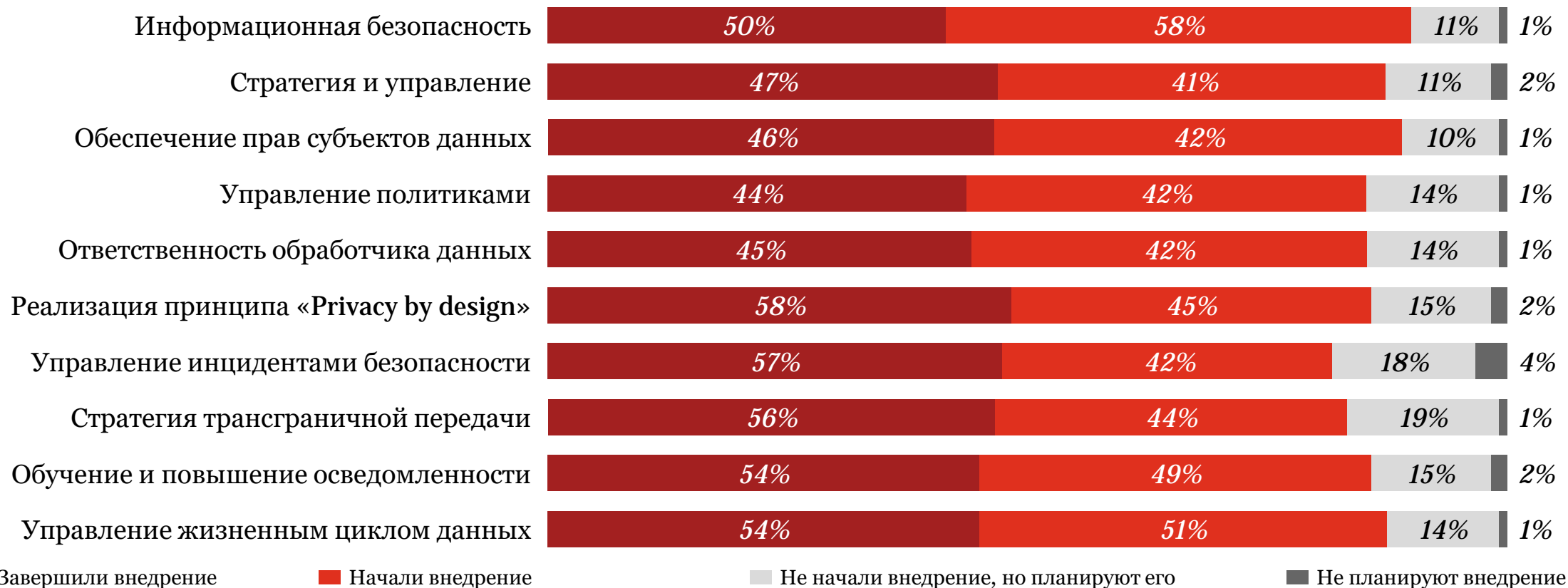


Ответственный за реализацию требований GDPR в компании	Не начали проект	Начали оценку	Завершили оценку	Приводят в соответствие	Завершили проект
Генеральный директор	35%			17%	44%
Технический директор\ ИТ-директор		20%	32%	23%	31%
Директор со соответствию требованиям		33%	32%	27%	15%
Совет директоров				15%	

*По данным опроса PwC *Pulse Survey: CEO involvement helps boost GDPR preparations*

- <https://www.pwc.com/us/en/cybersecurity/general-data-protection-regulation/pulse-survey-ceo-involvement.html>

