
GDPR (General Data Protection Regulation)
Новые требования Европейского Союза
в области обработки и защиты Персональных Данных
Важные аспекты применения
Сентябрь 2017
EY
Совершенствуя бизнес,
улучшаем мир

Содержание

EY

Совершенствуя бизнес,
улучшаем мир

Основные термины

Персональные данные (ПДн)	Любая информация, относящаяся к идентифицированному или идентифицируемому физического лица (субъект ПДн) (включая, IP-адрес)
Идентифицируемое физическое лицо	Физическое лицо, которое может быть идентифицировано прямо или косвенно, в частности с использованием идентификатора, например: имени, идентификационного номера, данных о местоположении, онлайн-идентификатора; или с использованием параметров, характеризующих данное физическое лицо с физиологической, генетической, психологической, экономической, культурной или социальной точки зрения
Обработка ПДн	Любая операция или набор операций, выполняемых с ПДн или с набором ПДн как с использованием средств автоматизации, так и без использования оных, включая: сбор, запись, структурирование, хранение, адаптацию или изменение, использование, распространение, ограничение, уничтожение
Оператор ПДн (Controller)	Физическое или юридическое лицо, государственный орган, учреждение, которое в одиночку или совместно с другими определяет цели и средства обработки ПДн
Обработчик ПДн (Processor)	Физическое или юридическое лицо, государственный орган, учреждение, которое обрабатывает ПДн по поручению оператора ПДн
Псевдонимизация ПДн	Обработка ПДн, при которой ПДн не могут быть отнесены к конкретному субъекту ПДн без использования дополнительной информации, при условии, что такая дополнительная информация хранится отдельно и защищена техническими и организационными мерами, для того чтобы исключить ассоциацию ПДн с идентифицированным или идентифицируемым физическим лицом

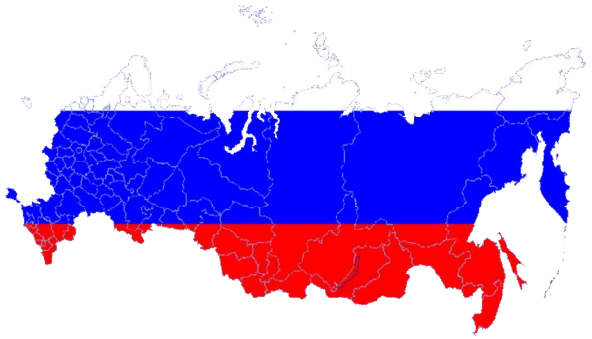
Развитие требований по обработке и защите персональных данных в Европейском Союзе / ЕС

- 24 октября 1995 г была представлена Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (Директива). Директива определяла термин «персональные данные», а также формулировала требования к сбору и обработке персональных данных

- Развитие информационных технологий и переход бизнеса в цифровое пространство потребовали пересмотра регуляторных требований к обработке и защите персональных данных. Как результат в 2016 г был выпущен General Data Protection Regulation (GDPR), который заменит требования Директивы 95/46/ЕС

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:
   - Предложение товаров или услуг находящимся на территории ЕС субъектам персональных данных как на возмездной, так и на безвозмездной основе; или
   - Отслеживание их действий при условии, что таковые осуществляются в пределах ЕС»

Комментарии:

- *В критериях нет привязки к гражданству субъекта ПД; под защиту GDPR попадают ПДн всех субъектов в момент нахождения их внутри ЕС*
- *Формулировка «предложение товаров и услуг находящимся на территории ЕС субъектам персональных данных» главным образом нацелена на сайты электронной коммерции компаний, которые не имеют штаб-квартиры или какого-либо иного присутствия на территории ЕС*

О применимости GDPR к российским компаниям (2/3)

- Согласно критерию №1, если у организации есть дочерние структуры в ЕС, то эти дочерние структуры попадают под GDPR
- Согласно критерию №2, в контексте формулировки про «отслеживание» [субъектов ПДн], российские организации подпадают под действие регламента GDPR в случае, если они будут отслеживать физических лиц в режиме онлайн 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 рекламы)

  Таким образом в качестве предпосылок для применимости GDPR можно привести следующие ситуации:

  - 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
  - Услуги электронной коммерции (интернет-магазины)

О применимости GDPR к российским компаниям (3/3)

