



# Генеральный регламент о защите персональных данных

—

Андрей Дроздов, CISA, CISM, CGEIT

# Несколько слов о GDPR



Генеральный регламент о защите персональных данных (GDPR) отменяет действие Директивы ЕС о защите данных 95/46/ЕС и предназначен:

- ✓ для унификации законов по защите данных, принятых в странах ЕС;
- ✓ для защиты ПДн и расширения прав на конфиденциальность ПДн всех граждан ЕС;
- ✓ для изменения мер, принятых организациями ЕС в целях защиты ПДн субъектов.

**GDPR вступает в силу 25 мая 2018 года**

GDPR является законом прямого действия и относится ко всем организациям, обрабатывающим ПДн субъектов ПДн в ЕС, вне зависимости от месторасположения организации.

**GDPR применим к следующим организациям:**

**1. организациям, учреждённым в ЕС и являющимся операторами\* (controllers) и/или обработчиками (processors) ПДн**

к организациям, не учреждённым в ЕС и являющимся операторами (controllers) и/или обработчиками (processors) ПДн, и вид деятельности которых связан с

**2. предоставлением товаров или сервисов гражданам ЕС**

**3. мониторингом поведения субъектов ПДн в пределах ЕС**

\*Здесь и далее представлен перевод терминов из GDPR, который не является официальным

# Что можно отнести к персональным данным?

**Персональные данные** – любая информация, относящаяся к физическому лицу или к «субъекту данных», которая может быть использована прямо или косвенно для определения физического лица.



# Что подразумевается под обработкой персональных данных?

## Законодательство

**Обработка ПДн** – любое действие, совершаемое с ПДн с использованием или без использования средств автоматизации, включая сбор, использование, запись и т.д.

*Операции, совершаемые с ПДн:  
ручные или автоматизированные*

- сбор,
- запись,
- организация,
- структурирование,
- хранение,
- адаптация или изменение,
- восстановление,
- консультация,
- использование,
- раскрытие при передаче,
- распространение или обеспечение доступности,
- группировка или комбинация,
- ограничение,
- стирание или уничтожение

## Обработка

## Примеры

*Несколько примеров обработки ПДн:*

- удаленный доступ или доступ только на чтение;
- хранение ПДн без совершения других действий с ПДн;
- Обработка ПДн с использованием средств автоматизации без привлечения человека;
- использование псевдонимизированных данных

# Ключевые моменты GDPR



# Основные принципы обработки персональных данных



Законность,  
справедливость и  
понятность процессов  
обработки ПДн в  
отношении субъектов ПДн



Ограничение обработки  
ПДн в соответствии с  
целями обработки



Снижение избыточности  
обрабатываемых ПДн



Обеспечение точности и  
актуальности  
обрабатываемых ПДн



Ограничение времени  
хранения ПДн



Обеспечение целостности  
и конфиденциальности  
обрабатываемых ПДн

# Ключевые изменения, внесенные GDPR



## Штрафы

Многоуровневая система штрафов в зависимости от тяжести нарушения.  
Уровень 1 → **2% от глобального оборота** или €10M (что выше).  
Уровень 2 → **4% глобального оборота** или €20M (что выше)



## Офицер безопасности данных (DPO)

**Наличие DPO** в государственных структурах и организациях, осуществляющих **широкомасштабные наблюдения (исследования)** или **широкомасштабную обработку специальных категорий ПДн**



## Расширение прав контролирующих органов

Передача **широких полномочий** контролирующим органам: SAs (supervisory authority), ведущему контролирующему органу (lead supervisory authority), Совету ЕС по защите данных



## Инвентаризация

Проведение организациями инвентаризации информационных активов



## Уведомление об утечках

Предоставление регулятору и в дальнейшем субъекту ПДн отчетов об утечках данных в течение 72 часов с момента регистрации инцидента



## Безопасность

**Особые требования** в части мониторинга, шифрования и обезличивания



## Оценка воздействия на конфиденциальность (PIAs)

Требование к проведению PIAs организациями, деятельность которых является высокорискованной



## Права субъектов ПДн

Расширение прав до **права на перенос ПДн, права на удаление ПДн и права на доступ к ПДн**



## Специальные категории ПДн

Добавление **биометрических и генетических данных**



## Согласие

Требование к получению понятных и детальных **согласий на обработку ПДн**



## Обработчики данных

Требования к **обработчикам ПДн**. Операторы ПДн должны проводить надлежащую проверку обработчиков ПДн



