VIII МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

GDPR (General Data Protection Regulation)

Новые требования Европейского Союза в области обработки и защиты Персональных Данных

Важные аспекты применения

Ноябрь 2017

У вас есть вопрос? У нас есть ответ.
Решая сложные задачи бизнеса, мы улучшаем мир.

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

EY
Совершенствуя бизнес, улучшаем мир

О применимости GDPR к российским компаниям (1/3)

Критерии применимости:

1. Действие GDPR распространяется на операции по обработке персональных данных в контексте присутствия на территории ЕС их оператора или обработчика, независимо от того, производится ли такая обработка на территории ЕС или нет
2. Действие GDPR распространяется на «обработку персональных данных, находящихся на территории ЕС субъектов, которая осуществляется оператором или обработчиком, не имеющим присутствия на территории ЕС, в тех случаях, когда такая деятельность по обработке относится к:

- Предложению товаров или услуг находящимся на территории ЕС субъектам персональных данных как на возмездной, так и на безвозмездной основе; или
- Отслеживанию действий субъектов ПДн при условии, что таковые осуществляются в пределах ЕС»

Ссылка: Article 3 GDPR

О применимости GDPR к российским компаниям (2/3)

Комментарии:

1. В критериях применимости отсутствует привязка к гражданству субъекта ПДн; под защиту GDPR попадают ПДн всех субъектов в момент нахождения их внутри ЕС
2. Формулировка «предложение товаров и услуг находящимся на территории ЕС субъектам персональных данных» главным образом нацелена на организаций, которые не имеют штаб-квартиры или какого-либо иного присутствия на территории ЕС и используют веб-сайты для предоставления/продвижения/оплаты своих услуг
3. Согласно критерию №1, если у организации есть дочерние структуры в ЕС, то эти дочерние структуры попадают под GDPR
4. Согласно критерию №2, в контексте формулировки про «отслеживание» [субъектов ПДн], российские организации подпадают под действие регламента GDPR в случае, если они будут отслеживать действия физических лиц для создания профилей, в том числе, в целях принятия решений для анализа/прогнозирования их личных предпочтений, поведения (например, скоринг, мониторинг транзакций, аналитика данных для целей таргетированной рекламы)

О применимости GDPR к российским компаниям (3/3)

В качестве примеров применимости GDPR можно привести следующие ситуации:

- Услуги, предоставляемые организацией в РФ субъектам ПДн, находящимся на территории ЕС (электронная коммерция, логистика и т.п.)
- Мониторинг банковских/телеком транзакций субъекта ПДн (например, в рамках антифрода) в то время, как субъект ПДн находится на территории ЕС
- Услуги по анализу персональных данных субъектов ПДн (например, в рамках банковского скоринга), находящихся на территории ЕС, которые родительская организация в РФ предоставляет своим дочерним подразделениям, находящимся в ЕС

Немного цифр

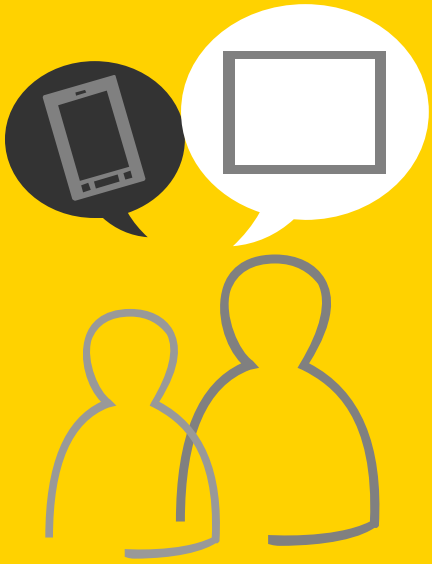
25 мая 2018 - GDPR вступает в силу

Высокий размер штрафов за несоответствие:

10M Евро или 2% от мирового годового оборота компании – максимальный размер штрафа за «незначительные» нарушения (например, несоблюдение принципов минимизации состава обрабатываемых ПДн, а также нарушение статей №8, 11, 25, 39, 42 и т.д.)

20M Евро или 4% от мирового годового оборота компании – максимальный размер штрафа за «более серьезные» нарушения (например, за несоблюдение принципов защиты данных, а также статей 5-7, 9, 12, 22, 44-49 и т.д.)

