Data Protection Officer
Stanislav Kovalenko

GDPR:

12 шагов к соответствию

Программа тренинга

1. Что такое GDPR и сфера его действия
2. Перечень рекомендуемых мероприятий для подготовки к соответствию требованиям GDPR
   - 2.1. Аудит соответствия требованиям GDPR
   - 2.2. Политика конфиденциальности, Политика использования файлов cookie
   - 2.3. «Правильное» согласие на обработку персональных данных
   - 2.4. Соблюдение 6 основных принципов
   - 2.5. Privacy by Design & Default
   - 2.6. Учетные записи об обработке персональных данных
   - 2.7. Data Protection Impact Assessment
   - 2.8. Трансграничная передача персональных данных
   - 2.9. Обучение сотрудников
   - 2.10. Представитель в ЕС
   - 2.11. Data Protection Officer
   - 2.12. Подготовка к утечке персональных данных
3. Ответственность за нарушение требований GDPR

Что такое GDPR и сфера его действия

General Data Protection Regulation

(GDPR) –

Общий регламент о защите данных*

- *Регламент ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА (ЕС) 2016/679 от 27 апреля 2016 о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, и об отмене Директивы 95/46/ЕС.*
- *GDPR вступил в действие 25 мая 2018 года, заменив Директиву 95/46/ЄС о защите физических лиц применительно к обработке персональных данных и свободном движении таких данных.*
- *Предметом регулирования GDPR являются персональные данные*

Персональные данные –
это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (субъекту данных), по которой его можно определить прямо или косвенно

К персональным данным относятся:

1. Общие ПД:

- имя, фамилия, возраст, пол, контактные данные (телефон, e-mail), место рождения, информация о доме и работе, идентификационный номер, интересы и увлечения, финансовая информация, данные о местоположении, онлайн-идентификатор.

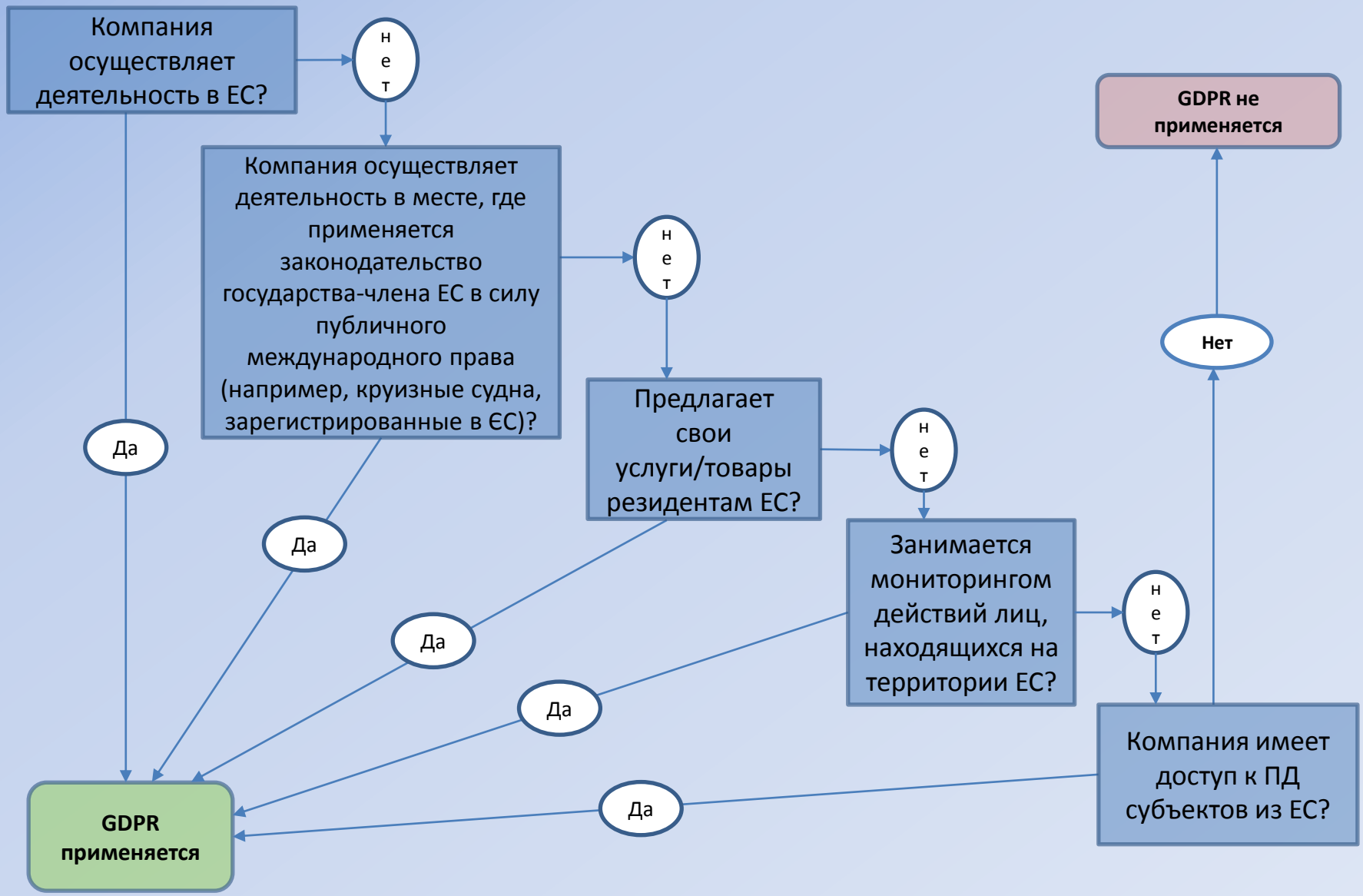
2. Специальные (чувствительные) ПД:

- данные о расовом и этническом происхождении, политические взгляды, религиозные и философские верования, членство в профсоюзах, генетических данные, биометрические данные, данные о здоровье, половая жизнь и сексуальная ориентация. Регламент предоставляет государствам-членам ЕС право уточнять в своих внутренних нормативных актах положения о специальных категориях персональных данных.

3. Данные о судимости и уголовных преступлениях или о связанных с этим мерах безопасности.

Основные нововведения GDPR:

- ✓ расширяет используемую терминологию, изменяет устоявшиеся термины, в частности основополагающее понятие «персональные данные» истолковывается более широко
- ✓ предоставляет физическим лицам больше прав в части контроля за их персональными данными
- ✓ налагает на контролеров и процессоров персональных данных обременительные обязательства
- ✓ имеет экстерриториальное действие, т.е. распространяется на компании (организации) за пределами ЕС
- ✓ предусматривает размеры штрафов и дает национальным регуляторам право их налагать на лиц, которые нарушают требования GDPR
- ✓ страны ЕС имеют право дополнительно устанавливать уголовную ответственность за нарушение требований GDPR


Компания осуществляет деятельность в ЕС?
нет
Компания осуществляет деятельность в месте, где применяется законодательство государства-члена ЕС в силу публичного международного права (например, круизные судна, зарегистрированные в ЄС)?
нет
Предлагает свои услуги/товары резидентам ЕС?
нет
Занимается мониторингом действий лиц, находящихся на территории ЕС?
нет
Компания имеет доступ к ПД субъектов из ЕС?
Нет
GDPR не применяется
Да
Да
Да
Да
Да
GDPR применяется

На контролеров и процессоров за пределами ЕС требования GDPR распространяются в следующих случаях:

При обработке персональных данных субъектов данных, находящихся в Союзе*, и:

- компания, организация осуществляет деятельность (поставляет товары/выполняет работы/предоставляет услуги) на территории ЕС или для лиц, находящихся на территории ЕС, независимо от факта оплаты от таких субъектов данных; или
- компания, организация осуществляет мониторинг** поведения субъектов данных, если такое поведение имеет место в пределах ЕС; или
- компания, организация имеет доступ к персональным данным субъектов из ЕС (например, на компанию работают граждане ЕС).

* Гражданство, место жительства или другой правовой статус субъекта данных не имеют значения.

** Мониторинг может включать: отслеживание лиц из ЕС в Интернет; использование методов обработки данных для профилирования лиц, их поведения или их отношения к чему-либо (например, для анализа или прогнозирования личных предпочтений).

Основные используемые термины:

1) «Обработка» персональных данных означает любую операцию или ряд операций с персональными данными или наборами персональных данных с использованием автоматизированных средств или без них, такие как сбор, регистрация, организация, структурирование, хранение, адаптация или изменение, поиск, ознакомление, использование, раскрытие через передачу, распространение или предоставление иным образом, упорядочение или комбинирование, ограничение, стирание или уничтожение.

2) «Субъект» персональных данных – это идентифицированное или идентифицируемое физическое лицо. Субъектами персональных данных в ЕС являются субъекты, находящиеся на территории ЕС, например, граждане/резиденты ЕС, субъекты, временно пребывающие в ЕС на основании виз, беженцы.

3) «Контролер» персональных данных - это физическое или юридическое лицо, орган публичной власти, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных; если цели и средства такой обработки определяются законодательством ЕС (государства-члена), то контроллер или специальные критерии его назначения могут быть предусмотрены в таком законодательстве.

4) «Процессор» («оператор») персональных данных – это физическое или юридическое лицо, орган публичной власти, агентство или иной орган, который обрабатывает персональные данные от имени контроллера.

