KPMG

Общий регламент о защите данных (General Data Protection Regulation, GDPR). Его влияние на деятельность финансовых институтов

Справочная информация

Защита данных клиентов - физических лиц

Более надежные отрасли

41%
Банки

33%
Органы местного самоуправления

36%
Правоохранительные органы

39%
Здравоохранение

23%
Коммунальные предприятия

Менее надежные отрасли

21%
Технологии

14%
Ритейл

17%
Супермаркеты

14%
Игры

13%
Социальные сети

Глобальные перспективы

Более 50% респондентов поделились бы данными об образовании и этнической принадлежности онлайн

Менее 20% респондентов раскрыли бы информацию об истории поиска в сети Интернет, о доходах, местоположении, адресе или медицинских данных

55% респондентов не осуществляют онлайн покупки через сайты, не обеспечивающие должный уровень защиты данных

Респонденты большинства стран считают, что обеспечение защиты данных людей важнее, чем удобство

По мнению большинства респондентов, социальные сети, игровые и развлекательные компании обрабатывают избыточное количество данных

По мнению **75%** респондентов, их данные были переданы третьим лицам

Источник: KPMG Crossing the line, Consumer Data Privacy Survey

Несколько слов о GDPR

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Общий регламент о защите персональных данных (GDPR) отменяет действие Директивы ЕС о защите данных 95/46/ЕС (которая в свою очередь основана на Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 г.) и предназначен:

- ✓ для унификации законов по защите данных, принятых в странах ЕС;
- ✓ для защиты ПДн и расширения прав всех субъектов ПДн в ЕС;
- ✓ для совершенствования мер защиты ПДн субъектов ПДн в ЕС.

GDPR вступил 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.

Если оператор и обработчик не представлен в ЕС, может потребоваться назначение представителя

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 субъектам персональных данных в ЕС

3. мониторингом поведения субъектов ПДн в пределах ЕС

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

Ключевые для Российских организаций статьи GDPR

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 27

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

Важные положения GDPR

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity

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.

Обработка

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

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

Основные принципы обработки ПДн

Законность, справедливость, понятность

Обработка ПДн должна осуществляться на законной и справедливой основе

Ограничение обработки ПДн в соответствии с целями обработки

Обработка ПДн должна ограничиваться достижением конкретных, определенных и законных целей

Снижение избыточности обрабатываемых ПДн

Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки

Обеспечение точности и актуальности обрабатываемых ПДн

При обработке ПДн должны быть обеспечены точность и актуальность ПДн

Ограничение времени хранения ПДн

Хранение ПДн должно осуществляться не дольше, чем этого требуют цели обработки

Обеспечение безопасности обрабатываемых ПДн

Отчетность

Все операторы и обработчики ПДн должны продемонстрировать соответствие принципам обработки ПДн

Права субъектов ПДн

Ключевые моменты GDPR

Ключевые изменения, внесенные GDPR

Штрафы

Многоуровневая система штрафования 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 EDPB)

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

Представитель в ЕС

Требование к наличию у оператора или обработчика ПДн, расположенного не в ЕС и обрабатывающего на регулярной основе ПДн и/или случайной основе большие объемы ПДн (спец. категории, данные о правонарушениях или приговорах) **представителя в ЕС**

Проектируемая конфиденциальность

Соблюдение требований по ИБ при проектировании ИТ-решений

KPMG

Ключевые положения GDPR

Офицер безопасности данных (Data Privacy Officer, DPO)

DPO необходим:

- Если обработка ПДн выполняется государственной структурой.
- Если обрабатываются специальные категории ПДн.
- Если обработка требует систематического мониторинга субъектов ПДн

Квалификация DPO

DPO должен обладать экспертными знаниями по защите информации

Контракт на 2 года

DPO должен быть назначен не менее чем на два года. DPO может быть как в штате, так и стороннее лицо

ФИО

ФИО и контактные данные DPO должны быть доведены до контролирующего органа и субъектов ПДн

Обязанности DPO

DPO может иметь другие профессиональные обязанности, но они должны быть совместимыми и не приводить к конфликту интересов

Назначение DPO в организации

DPO может быть назначен одновременно в нескольких организациях

Нарушения и штрафы

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), определённых 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)**

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).

Ключевые положения GDPR.

