

www.pwc.ru

Важен ли GDPR российским банкам? Как российским компаниям подготовиться к GDPR и что будет за невыполнение?

Ноябрь 2018 г.



pwc

- Новые требования, единые для стран ЕС и компаний, работающих на рынке ЕС
- Защищаются права субъектов, находящихся в ЕС (не только граждан)

В мире:



Facebook

Facebook заявил о планах реализовать меры защиты данных клиентов по GDPR по всему миру, а не только в Европе

Microsoft

Microsoft заявил о защите прав субъектов данных по всему миру на уровне, требуемом GDPR

Apple

Apple реализовал GDPR для Европы и планирует сделать это для клиентов по всему миру в ближайшие месяцы

SAP

SAP реализовал функциональность для соответствия GDPR в своих продуктах

В России:



Сбербанк

Сбербанк опубликовал информацию о соответствии GDPR обработки данных клиентов на своём вебсайте

Яндекс

Яндекс опубликовал информацию о соответствии сервиса Яндекс.Метрика требованиям GDPR

РЖД

РЖД запрашивает при регистрации на вебсайте согласие клиентов на обработку данных по GDPR

1. Определить применимость GDPR

1

Реальная деятельность в ЕС через постоянную структуру или случай совместных контролеров



Триггеры применимости*

- » Единая система оценки KPI работников
- » Единая адресная книга (Outlook, Intranet portal)
- » CRM/КУС общие базы ПД, АСУ и т.п.

Например, российская компания, которая:

- обрабатывает ПД в связи с деятельностью **филиала** в ЕС (общая CRM система, система оценки KPI работников, т.п.)
- имеет **агента** в ЕС (взыскание задолженности, заключение договоров, иное представительство)
- сотрудничает с партнёром в ЕС, который, например, продвигает услуги, обрабатывает ПД контрагентов

* Примеры факторов, которые могут свидетельствовать о применимости GDPR к компании. Для точного определения того применим ли GDPR необходим детальный анализ процессов и информационных систем компании.

GDPR | Важен ли GDPR российским банкам?

PwC

1. Определить применимость GDPR

2 Направленность деятельности на ЕС

Предложение услуг в ЕС

- Язык сайта при оказании услуг
- Валюта платежей
- Таргетирование и ссылка на наличие клиентов в ЕС
- ???

и/или

Мониторинг поведения в ЕС

- Отслеживание в Интернете
- Постоянные cookie-файлы
- Создание профиля по активности пользователя
- ???



Триггеры применимости*

- » Cookie-файлы и IP-адрес
- » Программы лояльности
- » On-line кабинеты
- » Системы безопасности (antifraud)
- » Продвижение сайта для ЕС
- » Трекинг геопозиции смартфона
- » Обучение, конференции, форумы с участием лиц из ЕС

Например, российская компания, которая:

- предлагает находящимся в ЕС лицам товары и услуги через сайт или почтовую рассылку (**банки, отели, турфирмы, магазины**)
- ведёт мониторинг находящихся в ЕС лиц (**мобильные приложения ДБО, страхование, «умные» устройства**)
- создает профили пользователей вебсайта, в т.ч. с использованием cookies и метрик, предоставляемых третьими сторонами

* Примеры факторов, которые могут свидетельствовать о применимости GDPR к компании. Для точного определения того применим ли GDPR необходим детальный анализ процессов и информационных систем компании.

GDPR | Важен ли GDPR российским банкам?

PwC

Применимость GDPR к системам в российских компаниях



1. Определить применимость GDPR

Если GDPR **не** применим к компании

- задокументировать объем (процессы, системы, продукты) и результаты анализа о применимости GDPR
- подготовить коммуникацию для партнеров, контрагентов и клиентов в ЕС о неприменимости GDPR
- принять методологию оценки новых продуктов, изменений бизнес-процессов и ИТ-архитектуры на применимость GDPR



1. Определить применимость GDPR






2. Привести в соответствие с требованиями GDPR














GDPR vs 152-ФЗ: принципы обработки данных

	152-ФЗ
Трактовка термина «персональные данные»	
Законность и 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 (DPO)	>	

 соответствует  частично соответствует  не соответствует

GDPR | Важен ли GDPR российским банкам?

