KPMG

Новый регламент ЕС по защите данных (GDPR): а вы готовы?

КПМГ в России и СНГ

kpmg.ru/cyber

2018 Вступление в силу GDPR

2006 152-ФЗ

2005 Ратификация ETS 108

1998 Ратификация ETS 005

1995 Директива EC95/46/EC

1981 ETS 108

1953 ETS 005

GDPR – новый регламент Европейского союза по защите данных

Ужесточение регуляторных требований в области информационной безопасности и ответственности за их соблюдение, особенно в сфере защиты персональных данных (далее ПДн), стало мировым трендом. 25 мая 2018 года в полном объеме вступает в силу новый закон Европейского союза о защите данных – GDPR (General Data Protection Regulation/ Генеральный регламент по защите данных), отличающийся беспрецедентными штрафными санкциями за нарушение требований закона, а также оказывающий влияние на международную деятельность организаций, в том числе и организаций с российским капиталом.

Ключевые принципы защиты частной жизни (privacy) были определены в Конвенции о защите прав человека и основных свобод Совета Европы (ETS 005), вступившей в силу в 1953 году, которую в 1998 году ратифицировала Российская Федерация. С наступлением эры информатизации важнейшим документом стала Конвенция о защите физических лиц при автоматизированной обработке персональных данных Совета Европы от 1981 года (последняя редакция известна как ETS 108), которую в 2005 году ратифицировала РФ и в соответствии с принципами которой был позднее принят Федеральный закон 152-ФЗ «О персональных данных». В свою очередь, руководящими органами Европейского союза в 1995 году на основе ETS 108 была принята действующая в настоящий момент Директива Европейского союза о защите данных 95/46/EC, которую и заменит GDPR в мае 2018 года.

GDPR предназначен:

для унификации законов по защите данных, принятых в странах ЕС;

для защиты ПДн и расширения прав на конфиденциальность ПДн всех субъектов ПДн в ЕС;

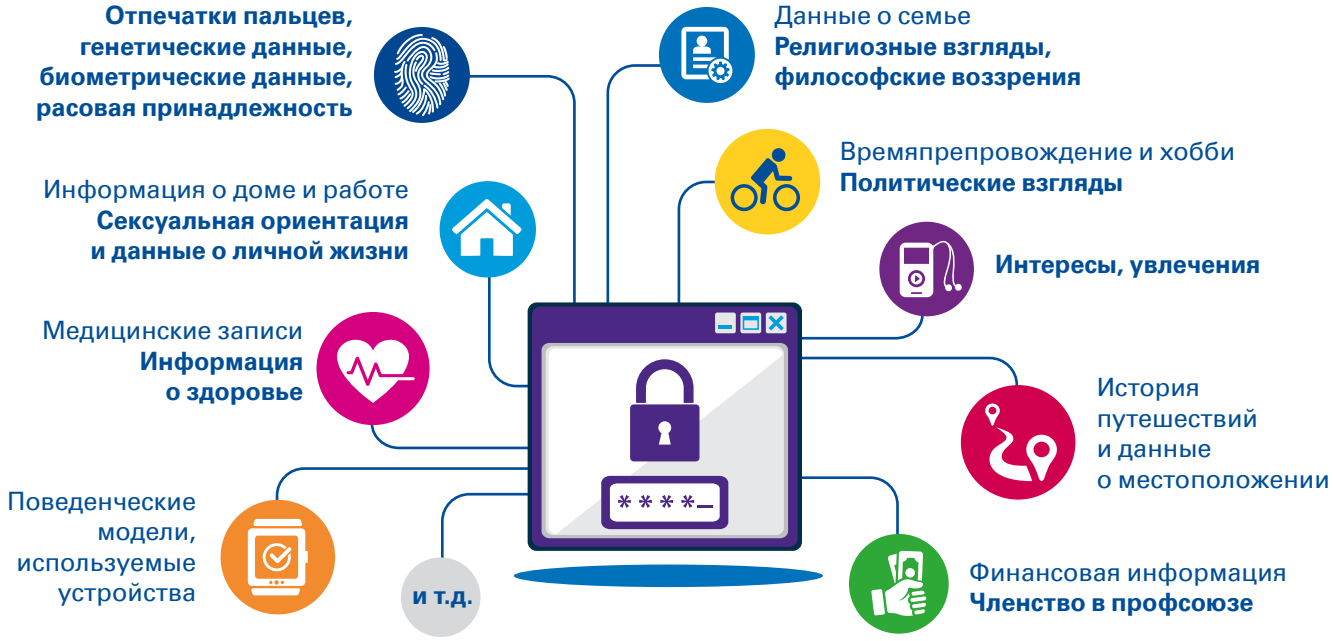
для актуализации процедур, принятых организациями ЕС в целях защиты ПДн субъектов ПДн в ЕС, с учетом современных тенденций.