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

- GAP-анализ / аудит соответствия требованиям GDPR
- Анализ текущих процессов обработки персональных данных (ПДн) на предмет:
  - определения целей обработки
  - минимально необходимого для достижения целей обработки набора персональных данных, а также типов обрабатываемых ПДн
  - определение юридической законности для обработки ПДн (особенно важно при использовании больших данных – big data и внешних источников ПДн, таких как социальные сети)
  - определение сроков хранения
  - выявление задействованных информационных систем
  - определение типов получателей ПДн (извне организации), включая транграничную передачу данных, а также юридическое обоснование передачи ПДн вовне
- Пересмотр существующих и планируемых к внедрению информационных решений и процессов на предмет соответствия концепциям проектируемой конфиденциальности и конфиденциальности по умолчанию (privacy by design & by default)
- Определить необходимость в назначении ответственного за защиту данных (Data Privacy Officer) и решить, как будет организована внутренняя система управления защитой данных
- Внедрение новых, специфичных для GDPR процессов (по оценке рисков нарушения конфиденциальности, по уведомлению регулятора о выявленных фактах нарушения), политик и процедур
- Провести оценку рисков нарушения конфиденциальности (Data Protection Impact Assessment – DPIA) для критичных процессов обработки ПДн
- Пересмотреть существующие организационно-технические меры защиты информации с т.з. требований GDPR

Ключевые аспекты GDPR (1/4)

- Новые требования Европейского Союза (ЕС) по защите персональных данных (GDPR) вводятся в действие и обязательны к исполнению с 25 мая 2018 года
- Контроль исполнения требований GDPR лежит на локальных представительствах регуляторов (supervisory authorities)
- GDPR вводит принцип «единого окна» (one stop shop) - компания может выбрать одно из 28 локальных представительств регуляторов (supervisory authorities), так называемый «lead supervisory authority», с которым будет координировать свои действия в области обработки и защиты ПДн

Штрафы при нарушении требований GDPR

- За «незначительные» нарушения требований GDPR штраф составляет до 10 миллионов евро или 2% от мирового годового оборота (в зависимости от того, какая из этих сумм окажется выше)
- За «более серьезные» нарушения (например, за несоблюдение принципов защиты данных) предусмотрен более высокий размер штрафа - до 20 миллионов евро или 4% от мирового годового оборота (в зависимости от того, какая из этих сумм окажется выше)
- Штрафные санкции будут применяться в отношении юридических лиц, находящихся в соответствующих странах-участницах ЕС. Если компания-нарушитель не имеет присутствия в ЕС, то штрафные санкции могут быть применены непосредственно в отношении компании, расположенной за пределами ЕС
  (примечание: механизм обеспечения и взыскания штрафов пока не проработан)

Ключевые аспекты GDPR (2/4)

- 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.)
- Отсутствие жестких требований к использованию сертифицированных средств защиты информации
- Необходимость поддерживать в актуальном состоянии реестр процессов обработки ПДн, отражающий:
  - Наименование и контактные данные оператора / обработчика, представителя оператора / обработчика и DPO (data protection officer'а)
  - 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
- Оператор ПДн должен уведомить 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

Ключевые аспекты GDPR (3/4)

- 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 проектировании дизайна процесса обработки, формировании функциональных требований к ИТ-системам, настройке механизмов безопасности в ИТ-системах и средствах защиты, при передаче данных в архивное хранение 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 обработки должны процессить минимально необходимый состав ПДн
- Право 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.

Ключевые аспекты GDPR (4/4)

- Право «на забвение»

Субъект ПДн имеет право поручить оператору ПДн удалить соответствующие ПДн, а оператор ПДн обязан удалить соответствующие ПДн в случае*:

- ПДн более не являются необходимыми для выполнения целей, в соответствие с которыми они были собраны/обрабатывались
- Владелец ПДн отозвал согласие на обработку ПДн, при этом отсутствуют другие юридические основания для обработки ПДн
- Незаконной обработки ПДн
- ПДн должны быть удалены в соответствие с требованиями законодательства ЕС или соответствующих стран-членов ЕС

**Комментарий: полный перечень условий см. в статье 17 GDPR*

GDPR: европейский опыт EY

Соответствие GDPR, проверки, штрафные санкции / GDPR compliance and penalties

Здесь и далее приведены наиболее популярные вопросы, ответы на которые представит наш гость – **Фабрис Нафтальски** - Партнер EY, отвечающий за предоставление услуг по GDPR в Европе и являющийся Data Privacy Officer в EY France

Каким образом регулятор будет проверять выполнение требований, и кто будет проводить проверки? /

How compliance will be verified by the regulator and who will be the auditor?

Могут ли компании передавать персональные данные субъектов, находящихся в ЕС подразделениям в России и, если да, то какие меры следует заблаговременно предпринять? /

Is it allowed to transfer personal data of data subjects located in EC to Russia and if yes what actions should companies think about beforehand?

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? /

How penalties will be applied: to the legal entities located in EU/to parent company located outside of EU/other? What will be the basis for penalty calculation: total annual revenue of the non-compliant legal entity or the whole total annual revenue of the group?