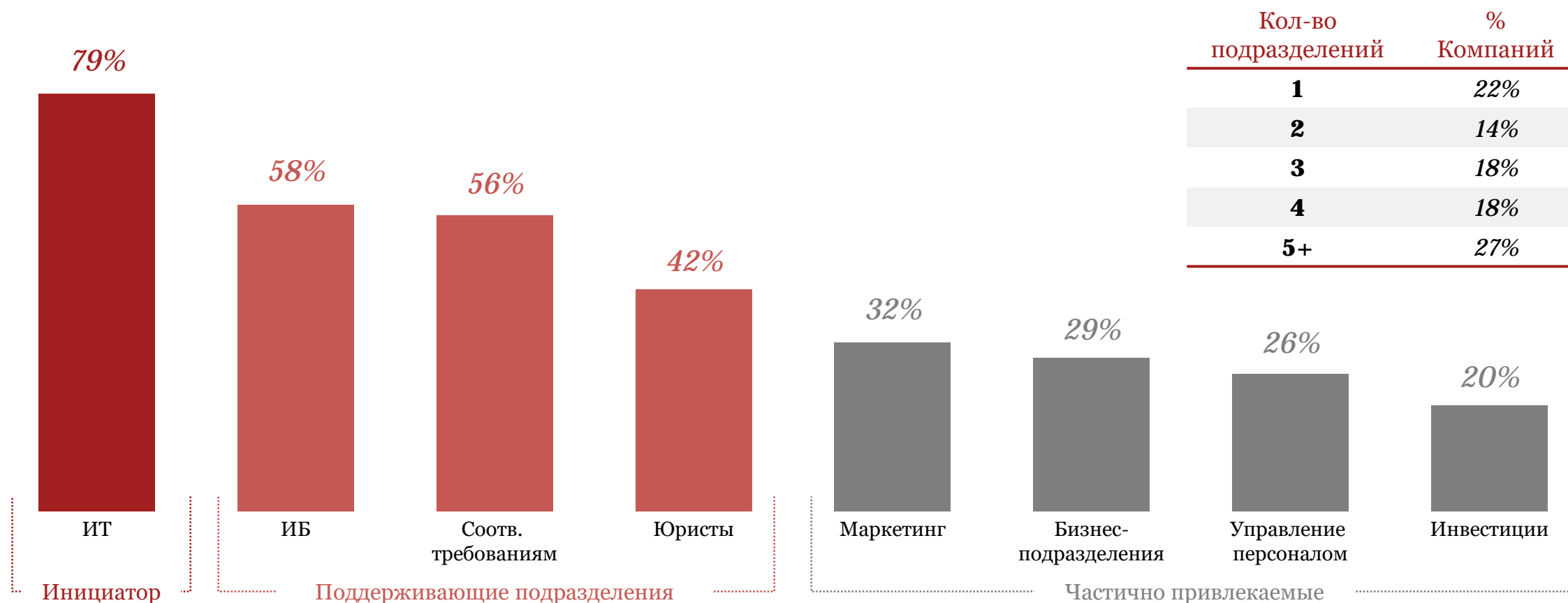
Оценка степени внедрения компонентов программы GDPR



*По данным опроса PwC *Pulse Survey: CEO involvement helps boost GDPR preparations*

- <https://www.pwc.com/us/en/cybersecurity/general-data-protection-regulation/pulse-survey-ceo-involvement.html>

Вовлеченность подразделений при внедрении требований GDPR



*По данным опроса PwC *Pulse Survey: CEO involvement helps boost GDPR preparations*

- <https://www.pwc.com/us/en/cybersecurity/general-data-protection-regulation/pulse-survey-ceo-involvement.html>

Распределение задач между подразделениями при внедрении требований GDPR

Команда приватности

- Определение общей стратегии выполнения требований GDPR.
- Координация инициатив по обеспечению конфиденциальности и выполнению требований GDPR от других ролей в бизнесе.
- Внедрение механизмов контроля и отчетности для постоянного соблюдения требований.

Безопасность и риски

- Выбор и реализация средств контроля безопасности и политик для выполнения стратегии реализации требований GDPR.
- Организация процессов и поддержка других команд в выявлении и классификации данных, а также оценки рисков.
- Применение технологий безопасности для постоянного мониторинга.

Маркетинг и другие бизнес-подразделения

- Идентификация обрабатываемых данных о потребителях, в т.ч. передаваемых третьим сторонам.
- Определение данных, подпадающих под требования GDPR и лиц, имеющих к ним доступ.
- Сбор и организации возможности анализа и пересмотра соглашений относительно обработки персональных данных с третьими сторонами и потребителями.