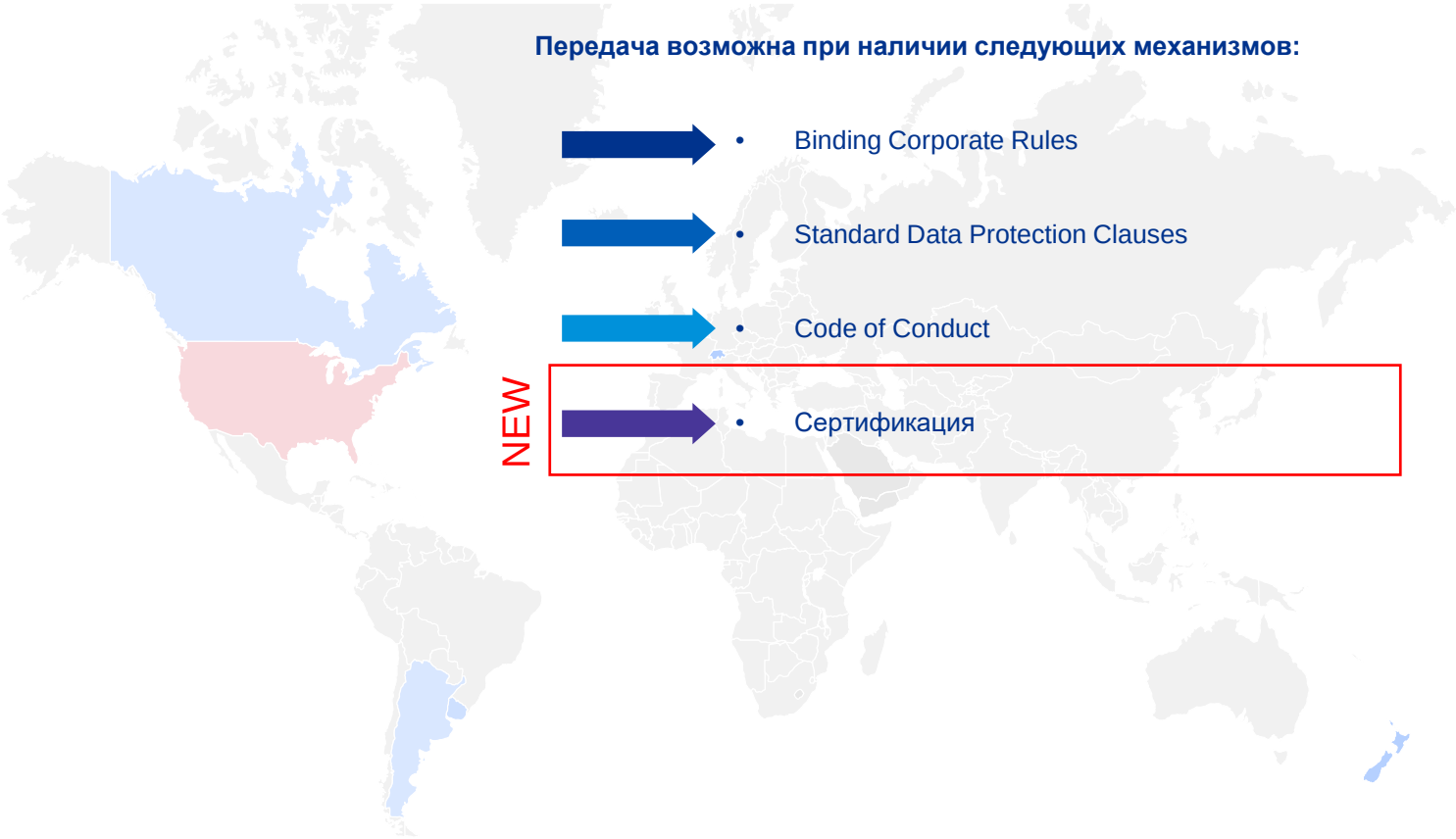
Передача ПДн за пределы ЕС

Передача ПДн в другую страну или международную организацию может осуществляться только в том случае, если Европейская Комиссия приняла решение, что данная страна или территория, или один или несколько конкретных секторов этой страны, или соответствующая международная организация обеспечивают надлежащий уровень защиты. Такая передача не требует специального разрешения

Европейская Комиссия признала, что следующие локации обеспечивают надлежащий уровень защиты:

- Андорра,
- Аргентина,
- Канада (коммерческие организации),
- Фарерские острова,
- Гернси,
- Израиль,
- Остров Мэн,
- Джерси,
- Новая Зеландия,
- Швейцария,
- Уругвай
- США (в рамках Privacy Shield framework)

Ведутся переговоры с Японией и Южной Кореей



Передача возможна при наличии следующих механизмов:

- Binding Corporate Rules
- Standard Data Protection Clauses
- Code of Conduct
- Сертификация

NEW

Влияние GDPR на финансовые институты

- Крупные штрафные санкции (особенно при наличии дочерних структур российских организаций в ЕС)
- Мониторинг поведения может попадать под область применимости GDPR (Ст3. 2b)
- Необходимо дополнительно учитывать PSD2
- Помнить, что платежи за членство в профсоюзе относятся к спецкатегории
- Репутационные риски, проблемы отношений с партнерами в ЕС, блокировка вэб-сайтов, счетов в валют ЕС

Возможный подход по приведению компании в соответствие с GDPR

1. Определить попадает ли организация под GDPR и нужно ли работать с ЕС
2. Запустить проект о приведении к GDPR, определить необходимость в представителе в ЕС
3. Провести консультации с офисом в ЕС (для международной компании), деловыми партнерами в ЕС и, по возможности, с регулятором по защите данных в стране ЕС, с которой ведется бизнес
4. Провести инвентаризацию ПДн (без этого невозможно выполнить требования об удалении и переносу данных)
5. Определить текущий уровень защиты данных, в том числе выполнение применимых нормативных и отраслевых требований
6. Назначить DPO в случае необходимости
7. Оптимизировать бизнес-процессы с целью минимизации обработки личных данных, по возможности обезличить данные. Провести классификацию данных. Внедрить дополнительные политики, процедуры, шаблоны и меры контроля. Особое внимание – формам согласия на обработку ПДн
8. Тренинги и повышение осведомленности
9. Формировать и хранить доказательства соблюдения GDPR
10. Провести PIA и сертификацию

KPMG

cyber@kpmg.ru

kpmg.ru

kpmg.com/app