Перечень рекомендуемых мероприятий для подготовки к соответствию требованиям GDPR

1. Провести аудит соответствия требованиям GDPR:

• Проанализировать все бизнес процессы и внутренние процедуры, касающиеся обработки персональных данных (в частности, путем проведения интервью с ключевыми сотрудниками). При анализе процессов и процедур необходимо обращать внимание на соблюдение прав субъектов данных и соблюдение основных принципов обработки персональных данных, включая способы удаления персональных данных, их предоставления на запрос и т.п.
• Идентифицировать и задокументировать имеющиеся персональные данные, а также определить законные основания для их дальнейшей обработки (в соответствии со ст. 6 Регламента). Документирование персональных данных поможет соблюсти принцип отчетности и в дальнейшем поможет при подготовке учетных записей об обработке персональных данных.
• Проверить договорные обязательства по обработке персональных данных с контрагентами, независимо от того, контроллером или процессором является компания, организация.
• Проанализировать внутренние положения, касающиеся обработки и защиты персональных данных. В компании, организации должны существовать политики/положения, регулирующие порядок обработки и защиты персональных данных (для разных категорий данных могут быть разные политики, например, в отношении персональных данных сотрудников, контрагентов, клиентов и т.п.). Также рекомендуется внедрить политику/положение о нарушении персональных данных.
• Провести инвентаризацию информационных систем и баз персональных данных.
• Провести анализ ландшафта ИТ систем на соответствие средств защиты требованиям GDPR.
• Проанализировать интерфейсы систем ИТ и сайта компании, организации.
• Провести обзор существующих мер физической безопасности информации.
• Провести оценку воздействия на защиту персональных данных (Data Protection Impact Assessment) и внедрить контроли.
• Разработать план мероприятий по достижению соответствия требованиям GDPR.

2. Разработать и опубликовать Политику конфиденциальности (Privacy Policy), Политику использования файлов cookie (Cookie Policy):

Внедрение таких политик необходимо с целью выполнения требований GDPR по законности и прозрачности обработки персональных данных, а также для соблюдения прав субъектов данных на доступ и быть проинформированным (п.30 Преамбулы, ст.ст. 5, 13, 14, 15 GDPR).

В соответствии с GDPR идентификаторы cookie и IP адрес расцениваются как персональные данные. Зачастую в компании, организации это единственный источник получения персональных данных.

Политика/политики размещаются в доступных субъектам персональных данных местах (легкодоступность), в частности на веб-сайте компании, организации, и должны быть краткими, написанными на понятном и простом языке.

GDPR требует, чтобы компании, организации предоставляли людям информацию об обработке и о конфиденциальности данных во время получения от них личных данных. Если контролер собирал данные о клиентах до 25 мая 2018 года, ему следует убедиться, что таким клиентам было предоставлено соответствующее уведомление, отвечающее требованиям Регламента. Если контролер не предоставлял этого, он должен как можно скорее предоставить информацию об обработке и о конфиденциальности данных, требуемую в соответствии с GDPR. Контролер также должен будете сделать это, если способ обработки персональных данных или причины обработки изменились после 25 мая 2018 года.

3. Получить «правильное» согласие на обработку персональных данных и обновить процедуры получения согласия субъектов на обработку:

GDPR требует «свободного конкретного информированного и однозначного» пользовательского согласия.

Согласно п. 171 Преамбулы GDPR нет необходимости в получении нового согласия, если ранее полученное согласие на обработку ПД соответствует требованиям GDPR.

В тоже время рекомендации Рабочей группы ЕС по защите ПД (29 Working party) wp259 предусматривают необходимость получения нового согласия, если предыдущее согласие субъекта ПД не соответствует требованиям GDPR.

Определение согласия в Статье 4(11) GDPR похоже на старое определение в Директиве 95/46/ЕС о защите физических лиц в отношении обработки персональных данных, но добавляет некоторые детали того, как должно быть дано согласие:

Определение Директивы 95/46/ЕС:	**Определение GDPR:**
«Любое свободно предоставленное конкретное и информированное указание его пожеланий, которым субъект данных дает свое согласие на обработку персональных данных, касающихся его»	**«Любое свободно предоставленное, конкретное, информированное и однозначное указание желания субъекта данных, с помощью которого он посредством заявления или явного позитивного действия дает согласие на обработку относящихся к нему персональных данных»**

3. Получить «правильное» согласие на обработку персональных данных и обновить процедуры получения согласия субъектов на обработку:

Можно выделить следующие ключевые моменты, связанные с получением согласия субъекта данных на обработку:

1) Отделение: запросы о согласии должны быть отделены от других условий. Согласие не должно быть предварительным условием получения услуги, за исключением случаев, когда это необходимо для этой услуги.

