GDPR:
Практическое руководство

REVERA

Оглавление

Введение

25 мая 2018 года вступил в силу ***Регламент (General Data Protection Regulation или GDPR)***, который затрагивает деятельность многих компаний, ориентированных на европейский рынок. GDPR представляет собой единый законодательный акт по защите персональных данных, который унифицирует стандарты и правила обработки персональных данных в Европе, что позволяет бизнесу легко адаптироваться под единые требования к обработке персональных данных.

Несмотря на то, что GDPR является общеобязательным нормативным актом Европейского Союза (ЕС), он также применяется на территории всей Европейской экономической зоны. Нормы GDPR предоставляют государствам-членам вводить дополнительные требования и правила обработки персональных данных, которые будут применяться к субъектам конкретного государства.

GDPR действует не просто на компании, он применяется к бизнес-процессу по обработке персональных данных. Соответственно, если ваша компания обрабатывает персональные данные, вы можете ознакомиться с нашим обзором ключевых аспектов GDPR, который будет полезен бизнесу для начала приведения деятельности компании в соответствие с требованиями GDPR.

При несоблюдении правил, штрафы могут достигать 20 млн евро или 4% от годового мирового оборота компании (выбирается большая сумма). При этом санкции могут налагаться не только за утечки, но и за отсутствие необходимых документов или некорректно собранные согласия.

Сфера действия GDPR

Если деятельность компании, так или иначе, связана с Европейской экономической зоной (ЕЭЗ), компании необходимо проанализировать, применяется ли к ней GDPR. При этом бизнесу не обязательно иметь зарегистрированную компанию на территории ЕЭЗ, чтобы к нему применялся GDPR.

Итак, для определения, стоит ли вашей компании задуматься над тем, чтобы начать работу по внедрению требований GDPR в свои бизнес-процессы, можно ответить на вопросы ниже.

Есть ли у вашего бизнеса организационная единица на территории ЕЭЗ?

GDPR (п. 1 ст. 3) устанавливает, что его требования применимы к обработке персональных данных в рамках деятельности организационной единицы. Организационная единица подразумевает эффективное и реальное осуществление деятельности постоянных структур. Организационной единицей в контексте данной нормы может пониматься созданная на территории ЕЭЗ компания, филиал, представительство или офис. Кроме того, в отдельных случаях организационной единицей может признаваться даже отдельный работник.

Если у вашей компании есть организационная единица в одной из стран ЕЭЗ и обработка данных связана с деятельностью этой единицы, к такой обработке применяются правила GDPR.

Обрабатываете ли вы персональные данные физических лиц, находящихся в ЕЭЗ, независимо от местоположения вашей компании?

Если вы обрабатываете персональные данные лиц, находящихся в ЕЭЗ, даже если ваша организация зарегистрирована за пределами Европы, GDPR будет применим. Например, если вы храните или анализируете данные клиентов из ЕЭЗ (адреса электронной почты, имена, контактные данные и т.д.), вы обязаны соблюдать требования регламента. Обработка данных включает в себя любые операции, выполняемые с персональными данными: их сбор, запись, хранение, передачу или удаление.

Предоставляете ли вы товары или услуги, в том числе бесплатно, гражданам или резидентам ЕЭЗ?

Согласно п. 2(a) ст. 3 GDPR любые предложения товаров или услуг субъектам данных, находящимся на территории ЕЭЗ, подразумевает применимость GDPR к таким отношениям. В данном случае важно установить намерение предоставлять товары или услуги на территории одного или нескольких государств-членов. Обычная доступность вашего веб-сайта в таких государствах не означает направленность на предоставление там ваших товаров или услуг. Намерение могут подтверждать использование валюты или языка одного или нескольких государств-членов с возможностью заказывать товары и услуги на этом языке, упоминание адресов или телефонных номеров для связи со страной ЕЭЗ, использование доменного имени верхнего уровня, связанного с конкретным государством-членом (например, «.de») или с ЕС в целом («.eu»).