ЭЯ европейский опыт исполнения требований GDPR / EY EU GDPR practice and implementation

Как реагируют клиенты в ЕС на регламент GDPR: внедряют/ проводят только проверку соответствия/ ничего не делают и ждут дополнительных инструкций/ другое?

How the clients in EU are reacting on the GDPR: implementing/perform compliance audit only/do nothing and wait for further instructions/other?

На какие моменты в части соблюдения новых требований должны обратить первоочередное внимание директор по информационным технологиям или директор по информационной безопасности? /

What is the most important part of implementation process from the CIO/CISO point of view?

С какими главными трудностями столкнутся компании при реализации регламента? /

What is the most difficult part of implementation process?

Ключевые факторы успешной реализации регламента GDPR /

Key success factors for GDPR implementation?

Спасибо за внимание

Наши контакты

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

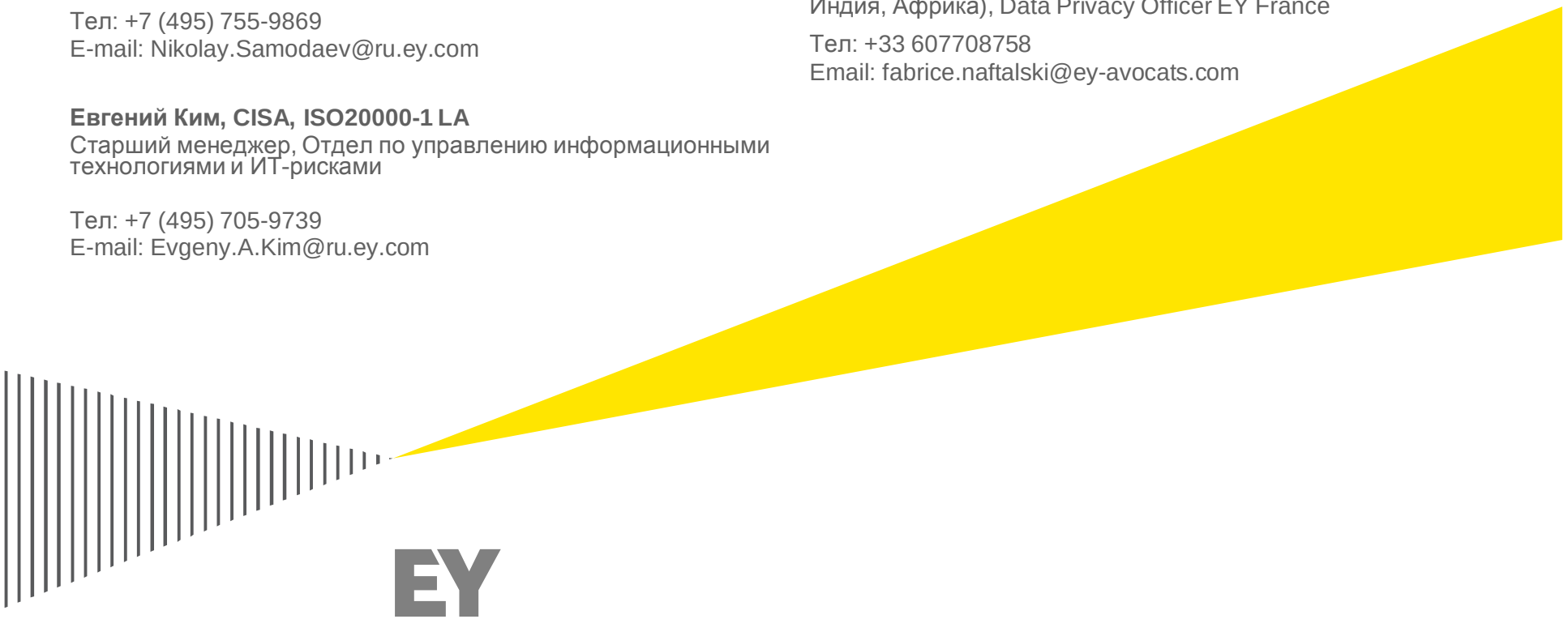
Тел: +7 (495) 755-9869
E-mail: Nikolay.Samodaev@ru.ey.com

Евгений Ким, CISA, ISO20000-1 LA
Старший менеджер, Отдел по управлению информационными технологиями и ИТ-рисками

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

Фабрис Нафтальски, CIPP/E, CIPM,
Партнер, Руководитель юридической практики в области защиты данных в регионе EMEIA (Европа, Ближний Восток, Индия, Африка), Data Privacy Officer EY France

Тел: +33 607708758
Email: fabrice.naftalski@ey-avocats.com



EY
Совершенствуя бизнес,
улучшаем мир