

# *GDPR:*

## Что нужно знать российскому бизнесу?

12 сентября 2017



# Предпосылки GDPR



**Big Data  
IoT**



**Data  
privacy**



**Digitalization  
& globalization**

# Развитие регулирования

**2018**

Действие  
GDPR

**2016**

Принятие  
GDPR

**1981**

Страсбургская  
конвенция

**1995**

Директива  
95/46/ЕС

# Применение GDPR



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



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



- Страны ЕС
- Субъекты персональных данных (ПД) – лица в ЕС
- Контролёры и процессоры – экстерриториальное применение

# Применение GDPR



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



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



- Страны ЕС
- Субъекты персональных данных (ПД) – лица в ЕС
- Контролёры и процессоры – экстерриториальное применение

# Применение GDPR



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



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



- Страны ЕС
- Субъекты персональных данных (ПД) – лица в ЕС
- Контролёры и процессоры – экстерриториальное применение

# Кто должен соблюдать GDPR в России?

## 1. Реальная деятельность в ЕС через постоянную структуру

**Например, российская компания, которая:**

- обрабатывает данные в связи с деятельностью своего **филиала** в ЕС
- поручила обработку данных **дочерней компании** в ЕС (турагент)
- имеет **агента** в ЕС (судебное представительство, взыскание задолженности, т.п.)
- определяет цели/способы обработки **совместно** с компанией из ЕС (**совместный контролёр**)

# Кто должен соблюдать GDPR в России?



## 2. Направленность деятельности на ЕС



### Предложение товаров/услуг в ЕС

- Язык сайта при заказе
- Валюта платежей
- Таргетирование и указание потребителей в ЕС
- ???

### Мониторинг поведения в ЕС

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

# Кто должен соблюдать GDPR в России?



## 2. Направленность деятельности на ЕС



**Например, российская компания, которая:**

- предлагает резидентам ЕС бесплатные услуги через сайт с хостингом в России (**социальные сети**)
- предлагает резидентам ЕС платные услуги через сайт с хостингом в России (**онлайн-игры**)
- отслеживает запросы пользователей (в том числе из ЕС) с помощью cookie-файлов для таргетированной рекламы
- принимает оплату от резидентов ЕС в Евро (**онлайн-кинотеатры**)



# Требования GDPR






# GDPR vs 152-ФЗ: принципы обработки данных

	152-ФЗ
Законность и справедливость, понятность процессов гражданину	
Точность и актуальность данных	
Обработка только для заявленных целей	
Отсутствие избыточных данных	
Ограниченный срок сохранения	
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	
Назначать ответственного за защиту данных	

 соответствует  частично соответствует  не соответствует

# Требования GDPR – на что обратить внимание?



---

## *Требования GDPR – на что обратить внимание?*

Переносимость данных

**Штрафы**

**Согласие**

**Представитель в ЕС**

**Право на забвение**









Принятие решений на основании автоматической обработки




**Полномочия регуляторов**

**Извещение о проблемах с данными**

**Privacy by design and default**

## 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 получения онлайн услуг	
Отозвать также просто, как и получить	
Контролер должен доказать получение согласия	

 соответствует  частично соответствует  не соответствует

# Сообщение о проблемах с данными



## Содержание сообщения:

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



# 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
- Данные защищены так, что не могут быть прочтены посторонним лицом
- Приняты меры, не дающие риску материализоваться
- Было публичное сообщение о проблеме, т.к. тяжело разослать индивидуальные сообщения

# Право на удаление данных (право на забвение)



**Требование должно быть исполнено, если:**

- Выполнены цели обработки
- Отозвано согласие
- Данные получены незаконно
- Есть обязанность удаления данных по праву ЕС
- *Н.В! Данные получены от ребёнка для оказания онлайн услуг*
- *Н.В! Гражданин возражает против дальнейшей обработки и нет правовых оснований для отклонения этого возражения*

# 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** персональных данных.
- Получение **своих** персональных данных.
- **Предоставленных** субъектом контролёру.
- **Формат.**
- Передача **другому контролёру.**
- **Отсутствие препятствий.**
- Данные, обрабатываемые на основании **согласия или договора.**
- **Автоматизированная** обработка.

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

## 1. Регулярное систематическое наблюдение в больших объёмах

Услуги сотовой связи и Интернета



Трекинг местонахождения



Видеомониторинг



Программы лояльности



Поведенческая реклама



Создание профилей и скоринг для оценки рисков



Мониторинг через «умные» устройства



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

## 2. Обработка больших объёмов специальных категорий ПД

Медицинские организации



Пациентские организации



Страховые компании



Банки?