2) Активное согласие: предварительно отмеченные флажки в чекбоксах больше недействительны, используйте пустые чекбоксы для проставления отметок или аналогичные активные методы.

3) Выборочность: предоставьте различные варианты для получения отдельного конкретного согласия на различные виды обработки (с разными целями), где это необходимо.

4) Наименование: назовите вашу компанию, организацию и других контролеров и процессоров, которым будут передаваться полученные данные на основании согласия. Если вы полагаетесь на согласие, полученное кем-то другим, убедитесь, что вас конкретно назвали при получении согласия.

5) Документирование: ведите записи, чтобы продемонстрировать, на что субъект дал согласие, в том числе когда и как он дал согласие.

6) Легкость отзыва: скажите людям, что они имеют право отозвать свое согласие в любое время, и как это сделать. Его должно быть так же легко отозвать, как и дать.

4. Соблюдение 6 основных принципов GDPR:

1. Персональные данные следует обрабатывать прозрачно, справедливо и законно (*Lawfulness, fairness and transparency).
2. Персональные данные можно обрабатывать только для явно указанных законных целей (*Purpose limitation).
3. Собирать и хранить следует только минимальное количество персональных данных, достаточных для указанной цели (*Data minimisation).
4. Обеспечение точности персональных данных, а также возможности их редактирования (обновления) и удаления (*Accuracy).
5. Персональные данные имеют ограниченный срок хранения (не более, чем это необходимо для определенной цели) (*Storage limitation).
6. Обеспечение безопасности, целостности и конфиденциальности персональных данных (*Integrity and confidentiality).
7. Контроллер должен быть готовым и способным продемонстрировать соблюдение вышеуказанных принципов (*Accountability).

Информация, которую необходимо предоставить субъекту данных (ст. 13, 14 GDPR)

Какую информацию обязаны предоставить	*Если данные собраны от субъекта*	*Если данные получены из других источников*
Наименование и контактные данные компании, организации	✓	✓
Наименование и контактные данные представителя в ЕС	✓	✓
Контактные данные офицера по защите данных (DPO)	✓	✓
Цели обработки	✓	✓
Правовая основа (законное основание) для обработки	✓	✓
Законные интересы контроллера или третьей стороны	✓	✓
Полученные категории персональных данных		✓
Получатели или категории получателей персональных данных	✓	✓
Детали передачи персональных данных третьим странам или международным организациям	✓	✓
Период хранения персональных данных, или, если это невозможно, - критерии определения такого периода	✓	✓
Права, доступные субъектам данных, в связи с обработкой	✓	✓
Источник персональных данных		✓
Является ли предоставление данных уставным или договорным требованием, или необходимым для заключения контракта	✓	
Наличие автоматизированной обработки и принятия решений, в том числе профайлинга	✓	✓

5. Привести информационные решения и процессы в соответствие концепциям privacy by design & by default:

«*Privacy by design*» (ст. 25(1) Регламента): принимая во внимание уровень техники, стоимость реализации и характер, объем, контекст и цели обработки, а также риски различной вероятности и серьезности для прав и свобод физических лиц, возникающие при обработке, контролер должен как во время определения средств для обработки, так и во время самой обработки, реализуют соответствующие технические и организационные меры, такие как псевдонимизация, которые предназначены для реализации принципов защиты данных, таких как минимизация данных, в эффективный способ и интегрировать необходимые защитные меры в обработку для соответствия требованиям настоящего Регламента и защиты прав субъектов данных.

По сути, это означает, что компания, организация должна интегрировать (внедрить) защиту персональных данных в свою деятельность по обработке и все бизнес-процессы, касающиеся обработки персональных данных.

«*Privacy by default*» (ст. 25(2) Регламента): контролер должен принять соответствующие технические и организационные меры для обеспечения того, чтобы по умолчанию обрабатывались только те персональные данные, которые необходимы для каждой конкретной цели обработки.

Обязательство конфиденциальности по умолчанию распространяется на количество собранных персональных данных, степень их обработки, срок их хранения и доступность. В частности, такие меры должны обеспечивать, чтобы по умолчанию личные данные не были доступны неопределенному числу физических лиц.