Сам Регламент GDPR представляет собой документ объемом 88 страниц (в официальном издании на английском языке) и состоит из вводной части и 99 статей, распределенных по 11 главам. Большая часть текста основана на действующей Директиве ЕС о защите данных 95/46/EC, однако появились и новые требования.

KPMG

Терминология, используемая в GDPR

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



Обработка ПДн (processing) – любое действие, совершаемое с ПДн с использованием или без использования средств автоматизации, включая сбор, запись, организацию, структурирование, хранение, адаптацию или изменение, восстановление, консультацию, использование, раскрытие при передаче, распространение или обеспечение доступности, группировку или комбинацию, ограничение, стирание или уничтожение.

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.

Субъекты ПДн в ЕС (subjects who are in the Union) – субъекты ПДн, находящиеся на территории ЕС, например, граждане ЕС, резиденты ЕС, субъекты, пребывающие в ЕС на основании виз, беженцы.

Оператор ПДн (controller) – физическое или юридическое лицо, государственный орган, учреждение или другое лицо, самостоятельно или совместно с другими лицами определяющее цели и средства обработки персональных данных.

Обработчик ПДн (processor) – физическое или юридическое лицо, государственный орган, учреждение или другое лицо, обрабатывающее персональные данные по поручению оператора персональных данных.

Ключевые изменения, внесенные GDPR

Штрафы

Многоуровневая система штрафования в зависимости от тяжести нарушения.

Уровень 1: **2% от глобального оборота** или €10 000 000 (что выше).

Уровень 2: **4% глобального оборота** или €20 000 000 (что выше).

Офицер безопасности данных (DPO)

Требование к **наличию** 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 (Board) ЕС по защите данных.

Инвентаризация

Требование к проведению организациями инвентаризации информационных активов.

Уведомление об утечках

Необходимость предоставления регулятору отчетов об утечках данных в течение 72 часов с момента регистрации инцидента, а также своевременного информирования субъекта ПДн.

Безопасность

Особые требования в части мониторинга, шифрования и обезличивания персональных данных.

Оценка воздействия на конфиденциальность (DPIAs)

Требование к проведению DPIAs организациями, деятельность которых по обработке ПДн может привести к высоким рискам в отношении прав и свобод субъектов ПДн.

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** к специальным категориям ПДн.

Согласие

Требование к получению однозначных и добровольных **согласий на обработку ПДн**.

Обработчики данных

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

Представитель в ЕС

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

Проектируемая конфиденциальность

Необходимость соблюдения требований по ИБ при проектировании ИТ-решений.

Попадаете ли Вы под действие GDPR

GDPR применим к следующим организациям:

1. учрежденным в ЕС и являющимся операторами (controllers) и/или обработчиками (processors) ПДн (к примеру, наличие дочерней организации или филиала в ЕС);
2. не учрежденным в ЕС и являющимся операторами и/или обработчиками ПДн субъектов ПДн в ЕС, вид деятельности которых связан с:
   - предоставлением товаров или сервисов субъектам ПДн в ЕС вне зависимости от того, требуется ли оплата предлагаемых товаров и сервисов (к примеру, использование доступного в ЕС веб-сайта на языке страны – члена ЕС или валюты страны – члена ЕС для предоставления товаров или сервисов);
   - мониторингом поведения субъектов ПДн в пределах ЕС (профилирование субъекта ПДн, к примеру, для принятия решения в отношении субъекта или для анализа, прогноза личных предпочтений субъекта, поведения и взглядов).

Влияние GDPR на российские организации

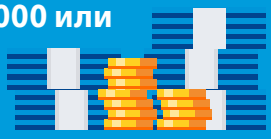
Российская Федерация не входит в ЕС, таким образом юрисдикция ЕС (в том числе применительно к GDPR) не распространяется на территорию РФ. Однако дочерние структуры российских организаций, работающие в ЕС, попадают под действие GDPR напрямую, а в отношении организаций, расположенных за пределами территории ЕС и обрабатывающих данные европейцев, влияние нового законодательства косвенное – через их деловых партнеров в ЕС, которые будут вынуждены учитывать риски сотрудничества с организациями, расположенными за пределами Евросоюза, с учетом возможных штрафов GDPR. Таким образом, несоответствие требованиям GDPR может привести к следующим негативным последствиям для российских организаций:

- **Крупные штрафные санкции (к примеру, по результатам проверки организаций, расположенных в ЕС, при этом источником информации могут быть обращения от субъектов ПДн к регулятору).**
- **Нарушение коммерческих и некоммерческих отношений с компаниями, расположенными в ЕС (к примеру, закрытие корреспондентских счетов банковской организации или добавление организации в «черный список»).**
- **Нарушение доступности веб-сайта для субъектов ПДн в ЕС, задействованного в сборе ПДн.**
- **Ухудшение репутации организации на международном рынке в части защиты данных.**

Нарушения и штрафы

€ 20 000 000 или

4%



За нарушение:

— Основных принципов обработки ПДн, в том числе условий согласия на обработку 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 организации, определенного в статьях 44, 45

— Обязательств, определенных в нормативных актах стран – членов ЕС, принятых в соответствии с главой IX

— Требований контролирующих органов (supervisory authority), определенных в статьях 58(1) и 58(2)

€ 10 000 000 или

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)

Что нужно сделать

С учетом упомянутого выше можно сделать вывод о том, что некоторые российские организации попадают под действие GDPR. При этом российским организациям, являющимся операторами ПДн, необходимо в первую очередь выполнять требования законодательства РФ в части защиты ПДн. Для исключения противоречий и пересечений требований законодательства РФ и GDPR при разработке мероприятий по приведению организации в соответствие с GDPR следует провести тщательный анализ законодательства РФ и GDPR и внедренных в организации процессов защиты данных.

1 **Оценка**

Провести анализ законодательства стран нахождения офисов организации. К примеру, соотнести требования 152-ФЗ и GDPR, чтобы сформировать методику проверки процессов обработки ПДн.

2 **Обследование**

Провести проверку процессов обработки ПДн в организации на соответствие требованиям GDPR и нормативных актов стран нахождения офисов организации в области защиты данных.

3 **Планирование**

Разработать план мероприятий и дорожную карту по достижению соответствия требованиям GDPR.

4 **Проектирование**

Определить необходимые организационные меры, процессы и контроли в части защиты данных (основы конфиденциальности).

5 **Внедрение**

Внедрить процессы и организационно-распорядительную документацию. Провести оценку воздействия на конфиденциальность (DPIAs) и внедрить контроли.

6 **Мониторинг**

Проводить постоянный мониторинг функционирования внедренных контролей защиты данных.

Услуги КПМГ

Экспресс-оценка применимости GDPR для организации

Быстрая оценка зоны воздействия GDPR на организацию и уровня ее готовности в части защиты данных

Анализ соответствия организации требованиям GDPR и разработка дорожной карты по дальнейшим шагам

— Проведение аудита процессов обработки ПДн в организации с учетом требований GDPR и локального законодательства. Выявление и анализ несоответствий

— Разработка дорожной карты по приведению организации в соответствие требованиям GDPR и локального законодательства, адаптация требований GDPR под бизнес-процессы организации, подготовка бюджета

Инвентаризация ПДн и их потоков

— Оценка процессов обработки ПДн. Выявление процессов обработки ПДн, представляющих высокий риск в отношении прав и свобод субъектов ПДн. Определение потоков ПДн, включая трансграничную передачу ПДн, ПДн, обрабатываемых с привлечением сторонних организаций.

— Определение перечня ПДн, перечня субъектов ПДн, мест, средств и способов обработки ПДн, лиц, имеющих доступ к ПДн

Повышение осведомленности

Проведение и/или разработка мероприятий (тренинги, круглые столы, семинары) по повышению осведомленности работников об основных принципах обработки ПДн и обеспечению конфиденциальности данных

Содействие во внедрении процессов по GDPR

Оказание содействия команде клиента во внедрении и мониторинге мер соответствия GDPR, включая разработку и внедрение процедур управления ПДн, внедрение требований GDPR в ИТ- и бизнес-процессы, внедрение мер, необходимых для приведения организации в соответствие требованиям GDPR

Содействие в проведении DPIAs

Содействие в проведении оценки воздействия на конфиденциальность: тщательный и документированный анализ рисков для субъектов ПДн при обработке ПДн, определение мер, митигирующих выявленные риски

Контакты

Андрей Лепехин
Руководитель Группы по оказанию услуг в области управления информационными рисками
Партнер
T: + 7 495 937 4444, доб. 14239
E: alepekhin@kpmg.ru

Илья Шаленков
Услуги в области управления информационными рисками
Старший менеджер
T: + 7 495 937 4444, доб. 10138
E: ishalenkov@kpmg.ru

kpmg.ru/cyber