Взаимодействие с потребителями

- Разработка типовых уведомлений и соглашений с потребителями.
- Установление соответствия между потребителем и обрабатываемыми наборами данных о нем.
- Разработка соответствующих требованиям механизмов коммуникации с потребителями.

Управление персоналом

- Идентификация обрабатываемых данных о работниках, в т.ч. передаваемых третьим сторонам.
- Определение данных, подпадающих под требования GDPR и лиц, имеющих к ним доступ.
- Сбор и организации возможности анализа и пересмотра соглашений относительно обработки персональных данных с третьими сторонами и работниками.

ИТ

- Помощь другим командам в идентификации и классификации данных.
- Обеспечение технической возможности для выполнения требований GDPR.
- Применение установленных требований политик обеспечения безопасности данных.

Управление поставщиками\ закупками

- Сбор и обеспечение возможности доступа и пересмотра соглашений с третьими сторонами.
- Разработка требований по обеспечению соответствия GDPR для включения в соглашения с третьими сторонами.
- Разработка процесса выполнения регулярного аудита выполнения третьими сторонами требований соответствия GDPR.

Юристы

- Анализ и пересмотр соглашений с третьими сторонами.
- Анализ и пересмотр соглашений с потребителями и работниками организации.
- Поддержка других команд в разработке и выполнении стратегии соответствия требованиям GDPR.

**Forrester Research, Inc.*

Методологии внедрения GDPR

5

Методологии внедрению GDPR

Методология PwC (1/2)

Процессы и документы



- Анализ существующих процессов на соответствие требованиям GDPR
- Внедрение или трансформация процессов обработки и защиты персональных данных
- Пересмотр и актуализация имеющихся политик и процедур
- Обеспечения доступа к данным для заинтересованных сторон
- Организация возможности коммуникации с субъектами данных
- Организация возможности уведомления об утечках данных

Системы



- Реализация права субъекта на забвение (right to be forgotten)
- Реализация права на перенос данных (data portability)
- Внедрение принципа «Защищенности данных по умолчанию» (Privacy by default)
- Внедрение принципа «Предусмотренной защищенности данных» (Privacy by design)
- Совершенствование процедур управления доступом.

Персонал



- Обучение персонала правилам обработки и защиты персональных данных
- Назначение Директора по защите данных (Data privacy officer или DPO), наделение его необходимыми полномочиями и обеспечение постоянного повышения квалификации DPO.

Данные



- Реализация подходов обеспечения законности обработки данных
- Защита прав и интересов субъектов персональных данных
- Инвентаризация обрабатываемых данных и определению мест обработки и хранения данных.



Методологии внедрению GDPR

Методология PwC (2/2)

Безопасность



- Внедрение или усовершенствование организационных и технических мер по защите информации.
- Использование средств, обеспечивающих защиту от преднамеренных и непреднамеренных утечек информации, от неавторизованного доступа к бумажным носителям и элементам систем, от случайного или намеренного искажения или уничтожения обрабатываемых данных
- Оперативное реагирование на инциденты информационной безопасности, связанные с обработкой персональных данных