6. Создать и обновлять, при необходимости, учетные записи об обработке персональных данных (records of processing activities*):

В учетных записях *контролера данных* и его представителя в ЕС (при необходимости) необходимо отобразить:

► Наименование и контактные контролера, его представителя в ЕС и Data Protection Officer (при необходимости)

► Цель обработки персональных данных

► Описание категорий субъектов данных и состав обрабатываемых персональных данных

► Категории получателей, которым персональные данные были или будут передаваться (включая трансграничную передачу)

► При необходимости передачи персональных данных третьей стране или международной организации, идентификацию такой третьей страны или международной организации

► Срок хранения персональных данных

► Общее описание технических и организационных мер защиты персональных данных

Процессор данных и, при необходимости, представитель процессора в ЕС должны вести учетные записи всех категорий обработки, осуществляющих от имени контроллера, которые содержат такую информацию:

► Наименование и контактные данные процессора и каждого контроллера, от имени которого действует процессора, и, при необходимости, представителя контроллера или представителя процессора в ЕС и Data Protection Officer

► Категории обработки, которые осуществляются от имени каждого контроллера

► При необходимости передачи персональных данных третьей стране или международной организации, идентификацию такой третьей страны или международной организации

► Общее описание технических и организационных мер защиты персональных данных

** Пример от the Information Commissioner's Office (ICO):*
https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx

7. Проведение оценки воздействия на защиту данных (Data Protection Impact Assessment)

Data Protection Impact Assessment (DPIA) – это процесс, предназначенный для описания обработки, оценки необходимости и соразмерности обработки и для помощи в управлении рисками для прав и свобод субъектов данных, возникающими в результате обработки персональных данных (путем их оценки и определения мер для устранения).

Проведение DPIA является обязательным в том случае, если обработка «может привести к высокому риску для прав и свобод субъектов данных» (ст. 35 Регламента). Это особенно актуально, когда внедряется новая технология обработки данных. Ссылка на «права и свободы» субъектов данных в первую очередь касается права на неприкосновенность частной жизни, но может также включать другие основополагающие права, такие как свобода слова, свобода мысли, свобода передвижения, запрет дискриминации, право на свободу, совесть и религию.

Некоторые примеры, когда обработка «может привести к высоким рискам»:

(a) систематическая и обширная оценка личных аспектов, касающихся физических лиц, которая основана на автоматизированной обработке, включая профилирование, и на которых основываются решения, которые создают правовые последствия в отношении физического лица или аналогичным образом оказывают значительное влияние на физическое лицо;

(b) обработка в больших масштабах специальных категорий данных, упомянутых в статье 9(1) Регламента, или персональных данных, касающихся судимости и уголовных преступлений;

(c) систематический мониторинг общедоступной территории в больших масштабах.

7. Проведение оценки воздействия на защиту данных (Data Protection Impact Assessment)

GDPR устанавливает минимальные характеристики DPIA (статья 35 (7) и пункты 84, 90 Преамбулы):

- описание предусмотренных операций обработки и целей обработки;
- оценка необходимости и пропорциональности обработки;
- оценка рисков для прав и свобод субъектов данных;
- меры, предусмотренные для устранения рисков и демонстрации соответствия Регламенту.

При этом один и тот же DPIA может использоваться для оценки нескольких операций обработки, которые схожи с точки зрения представленных рисков, при условии, что должное внимание уделяется конкретному характеру, объему, контексту и целям обработки. Это может означать, что для сбора данных одного типа для одних и тех же целей используется аналогичная технология.

Пример: железнодорожный оператор (контроллер) настраивает систему видеонаблюдения на всех железнодорожных станциях, тогда он может выполнить один DPIA.

8. Трансграничная передача персональных данных:

Если персональные данные передаются из ЕС контроллерам, операторам или получателям в третьих странах или международным организациям, уровень защиты физических лиц, который обеспечивает в ЕС Регламент, не должен быть ослаблен, в том числе в случаях дальнейших актов передачи персональных данных с третьей страны или международной организации к контроллерам, операторам в той же или другой третьей стране или международной организации. В любом случае акты передачи в третьи страны и международные организации можно осуществлять только при полном соответствии Регламенту. Передача может иметь место только в случае, если в соответствии с положениями Регламента, контроллер или оператор придерживаются условий, установленных в его положениях по передаче персональных данных в третьи страны или международных организации (п. 101 Преамбулы Регламента).

GDPR устанавливает дополнительные условия передачи персональных данных в страны, не входящие в Европейскую экономическую зону (ЕЭЗ), или международным организациям, таким образом ограничивая передачу данных и уменьшая риски для прав и свобод субъектов данных.

8. Основания осуществления ограниченного перевода данных (при трансграничной передаче):

(1) «Адекватное решение» (или «решение о соответствии») о стране, территории или определенном секторе в рамках третьей страны, или о международной организации (ст. 45 Регламента).

Если передача персональных данных происходит за пределы ЕЭЗ, но в страну, которая покрыта решением Комиссии ЕС «об адекватности», вы можете осуществить передачу без какой-либо дополнительной защиты или разрешения, т.к. такая передача данных будет аналогична передачи данных внутри ЕЭЗ.