## Проектируемая конфиденциальность

Соблюдение требований по ИБ при проектировании ИТ-решений

# Нарушения и штрафы

€ 20 000 000  
или  
4%

## За нарушение

- Основных принципов обработки ПДн, определенных в статьях **5, 6, 7 и 9**;
- Прав субъекта ПДн, определенных в статьях **12 – 22**;
- Порядка передачи ПДн за пределы ЕС и в международные страны, определенных в статьях **44, 45**;
- Обязательств стран-членов ЕС, определенных в главе **IX**;
- Требований контролирующих органов (supervisory authority), определенных в статьях **58(1) и 58(2)**

## За нарушение

- Обязанностей оператора и обработчика, определенных в статьях **8, 11, 25 – 39, 42 и 43**;
- Обязанностей органа сертификации, определенных в статьях **42 и 43**;
- Обязанностей органа мониторинга, определенных в статье **41(4)**

€ 10 000 000  
или  
2%

1

Для организаций, являющихся **операторами ПДн** и учреждённых более, чем в одном государстве-члене ЕС, местом основного учреждения (main establishment) будет являться место расположения центральной администрации в ЕС или место, где принимаются решения в отношении целей и средств обработки ПДн.

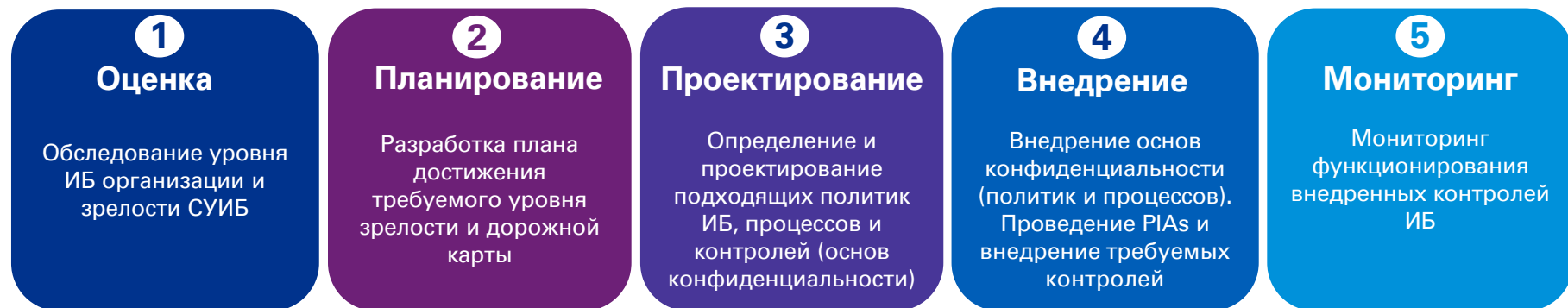
2

Для организаций, являющихся **обработчиками ПДн** и учреждённых более, чем в одном государстве-члене ЕС, местом основного учреждения будет являться место расположения центральной администрации в ЕС или место, осуществления основной деятельности по обработке ПДн (в случае, если у обработчика не предусмотрена центральная администрация).