Третьи стороны

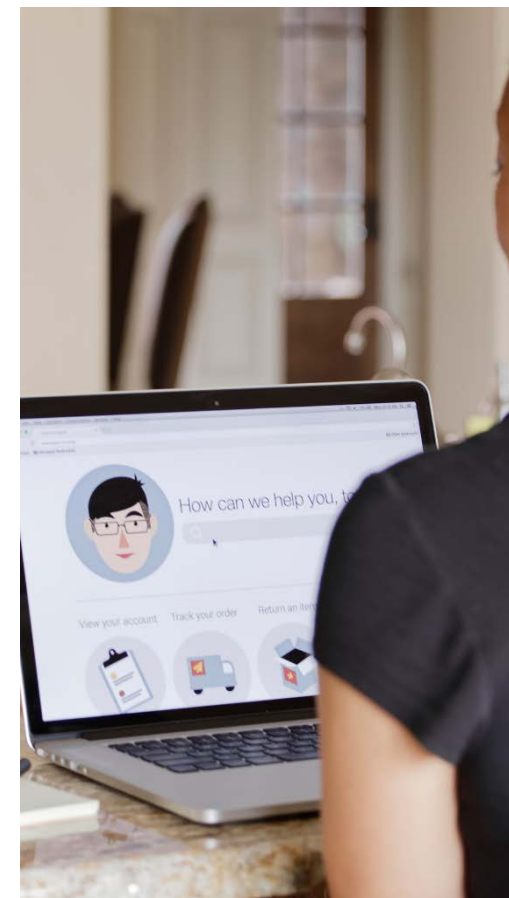


- Пересмотр, актуализация и учет требований GDPR в соглашениях с третьими сторонами
- Регулярный контроль и аудит исполнения требований GDPR третьими сторонами
- Учет требований GDPR при взаимодействии с потребителями

Лидерство



- Вовлечение руководства Компании для достижения положительных результатов при трансформации процессов обработки и защиты персональных данных.
- Осведомленность руководства о важности вопроса
- Своевременное принятие управленческих решений и выделение необходимых ресурсов.



Методологии внедрения *GDPR*

Модель зрелости Forrester



«Руководство» — определение подхода и стратегии защиты данных в соответствии с потребностями бизнеса, организация выделения ресурсов и реализации стратегии, оценка и контроль достижения целей.



«Технологии» — эффективная реализация стратегии защиты данных. Определение технических возможностей для защиты данных и управления доступом к данным. Управление сбором, обработкой **и хранением данных**.



«Процессы» — определение основных бизнес-процессов, необходимых для управления соблюдением конфиденциальности на протяжении всего жизненного цикла данных. Определение организационных и технологических мер контроля, которые помогают обеспечить конфиденциальность при работе с партнерами, правоохранительными органами и организациями за рубежом.



«Люди» — определение требований и ожиданий по защите данных от заинтересованных сторон, а также влияния на выполнение требований GDPR человеческих факторов.

**Forrester: The Framework For The Privacy Maturity Model*

GDPR: практика реализации требований
PwC

Июнь 2018
55

Методологии внедрения GDPR

Information Security Forum (ISF) GDPR Implementation guide

Люди, процессы и технологии

Требования GDPR затрагивает многие аспекты деятельности организации и эффективная программа реализации этих требований должна учитывать связи людей, технологий и процессов обработки данных. Подходы к обеспечению реализации требований в различных организациях могут отличаться в зависимости от специфики деятельности организации и интерпретации требований подразделением, которое является ответственным за их исполнение в организации.