(2) Применение соответствующих гарантий к субъекту данных при отсутствии решения об адекватности (ст. 46 Регламента).

Соответствующие гарантии: применение обязательственных корпоративных правил, стандартных положений о защите данных, принятых Комиссией ЕС, стандартных положений о защите данных, принятых контролирующим органом, или договорных положений, разрешение на которые даны контролирующим органом.

(3) Исключения (отступления) для специальных ситуаций передачи данных (ст. 49, пункты 111-113 Преамбулы GDPR).

Если планируется ограниченная передача данных, которая не покрывается ни решением об адекватности, ни соответствующими гарантиями защиты, такая передача возможна только в том случае, если на нее можно распространить одно из «исключений», изложенных в статье 49 GDPR.

8. Применение соответствующих гарантий: договорные положения о защите персональных данных (Agreement on Personal Data Transfer*):

Рекомендуется заключить соглашения об обработке/передаче персональных данных, которые должны содержать положения согласно ст. 28 GDPR. Соглашение важно для двух сторон, чтобы было понимание своих прав, обязанностей и ответственности.

В случае, если контрагент компании, организации является процессором данных, обработка персональных данных таким партнером должна регулироваться соглашением между ними (или иным правовым актом, документом).

Контроллеры могут привлекать только тех процессоров, которые могут дать достаточные гарантии того, что они будут реализовывать соответствующие технические и организационные меры, чтобы гарантировать, что их обработка будет отвечать требованиям GDPR и защищать права субъектов данных.

В случае привлечения процессором дополнительного процессора к осуществлению обработки данных от имени контроллера (т.е. субпроцессора), те же обязанности по защите данных, которые установлены между контроллером и процессором в соглашении (или ином правовом акте, документе), необходимо возложить на такого субпроцессора соглашением (или иным правовым актом, документом). Процессоры остаются ответственными перед контроллером за соответствие любых субпроцессоров, которых они задействуют.

** Standard contractual clauses for the transfer of personal data to processors established in third countries (2010/87/EU) / An alternative set of standard contractual clauses for the transfer of personal data to third countries (2004/915/EC)*

9. Обучить сотрудников компании, связанных с обработкой персональных данных:

Программа внедрения требований GDPR и дальнейшая защита персональных данных не может быть успешной без обучения сотрудников.

Рекомендуется разработать отдельную программу обучения сотрудников. При этом такое обучение не должно быть разовой акцией, т.к. в компании, организации постоянно меняются, обновляются бизнес-процессы, появляются новые практики и разъяснения в отношении норм действующего законодательства по защите персональных данных.

Если в компании, организации, обрабатывающей большой объем персональных данных, определено лицо, ответственное за обработку и защиту таких данных (Data Protection Officer), есть смысл определить ответственных сотрудников в соответствующих структурных подразделениях, которые будут взаимодействовать со специалистом по защите данных (DPO) в части имплементации требований Регламента.

Китайская поговорка гласит: «Те, кто хочет выполнить работу, должны сначала заточить свои инструменты» ☺

10. Назначить представителя в ЕС:

Согласно ст. 27 GDPR компании, организации, не учрежденные в ЕС (как контролеры, так и процессоры), но на которые распространяется действие Регламента, должны назначить своего представителя в случае, если они обрабатывают персональные данные специальных категорий («чувствительные») в больших масштабах, данные о судимостях и уголовных преступлениях, если есть вероятность риска для прав и свобод физических лиц, учитывая специфику, масштаб и цели обработки, и если они при этом не являются органами, учреждениями государственной власти.

Представителя в ЕС необходимо назначать на основании письменного поручения (мандата) контроллера или процессора действовать от его имени в контексте его обязательств по Регламенту. Такое поручение может быть частью контракта на оказание услуг.

Назначение такого представителя не влияет на обязанности или ответственность контроллера или процессора в соответствии с Регламентом. Такой представитель должен выполнять свои обязанности в соответствии с полномочиями, полученными от контроллера или процессора, в том числе, сотрудничая с компетентными контролирующими органами.

На назначенного представителя распространяется применения исполнительного производства в случае нарушений со стороны контроллера или процессора. Это включает возможность налагать административные штрафы и санкции, а также привлекать представителя к ответственности.

11. Назначить лицо, ответственное за обработку и защиту данных (Data Protection Officer):

Назначение DPO предусматривается положениями ст.ст. 13, 14, 30, 35, пунктом 4 Преамбулы GDPR.

Все компании, организации, независимо от типа или размера, которые обрабатывают персональные данные лиц, находящихся на территории ЕС, должны иметь кого-то в организации, которому поручено следить за соблюдением GDPR (часть «организационных мер», упомянутых в статье 25).