Отслеживаете ли вы поведение людей, находящихся в ЕЭЗ (например, с помощью аналитики, cookies или других способов мониторинга)?

Если вы отслеживаете каким-либо образом поведение людей, находящихся в ЕЭЗ, т.е. осуществляете мониторинг, то GDPR также будет применим. Однако не каждый онлайн-сбор или анализ персональных данных субъектов автоматически будет считаться мониторингом. Мониторинг включает, в частности: профилирование субъекта, анализ или прогнозирование его личных предпочтений, поведения и отношений. Например, вы будете осуществлять мониторинг, если вы предлагаете поведенческую рекламу, осуществляете геолокализацию деятельности, используете онлайн отслеживание с помощью файлов cookie. В таком случае у вас возникает обязательство по соблюдению требований регламента.

Заключаете ли вы контракты с поставщиками услуг или субподрядчиками, которые находятся в ЕЭЗ и обрабатывают персональные данные для вас?

Заключение контрактов с поставщиками услуг или субподрядчиками, которые находятся в ЕЭЗ и осуществляют обработку персональных данных в ваших интересах, попадает под сферу действия GDPR (п. 2 ст. 3). Поставщики услуг или субподрядчики будут выступать в роли процессора, т.е. лица, которое обрабатывает персональные данные от имени и по поручению контролера; а ваша организация, несмотря на регистрацию за пределами ЕЭЗ, будет являться контролером (лицом, которое самостоятельно или совместно с другими определяет цели и средства обработки персональных данных). Соответственно, на такую обработку будет распространяться сфера действия GDPR, поскольку субъект данных и процессор находятся на территории ЕЭЗ.

Заключение

Если на любой из вопросов был дан положительный ответ, GDPR распространяется на вашу деятельность, и вам необходимо соблюдать его требования. Даже если ваша организация находится за пределами ЕЭЗ, правила GDPR могут быть применимы, если вы взаимодействуете с данными граждан или резидентов ЕЭЗ. Нарушение требований GDPR может привести к серьёзным штрафам, поэтому важно тщательно изучить, как регламент может затрагивать вашу работу.

Основную информацию о сфере действия GDPR мы систематизировали в схеме ниже.

Применяется ли GDPR к вашей компании?

Если хотя бы один ответ «да» – GDPR к вам применяется

Что есть «обработка персональных данных»?

В связи с тем, что GDPR применяется только к обработке персональных данных, ключевыми понятиями данного регулирования являются «персональные данные» и «обработка».

Начнем с понимания термина «персональных данных».

> *«**Персональные данные**» — это любая информация, относящаяся к «субъекту данных», то есть идентифицированному или поддающемуся идентификации физическому лицу; поддающееся идентификации физическое лицо — это лицо, которое можно прямо или косвенно идентифицировать, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайновый идентификатор, либо на один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица.*

Понятие персональных данных встречается в законодательстве о персональных данных каждой страны. Понятие «персональных данных», в соответствии с GDPR, непосредственно связано с понятием «субъекта данных». Иными словами, подход GDPR относит к персональным данным любую информацию, которая позволяет прямо или косвенно определить (идентифицировать) конкретного человека. Подробнее вопрос идентификаторов субъекта рассмотрен в разделе «Субъекты в сфере обработки персональных данных».

Далее обратимся к понятию обработки.

> *«**Обработка**» — это любое действие (операция) или совокупность действий (операций), совершаемых с персональными данными, включая сбор, запись, организацию, структурирование, хранение, адаптацию или изменение, загрузку, просмотр, использование, раскрытие посредством передачи, распространение или иной вид предоставления доступа, сопоставление или комбинирование, сокращение, удаление или уничтожение.*

Такие действия могут совершаться как с использованием средств автоматизации, так и без использования таких средств. В контексте обработки персональных данных следует более детально остановиться на автоматизированном принятии решений.