PwC

GDPR vs 152-ФЗ: ключевые требования к согласию 152-ФЗ

Свободное, конкретное, информированное, непротиворечивое	>	
Отсутствие необходимости письменной формы	>	
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

Учёт обработки (record-keeping)

Контролер обязан документировать:

- цели обработки
- категории субъектов и данных
- категории получателей
- способы обработки
- трансграничную передачу и принимаемые меры безопасности
- сроки хранения
- технические и организационные меры безопасности данных

Обязанности документирования есть и у **обработчика**, но в меньшем объеме.

The screenshot displays a complex spreadsheet template for GDPR record-keeping. It includes sections for 'Name and contact details', 'Data Protection Officer (DPO) details', and 'Representative (if applicable)'. The main body of the template is divided into columns for 'Business Function', 'Purpose of processing', 'Description of processing', 'Data categories', 'Data subjects', 'Data retention', and 'Data security'. The template is designed to be filled out with specific details for each data processing activity, ensuring compliance with GDPR requirements.

Учет ведется в **письменной и электронной** форме.

Материалы предоставляются **регулятору** по его требованию.

Сообщение об инцидентах 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, которые могут возникнуть в результате инцидента;
- Принятые/предлагаемые меры для решения проблемы (*например, рекомендации гражданину*);
- Контактное лицо контролера *по вопросам инцидента*.

Законопроект № 416052-6

- обязанность уведомлять Роскомнадзор в случае неправомерного раскрытия ПД неограниченному кругу лиц

Доступ к персональным данным

	<i>Raw data</i>	<i>Data portability</i>
Требование:	Предоставить копию ПД	<ul style="list-style-type: none">• Предоставить копию ПД• Передать другому контролёру
Объем ПД:	Обрабатываемые контролёром	Предоставленные субъектом контролёру
Формат ПД:	Широко используемый формат	<ul style="list-style-type: none">• Структурированные ПД• Широко используемый формат
Условия:		<ul style="list-style-type: none">• Обработка по согласию / договору• Автоматизированная обработка

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 ПД 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 взаимодействует с властями ЕС и гражданами
- **Привлекается к ответственности за нарушения контролера/обработчика**

Как назначить ответственного за защиту персональных данных (DPO)?

Может находиться
не в ЕС

Подчиняется
первому лицу

Может быть
внешним
сотрудником

Один на несколько
компаний

Защищен от
конфликтов
интересов и
влияния

Специальные
знания GDPR

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

1. 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)?

2. 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)?

3. Обработка больших объемов данных о судимости и правонарушениях

Данные о
правонарушениях



Данные об уголовных
приговорах



Данные о нарушении
правил безопасности



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

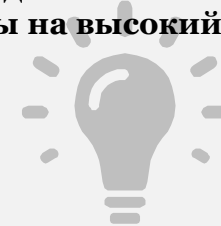
Принцип «Privacy by default»



- 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.
- Установка высокого уровня приватности по умолчанию может снизить маркетинговые возможности компании.

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

Также ограничение доступа и настройки безопасности по умолчанию должны быть установлены на высокий уровень



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

Принцип «Privacy by design»



- Принцип призван решить проблему «недалековидности» организаций в начале сбора персональных данных.
- Следуя этому принципу, организации должны продумывать риски и 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 проверять свидетельства того, что вопросы приватности и безопасности данных были рассмотрены уже на этапе планирования изменений.

Принцип должен соблюдаться как контролером, так и обработчиком.



Data protection impact assessment (DPIA)

Оценка
воздействия на
защищенность
персональных
данных



- Вопрос необходимости проведения DPIA тесно связан с принципом Privacy by Design и проектным управлением.
- Обязательно нужно проводить при скоринге, мониторинге публичных мест, при 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*).
- Контролер также 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.