Профсоюзы



Сервисы поиска людей по  
фотографиям



Основанные на биометрии  
системы доступа



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

## 3. Обработка больших объемов данных о судимости и правонарушениях

Детективные  
агентства



Сервисы поиска  
данных о  
неоплаченных  
штрафах



Страховые  
компании в сфере  
автострахования



## ***Как назначить ответственного за защиту персональных данных (DPO)?***

***Может ли находиться не в ЕС?***

***Кому подчиняется?***

***Сотрудник контролёра/ обработчика?***

***Один на несколько компаний?***

***Кто даёт ему указания?***

***Какими знаниями должен обладать?***

# Принятие юридически значимых решений исключительно на основе автоматической обработки данных

## Возможные случаи

GDPR

vs.

152-ФЗ

- Разрешено правом ЕС или страны ЕС, к которой относится контролёр
- Явно выраженное согласие гражданина
- ***NB!** Для заключения или исполнения договора гражданина с контролёром*

- Разрешено законами РФ
- Письменное согласие



# Принятие юридически значимых решений исключительно на основе автоматической обработки данных

Контролёр должен обеспечить

GDPR

vs.

152-ФЗ

для согласия и договоров

- *NB! Получение объяснения принятого решения*
- *NB! Выражение своей точки зрения гражданином*
- Оспаривание принятого решения
- *NB! Человеческое вмешательство со стороны контролёра*

всегда

- Разъяснение порядка принятия и последствия решения
- Разъяснение порядка защиты прав
- Возможность заявить возражения

# 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
- Обработка, не требующая идентификации
- Privacy by design and by default
- Совместный контроль ПД
- Назначение представителя в ЕС
- Обязанности обработчика и действия согласно указаниям контролёра
- Документирование обработки ПД
- Сотрудничество с надзорным органом
- Требования к безопасности ПД
- Сообщение об утечке ПД надзорному органу и субъекту ПД
- Предварительная оценка влияния на защиту ПД
- 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
- 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 авт. обработки

## Нарушения при передаче данных из ЕС

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

\*Выручка по всему миру за предшествующий финансовый год

# Как применяются штрафы?

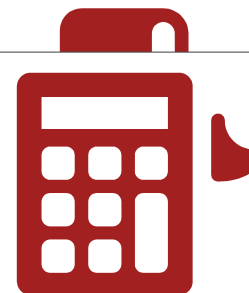
## Основные правила

**1** Штраф может не применяться

**2** Штраф должен быть **действенным, соразмерным и вразумляющим**

**3** Может быть наложен **в дополнение или вместо** других мер

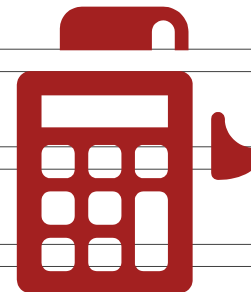
**4** За нарушение нескольких положений GDPR по одной или связанным операциям размер штрафа не должен превышать максимального для самого тяжёлого нарушения.



# Как применяются штрафы?

## Что будет учтено при определении размера?

- 1 Природа, тяжесть и продолжительность нарушения;
- 2 Число затронутых лиц и масштаб причинённого им вреда;
- 3 Совершено нарушение умышленно или по неосторожности;
- 4 Принятие мер по снижению последствий нарушения;
- 5 Предшествующие схожие нарушения;
- 6 Выдавались ли требования по тому же вопросу;
- 7 Уровень сотрудничества с регулятором для устранения нарушения и снижения негативного эффекта;
- 8 Доходы (снижение убытков), полученные от нарушения.



# Спасибо!



## **Евгений Гук**

Руководитель практики по интеллектуальной собственности, информационным технологиям и защите данных

*Тел. +7 (495) 967-6000, доб.4961  
evgeniy.gouk@ru.pwc.com*



## **Артем Дмитриев**

Старший юрист  
Практика по интеллектуальной собственности, информационным технологиям и защите данных

*Тел. +7(495) 967-6000, доб.4315  
artem.y.dmitriev@ru.pwc.com*

---

***www.pwclegal.ru***

**PwC Legal**  
**20 лет**  
успешной  
работы в России

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.

**PwC Legal** ([www.pwclegal.ru](http://www.pwclegal.ru)) – международная юридическая фирма, объединяющая более 2 500 юристов в 85 странах мира. В российских офисах фирмы – в Москве и Санкт-Петербурге – работают более 80 квалифицированных юристов, прошедших обучение в России и за рубежом. PwC Legal в России рекомендована ведущими рейтингами: Legal 500, Chambers&Partners, Best Lawyers International, «Право.Ru» и «Коммерсант».

© 2017 Общество с ограниченной ответственностью «ПрайсвотерхаусКуперс Юридические Услуги». Все права защищены. Под «PwC» понимается Общество с ограниченной ответственностью «ПрайсвотерхаусКуперс Юридические Услуги» или, в зависимости от контекста, другие фирмы, входящие в глобальную сеть PricewaterhouseCoopers International Limited (PwCIL). Каждая фирма сети является самостоятельным юридическим лицом.