Важно: Статья 22 GDPR содержит общий запрет на принятие решений, основанных только на автоматизированной обработке, независимо от того, предпринимает ли субъект данных какие-либо действия. Однако из этого правила существуют исключения, и, если применяется одно из них, требуется принятие необходимых мер для защиты прав, свобод и законных интересов субъекта данных.

В то же время действие данной статьи ограничено определенными случаями, когда решение, основанное только на автоматизированной обработке, включая профилирование, имеет юридические последствия для субъекта данных или аналогичным образом затрагивает его. Например, к подобным юридическим последствиям можно отнести: расторжение контракта, ошибочное предоставление социальных льгот/отказ в них, отказ в найме (при условии полного отсутствия вмешательства человека), отказ во въезде в страну и пр.

Отдельным аспектом, который необходимо затронуть, является цель обработки. Хотя в п. 2 ст. 4 GDPR не упоминает такого термина, цель определяет роль контролера данных, правовое основание обработки, определяет исключения, допускающие обработку особых категорий данных, и служит критерием минимизации данных.

В некоторых случаях одни и те же данные могут использоваться для реализации нескольких целей. Например, хранение адресов электронной почты позволяет компании:

1) осуществлять вход пользователей на свой веб-сайт,

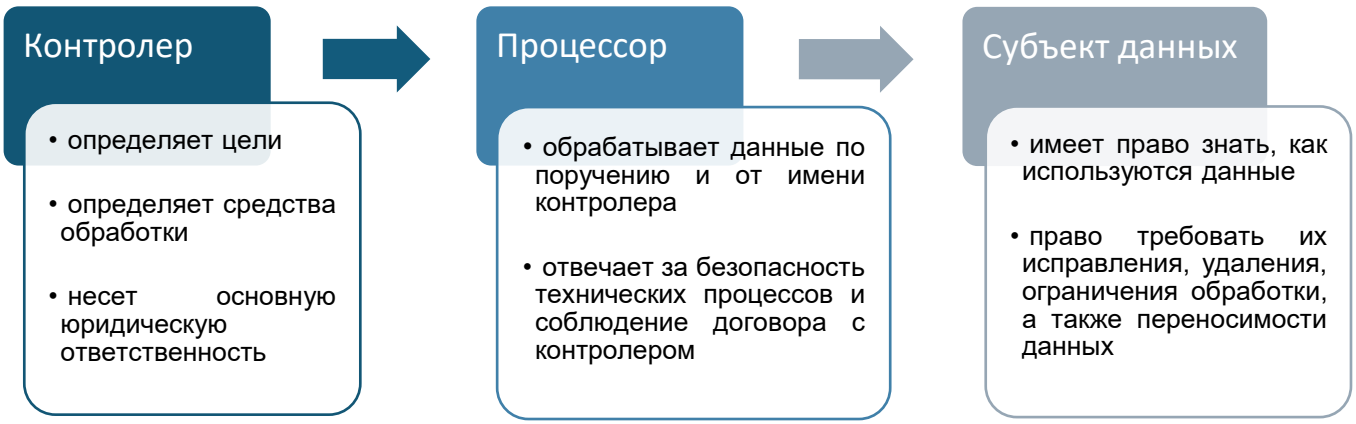
2) производить информационную и маркетинговую рассылки.

В данном случае хранение одних и тех же персональных данных как одна из операций обработки одновременно позволяет осуществлять две цели. Следовательно, прекращение действия одной из них (например, в результате отзыва согласия на рассылку маркетинговых электронных писем) не мешает компании продолжить действие другой (разрешить пользователю войти в систему).

Субъекты в сфере обработки персональных данных

В сфере обработки персональных данных можно выделить следующие категории субъектов:

1) контролер (controller);
2) процессор или обработчик (processor);
3) субъект данных (data subject).