Найм фактического сотрудника по защите данных требуется только, если компания, организация (орган) соответствует одному из трех критериев:

(1) обработка персональных данных осуществляется государственным органом, за исключением судебных органов;

(2) обработка персональных данных в больших масштабах является основным видом деятельности компании, организации, которая регулярно и систематически занимается мониторингом субъектов данных;

(3) обработка специальных (чувствительных) категорий персональных данных или данных о судимостях и уголовных преступлениях в больших масштабах является частью основной деятельности компании, организации.

Основные виды деятельности, в данном контексте, рассматриваются как такие, если компании, организации нужно обработать персональные данные для достижения ключевых (основных) целей.

12. Подготовиться к утечке персональных данных:

Необходимо убедиться в наличии процедур обнаружения и расследования утечки персональных данных (нарушении данных), а также в том, что они отвечают требованиям Регламента.

В соответствии со ст. 33 GDPR, в случае утечки персональных данных и высоких рисках для субъектов данных, компания, организация должна оповестить соответствующий контролирующий орган о факте утечки без неоправданной задержки, а в случае задержки оповещения продолжительностью более 72 часов после обнаружения утечки требуется прилагать письменное объяснение причин такой задержки.

Информация о нарушении данных, которая передается в соответствующий контролирующий орган, должна содержать:

- описание факта утечки, включая количество субъектов и категории персональных данных;
- имя и контрактные детали DPO (иного ответственного лица);
- вероятные последствия такой утечки персональных данных;
- меры, предпринятые компанией, организацией для устранения утечки персональных данных и уменьшения негативных последствий такой утечки.

В определенных ст. 34 GDPR случаях компания, организация должна оповестить и субъектов данных.

Ответственность за нарушение требований GDPR

Контролирующий орган страны-участницы ЕС имеет право (ст. 58 Регламента):

(A) направлять предупреждения контроллеру или оператору;
(B) выносить выговор контроллеру или оператору;
(C) приказывать контроллеру или оператору соблюдать запросы субъекта данных;
(D) приказывать контроллеру или оператору привести операции обработки в соответствии с положениями Регламента;
(E) предписывать контроллеру сообщить субъекту данных о нарушении его персональных данных;
(F) накладывать временное или окончательное ограничение, в том числе, запрет на обработку;
(G) приказывать осуществить исправление или удаление персональных данных, или ограничение обработки;
(H) отозвать сертификацию или приказать органу сертификации отозвать сертификацию, или не выдавать сертификат;
(I) налагать административные штрафы;
(J) приказывать приостановить потоки данных получателю в третьей стране или международной организации.

Право субъектов данных на защиту:

Каждый субъект данных имеет право на подачу жалобы в контролирующий орган, без ограничения любого другого административного или судебного средства правовой защиты.

Также субъект данных имеет право напрямую обратиться в суд для защиты своих прав и интересов.

В соответствии со ст. 82 GDPR любое лицо, подвергшееся материальному или моральному вреду в результате нарушения Регламента, имеет право на получение возмещения от контроллера или оператора за причиненный вред.

Административные штрафы за нарушение требований GDPR:

(1) До **10 млн. евро или 2% от мирового годового оборота** (в зависимости что больше) за незначительные нарушения, к которым относятся нарушения контроллером и оператором статей 8, 11, 25-39, 42, 43 Регламента.

(2) До **20 млн. евро или 4% от мирового годового оборота** (в зависимости что больше) за серьезные нарушения, к которым относятся нарушения контроллером и оператором:

(a) основных принципов обработки, в том числе условия предоставления согласия, в соответствии со статьями 5, 6, 7 и 9 Регламента;

(b) прав субъектов данных в соответствии со статьями 12-22 Регламента;

(c) статей 44-49 Регламента (за передачу персональных данных получателю в третьей стране или международной организации);

(d) любых обязанностей в соответствии с законом государства-члена ЕС, принятого в соответствии с главой IX Регламента;

(e) невыполнение постановления контролирующего органа, ограничения на обработку, или приостановления потоков данных согласно решению контролирующего органа в соответствии со статьей 58(2) или непредоставление доступа как нарушение статьи 58(1) Регламента.