95 % из 548
опрошенных организаций попадают под GDPR*



* Комментарий: по итогам международного исследования, проведенного EY и IAPP (International Association of Privacy Professionals в 2017 г

Ключевые аспекты GDPR (1/3)

- Акцент на обеспечение прав и свобод субъектов ПДн (дополнительные права субъектов ПДн – право на забвение, право на перенос данных; обработка минимально необходимого набора ПДн; оценка рисков нарушения прав и свобод субъектов ПДн в рамках Data Protection Impact Assessment и т.п.)
- Риск ориентированный подход к обработке и защите ПДн
- Обязанность оператора ПДн по уведомлению регулятора в течение 72 часов с момента обнаружения фактов нарушений в обработке или защите ПДн (в том числе компрометации ПДн). Описание выявленных нарушений, потенциальные последствия, а также компенсирующие меры по минимизации рисков должны быть задокументированы
- Право субъекта на перенос ПДн между организациями-операторами: если обработка ПДн осуществляется при помощи средств автоматизации, субъект ПДн имеет право на получение своих персональных данных в структурированном, общепринятом и распознаваемом автоматизированными системами формате для последующей передачи другому оператору ПДн
- Отсутствие ограничений в использовании средств защиты информации

Ключевые аспекты GDPR (2/3)

- Необходимость поддерживать в актуальном состоянии реестр процессов обработки ПДн, отражающий:
  - Наименование и контактные данные оператора / обработчика, представителя оператора / обработчика и DPO (data protection officer'a)
  - Цель обработки ПДн (применимо к операторам)
  - Описание категорий субъектов ПДн, а также состав обрабатываемых ПДн
  - Категории получателей (организации/физ. лица) соответствующих ПДн (включая трансграничную передачу данных)
  - Срок хранения ПДн
  - Общее описание применяемых технических и организационных мер по защите ПДн

Ключевые аспекты GDPR (3/3)

- Концепции проектируемой конфиденциальности и конфиденциальности по умолчанию (privacy by design and privacy by default)
  - Согласно концепции privacy by design организация должна учитывать риски, связанные с ПДн, на всех этапах жизненного цикла обработки данных (например, при формировании функциональных требований к ИТ-системам, настройке механизмов безопасности в ИТ-системах и средствах защиты информации, при передаче данных и при уничтожении данных). Основываясь на анализе рисков, организации должны внедрить соответствующие технические и организационные меры защиты персональных данных (например, псевдонимизацию данных)
  - Согласно концепции privacy by default организации в рамках четко сформулированных целей должны обрабатывать минимально необходимый состав ПДн

Перечень мероприятий, которые рекомендуется провести организации, в случае если она попадает под требования GDPR

GAP – анализ

Пересмотр существующих и планируемых к внедрению ИТ-решений на соответствие privacy by design и privacy by default

Внедрение новых, специфичных для GDPR процессов, политик и процедур (уведомление регулятора о выявленных нарушениях, BCR)

Внедрение мероприятий по мониторингу соответствия GDPR

Анализ процессов обработки ПДн. Составление реестра

Назначение DPO и выбор модели управления функцией защиты ПДн

Проведение оценки Data Protection Impact Assessment

Пересмотр существующих организационно-технических мер защиты информации с т.з. требований GDPR

Наиболее популярные вопросы

- Могут ли компании передавать персональные данные субъектов, находящихся в ЕС подразделениям в России и, если да, то какие меры следует заблаговременно предпринять?
- Каким образом будут применяться штрафные санкции: к юридическим лицам, находящимся в ЕС/к материнской компании, находящейся за пределами ЕС/прочее? Какой показатель будет использоваться в качестве основы для расчета суммы штрафа: общая годовая выручка юридического лица-нарушителя или общая годовая выручка группы?
- Что представляют собой Binding Corporate Rules (обязательные корпоративные правила)?
- Как реагируют клиенты в ЕС на регламент GDPR: внедряют/ проводят только проверку соответствия/ ничего не делают и ждут дополнительных инструкций/ другое?
- Какие ключевые факторы успешной реализации регламента GDPR?

Спасибо за внимание

Наши контакты

Николай Самодаев, CISA, MBCI
Партнер, Руководитель практики в области управления информационными технологиями и ИТ-рисками

Тел: +7 (495) 755-9869
E-mail: Nikolay.Samodaev@ru.ey.com

Евгений Ким, CIPP/E, CIPM, CISA
Старший менеджер, Отдел по управлению информационными технологиями и ИТ-рисками

Тел: +7 (495) 705-9739
E-mail: Evgeny.A.Kim@ru.ey.com