Европейские регуляторы разъясняют: для оценки необходимости DPIA необходимо провести качественную оценку рисков в процессах обработки персональных данных.



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**.



Ресурсы:

Штат регулятора в зависимости от страны составляет от 10 до 200 человек.

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*

Штрафы: практика за первый месяц

Известные судебные иски



25 мая



3,9 млрд

Три иска к **Facebook, WhatsApp и Instagram** через регуляторов в Австрии, Бельгии и Гамбурге на общую сумму в **3,9 миллиарда евро**.



25 мая



3,7 млрд

Иск к **Google** через регулятора во Франции на **3,7 миллиарда евро**, по поводу нарушений в ОС Android.



Иски направлены в день вступления в силу GDPR активистом Максом Шремсом.

Решение регулятора на текущий момент не известно.

Известные Штрафы



17 июля: штраф в размере 400 000 Евро для португальской больницы за избыточные права доступа персонала к данным пациентов.

Количество жалоб:



В разных странах только за первый месяц действия GDPR регуляторы получили от нескольких штук (Швеция, Бельгия, Словакия) до нескольких сотен жалоб (Чехия, Ирландия, Франция)

GDPR vs. PKH

?

Необходимо учитывать при внедрении групповых политик в РФ

- обязанность получения **письменного** согласия субъектов (решения на основании автоматизированной обработки, трансграничная передача и т.п.)
- живые и **мертвые...**
- требования к **поручению на обработку** ПД
- статус: **оператор vs. обработчик**
- **отсутствие** аналога EU Model Contractual Clauses *
- различия в списках **стран с адекватной защитой**
- обезличивание (**анонимизация**) – ограничение для бизнеса
- грядущие изменения в связи с обновлением Евроконвенции

*** Законопроект № 416052-6**

возможность обеспечения адекватной защиты данных стандартными условиями договора, утвержденными Роскомнадзором

Сложности при внедрении соответствия GDPR в РФ



Определение статуса учреждений (establishment) в ЕС (дочерние компании с малой долей владения, компании-посредники, действующие в ЕС сотрудники/подразделения российской компании)



Определение роли материнского юр. лица в России (Отдельный контролер? Совместный контролер? Обработчик?) по отношению к данным, передаваемым из европейского юр. лица группы



Обоснование трансграничной передачи в Россию, если данные получены европейским юр. Лицом (Россия для ЕС не считается страной, обеспечивающей адекватную защиту прав субъектов)



Координация всех линий бизнеса для определения применимости GDPR к системам, используемым сразу несколькими дочерними юр. лицами/направлениями (кто и какие данные заносит в систему?)



Донести до руководства компании кардинальные (вплоть до несовместимости) различия между ролью DPO и ролью ответственного за обработку ПДн



Различия в трактовках текста GDPR и связанного с ним законодательства в разных странах ЕС, в которых компания осуществляет деятельность, в том числе из-за неточностей перевода



Неготовность российских компаний к обязательному раскрытию данных об утечках



Переход от сбора согласий «по умолчанию» на все операции к определению других оснований для обработки (в т. ч. законных интересов) и получению согласий только для особых случаев обработки

Секция вопросов

Станислав Никитин, CRISC, CIPP/E
PwC, Кибербезопасность, Менеджер
+7 (903) 961-28-92
Stanislav.Nikitin@pwc.com

Цель данной презентации – дать общее представление о рассматриваемых в нём вопросах, презентация не является профессиональной консультацией. Не следует предпринимать каких-либо действий на основании информации, содержащейся в этой презентации, без предварительного обращения к профессиональным консультантам. В отношении точности или полноты информации, содержащейся в настоящей презентации, не дается никаких заверений или ручательств (явно выраженных или подразумеваемых), и в той степени, в какой это допустимо законодательством, фирма PwC, её участники, сотрудники и представители не берут на себя никакой ответственности и снимают с себя всякую ответственность за последствия ваших или чьих бы то ни было действий или бездействия исходя из достоверности содержащейся в настоящей презентации информации и за любое основывающееся на ней решение.