Страны ЕС имеют право устанавливать уголовную ответственность за нарушение требований GDPR

Результат действия GDPR

(выявленные нарушения, поданные иски, наложенные штрафы)

1. 25 мая 2018 австрийский активист и борец за конфиденциальность Max Schrems подал иски от имени организации None of Your Business против Google, Facebook, WhatsApp и Instagram на общую сумму 7,6 млрд евро. Основание - компании принудительно заставляют пользователей принимать их условия под угрозой ограничения доступа к их сервисам, не оставляя им «свободного выбора».
2. С 21 августа по 5 сентября 2018 в ходе хакерской атаки на веб-сайт и мобильное приложение British Airways произошла утеря данных с ФИО, адресами электронной почты и данных кредитных карт пассажиров. ICO расследует нарушение и предположило, что BA придется заплатить штраф, несмотря на заверения CEO, что субъектам данных будут возмещены потери на 100%.
3. 05.09.2018 Офис Информационного Комиссара (ICO) оштрафовал рекламное агентство Everything DM Ltd на 60 тыс. фунтов стерлингов за отправку 1,42 миллиона электронных писем без согласия получателей.
4. В сентябре 2018 года компания Uber подтвердила, что выплатит 133 млн. фунтов стерлингов, чтобы урегулировать все судебные иски против нее из-за кибератаки, произошедшей в 2016 году (утеря данных около 57 миллионов клиентов и водителей).
5. 01.10.2018 ICO штрафует фирму Bupa Insurance Services Limited на 175 тыс. фунтов стерлингов за то, что у него не было эффективных мер безопасности для защиты личной информации клиентов. В течение нескольких месяцев сотрудник Bupa смог извлечь личную информацию о 547 000 клиентов компании и продать ее в Интернете.
6. 50 миллионов евро составил штраф, наложенный 21 января 2019 года французским контролирующим органом (CNIL) на компанию Google за 2 вида нарушения: нарушение обязательств прозрачности и информированности (предоставленная информация не легко доступна для пользователей, некоторая информация не всегда ясна и полна), нарушение обязательства иметь законное основание для обработки данных с целью персонализации рекламы (собранное согласие не является ни «конкретным», ни «однозначным»).

Кейс с Google: подробнее

Жалоба на Google LLC была подана в CNIL двумя независимыми некоммерческими группами по защите конфиденциальности. CNIL начал свое расследование в отношении условий обслуживания и использования персональных данных для таргетинга объявлений, которые навязывается Google на сервисах, присутствующих в операционной системе Android (Google Search, Карты, Gmail и YouTube).

CNIL обнаружил, что Google не хватает прозрачности в отношении цели сбора данных, в том числе четких политик хранения данных, и что раскрытие соответствующей информации часто бывает неясным, общим или поверхностным.

Также было обнаружено, что согласие пользователя на обработку данных при таргетировании объявлений не было получено надлежащим образом, отчасти потому, что оно не было предоставлено «свободно». Раскрытие информации, касающейся операций обработки, было распространено в различных местах и связано с действиями, выполняемыми в рамках набора решений, предоставляемых Google. Это отсутствие ясности усугублялось использованием значений по умолчанию «opt-out» и общих флажков «Я согласен…», фактически предоставляющих Google широкое согласие на все, несмотря на то, что GDPR требует согласия, которое должно быть специфическим для каждой цели обработки.

В то время как Google LLC утверждала, что пользователи Android имели возможность отказаться от регистрации своей учетной записи Google при настройке Android, CNIL заметил, что этот вариант был далеко не очевиден. Кроме того, пользователи, пытающиеся отказаться от регистрации или использования учетной записи Google, были предупреждены о том, что функциональность устройства будет снижена без использования учетной записи Google.

21 января 2019 года CNIL опубликовал свое постановление, включая штраф в размере 50 миллионов евро.

Кейс с Google: какие выводы

Этот прецедент дает возможность сделать выводы о том как нельзя делать и что нужно перестроить в своей работе, особенно если ваша компания базируется за пределами ЕС и все еще не польностью соблюдает требования GDPR:

1. Убедитесь, что у вас есть четко определенное место «ведения основных хоз операций в ЕС». Как показывает опыт с Google, из-за отсутствия четкого места ведения бизнеса и назначенного DPO, обработка жалоб на не соответствие требованиям GDPR может быть в любой стране ЕС, с дополнительными требованиями к конфиденциальности, установленными в такой стране.

2. Необходимо проверить пользовательское согласие, предоставленное компании до 25 мая 2018 года. Возможно потребуется внести изменения и получить новое «правильное» согласие, соответствующее требованиям GDPR.

3. Использование настроек по умолчанию и необходимость пользователю «отказаться» от обработки его данных не соответствует требованиям GDPR (однозначное согласие).

4. Использование шаблона «Я согласен с условиями…» соответствует требованиям GDPR только применительно к конкретной операции обработки данных (для конкретной цели), а не ко всей предоставляемой услуге.

5. При определении санкций и штрафов регулирующие органы будут учитывать степень влияния нарушения на пользователей и продолжительность существования нарушения. Упреждающее решение выявленной проблемы до принятия решения регулирующим органом может снизить санкции.

Обрабатывайте чужие персональные данные так, как хотели бы, чтобы другие обрабатывали Ваши персональные данные ;)

Спасибо за внимание!