# Какие дальнейшие шаги?

## Этапы. Программа защиты ПДн

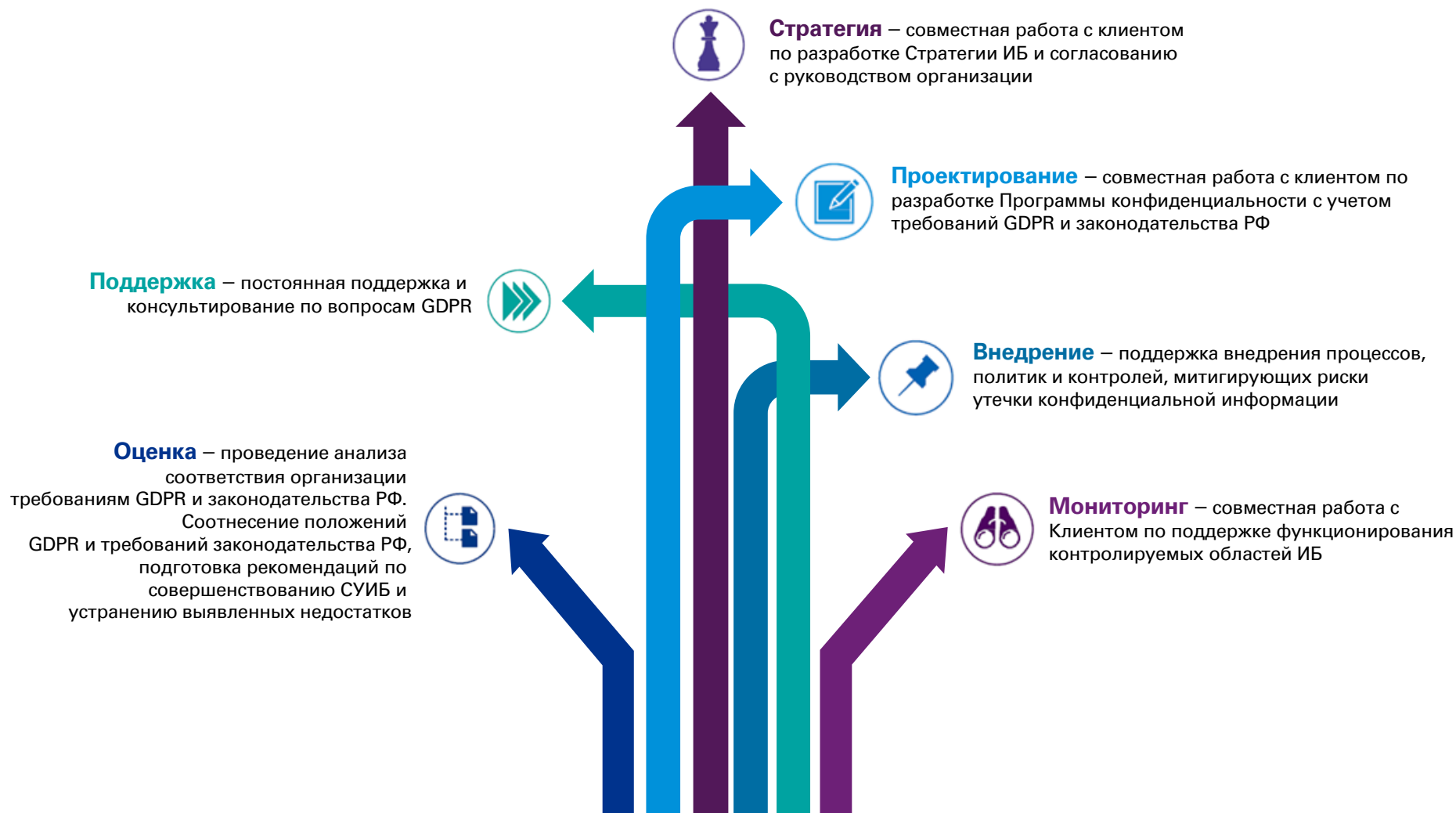


ISO 27001, SOC 2, SOC 3,  
регламенты проверок регуляторов (SAs)

## Примеры важных направлений по защите ПДн



# Как КПМГ может помочь?





# Спасибо!



## Илья Шаленков

Старший менеджер,  
Управление информационными рисками  
КПМГ Россия, Москва

+7 (495) 937-44-77  
[asksecurity@kpmg.ru](mailto:asksecurity@kpmg.ru)  
[www.kpmg.ru](http://www.kpmg.ru)



## Андрей Дроздов

Старший менеджер,  
Управление информационными рисками  
КПМГ Россия, Москва

+7 (495) 937-44-77  
[asksecurity@kpmg.ru](mailto:asksecurity@kpmg.ru)  
[www.kpmg.ru](http://www.kpmg.ru)



## Кристина Боровикова

Старший консультант,  
Управление информационными рисками  
КПМГ Россия, Москва

+7 (495) 937-44-77  
[asksecurity@kpmg.ru](mailto:asksecurity@kpmg.ru)  
[www.kpmg.ru](http://www.kpmg.ru)



[kpmg.ru](http://kpmg.ru)



[kpmg.com/app](http://kpmg.com/app)

Информация, содержащаяся в настоящем документе, носит общий характер и подготовлена без учета конкретных обстоятельств того или иного лица или организации. Хотя мы неизменно стремимся представлять своевременную и точную информацию, мы не можем гарантировать того, что данная информация окажется столь же точной на момент получения или будет оставаться столь же точной в будущем. Предпринимать какие-либо действия на основании такой информации можно только после консультаций с соответствующими специалистами и тщательного анализа конкретной ситуации.

© 2017 АО «КПМГ», компания, зарегистрированная в соответствии с законодательством Российской Федерации, член сети независимых фирм КПМГ, входящих в ассоциацию KPMG International Cooperative (“KPMG International”), зарегистрированную по законодательству Швейцарии. Все права защищены.