*Information Security Forum (ISF) GDPR Implementation guide

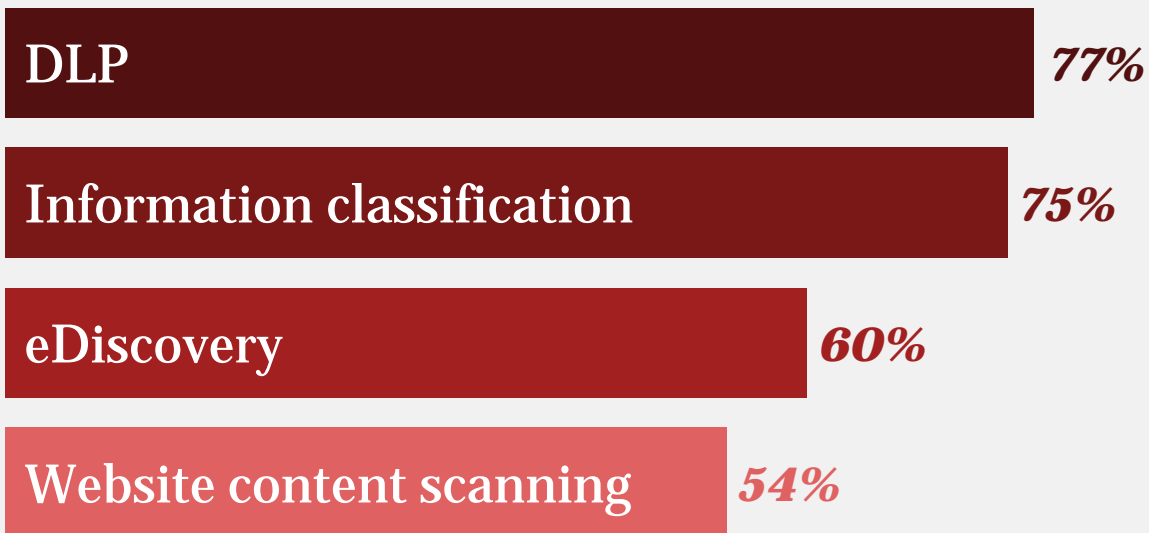
GDPR: практика реализации требо
PwC

Июнь 2018
56

Инструментарий внедрения **GDPR**

Значимость технологий обнаружений данных в проектах, связанных с GDPR

По версии участников Information Security Forum (ISF)*



*PwC является участником ISF с доступом ко всем материалам

Технологии обнаружения
данных



Компании, внедряющие
технологии защиты данных
в свои продукты



Рекомендуемые шаги

1

Применимость

- Проанализировать существующие бизнес-процессы компании и потоки данных. Выявить обработку персональных данных лиц, находящихся в ЕС, проанализировать применяемые для обработки персональных данных технологии.
- Определить область применения GDPR.

2

GAP Анализ

- Выявить какие процессы и системы требуют изменения для соответствия к GDPR;
- Определить потенциальные риски, связанные с GDPR;
- Проанализировать риски и определить их приоритетность.
- Разработать общую дорожную карту по приведению деятельности Компании в соответствие с требованиями GDPR.

3

Планирование

- Сформировать детальный план действий, необходимых для приведения процессов в соответствие с требованиями GDPR;
- Определить необходимые ресурсы для проведения трансформации, ответственных за трансформацию лиц, а также осуществить приоритизацию выполнения задач и согласовать сроки выполнения со всеми заинтересованными сторонами.

4

Исполнение

- Спроектировать и реализовать внедрение организационных мер, необходимых для соответствия GDPR;
- Обеспечить вовлеченность всех заинтересованных сторон в трансформацию процессов.

5

Поддержка

- Проводить регулярные повторные GAP-анализы с заранее определенной периодичностью и комплексностью.

Рекомендации по организации внедрения GDPR

Перед тем, как начать...

- **Включите GDPR в верхнюю часть приоритетов организации.**

Узнайте от бизнес-лидеров какое значение обработка персональных данных имеет для бизнеса организации. Вынесите вопросы GDPR на заседание совета директоров и продемонстрируйте ценность выполнения требования для бизнеса. Используйте бизнес-кейсы, тематические исследования и результаты сравнительного анализа, чтобы помочь сдвинуть взгляды руководителей с минимальных уровней соответствия и продемонстрировать конкурентные преимущества от соответствия требованиям GDPR.

- **Создавайте команды, которые ориентированы на взаимодействие с другими подразделениями.**

Вовлеченность в процесс реализации требований GDPR бизнес-подразделений поможет сфокусироваться на выполнении необходимого набора релевантных требований и избежать излишнего расходования ресурсов.

- **Расширяйте свое видение того, какие преимущества получает организация при реализации требований GDPR.**

Используйте информацию по отрасли и примеры успешной реализации требований GDPR.



Вопросы?



Роман Чаплыгин

PwC, Директор,
Кибербезопасность и непрерывность бизнеса

+7 (903) 272 1620

roman.chaplygin@ru.pwc.com

PwC в России (www.pwc.ru) предоставляет услуги в области аудита и бизнес-консультирования, а также налоговые и юридические услуги компаниям разных отраслей. В офисах PwC в Москве, Санкт-Петербурге, Екатеринбурге, Казани, Новосибирске, Ростове-на-Дону, Краснодаре, Воронеже, Владикавказе и Уфе работают более 2 500 специалистов. Мы используем свои знания, богатый опыт и творческий подход для разработки практических советов и решений, открывающих новые перспективы для бизнеса.

Под «PwC» понимается сеть PwC и/или одна или несколько фирм, входящих в нее, каждая из которых является самостоятельным юридическим лицом. Глобальная сеть PwC объединяет более 236 000 сотрудников в 158 странах. Более подробная информация представлена на сайте <http://www.pwc.ru/ru/about.html>