1. Контролер

> ***«Контролер (controller)»*** *— любое физическое или юридическое лицо, государственный орган, учреждение или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных (абз. 7 п. 1 ст. 4 GDPR);*

Понятие контролера содержит 5 основных элементов, которые будут рассмотрены далее:

- ***«любое физическое или юридическое лицо, государственный орган, учреждение или другой орган»;***

  GDPR не устанавливает ограничений в отношении того, кто может быть контролером. Это может быть как организация, так и физическое лицо или группа лиц.
  Важно отметить, что в качестве контролера по смыслу GDPR выступает именно организация, а не отдельное лицо внутри нее (например, директор или DPO). В рамках группы компаний особое внимание должно быть уделено вопросу о том, может ли отдельная дочерняя компания выступать в качестве самостоятельного контролера (со-контролера), либо будет являться процессором (см. пункт 2), например, при обработке данных от имени материнской компании.

- ***«определяет»;***

  Контролер непосредственно влияет на процесс обработки персональных данных, поскольку реализует полномочия по принятию решений в отношении обработки. Контролера можно определить путем анализа юридических и фактических обстоятельств, в частности, контролер может определять цели и средства обработки на основании своих полномочий в силу закона или осуществлять контроль в силу подразумеваемых компетенций.

  Так, национальное законодательство государства-члена ЕС может предусматривать ответственность государственных органов за обработку персональных данных в рамках своих компетенций.

  В случаях, когда полномочия контролера прямо не вытекают из закона, но деятельность лица и выполняемые им функции прямо связаны с обработкой персональных данных, такое лицо будет контролером в силу подразумеваемой компетенции. Например, если организация осуществляет управление базами данных в своих целях, то она будет также обрабатывать и персональные данные, что также влечет за собой применимость законодательства о персональных данных.

- «***самостоятельно или совместно с другими»;***

  Концепция контролера не ограничивается одним субъектом. Это означает, что допустима кооперация нескольких сторон для осуществления обработки. В частности, существует такое понятие как «со-контролеры», которое означает совокупность лиц, которые совместно определяют цели и средства обработки персональных данных.

  Каждый со-контролер обязан обеспечить наличие законных оснований для обработки персональных данных и не допускать обработку персональных данных способом, несовместимым с целями, для которых они были первоначально собраны.

  Со-контролеры могут заключить соглашение по вопросам, указанным выше. Унифицированная форма такого соглашения не установлена. Однако в целях обеспечения прозрачности, правовой определенности и подотчетности EDPB рекомендует принятие обязательного документа (договора или другого юридически обязательного акта в соответствии с законодательством ЕС или государств-членов).

  Суть соглашения, в частности порядок взаимодействия со-контролеров с субъектами данных, должна быть доступна субъектам.

- ***«цели и средства»;***

  Из определения «контролера» следует, что данное лицо определяет цели и средства обработки данных. То есть контролером по смыслу регламента будет являться то лицо, которое действительно (фактически) определяет, «зачем» обрабатывать те или иные данные.

Средства обработки, в частности, включают технические и организационные меры, которые применяются при осуществлении конкретной обработки. Лицо, определяющее средства обработки, будет считаться контролером только в том случае, если оно принимает решение об «основных средствах обработки». В качестве примеров «основных средств» можно привести:

1. категории данных, подлежащих обработке,
2. период хранения данных,
3. субъекты, от которых будут получены данные,
4. право доступа к данным,
5. третьи лица, кому передаются данные и пр.

В случае, если лицо определяет указанные выше категории самостоятельно, то оно будет считаться контролером по смыслу GDPR.

Важно: юридическому лицу не обязательно иметь доступ к персональным данным, чтобы считаться контролером. Достаточно иметь возможность определять цели и средства обработки, оказывать влияние на обработку данных или инициировать такую обработку, а также иметь возможность остановить ее или получать анонимную статистику, основанную на персональных данных, собранных и обработанных другим юридическим лицом.

- ***«обработки персональных данных».***

Согласно п. 2 ст. 4 GDPR обработка — это ***любое действие (операция) или совокупность действий (операций)***, совершаемых с персональными данными с использованием средств автоматизации или без использования таких средств, включая:

1. сбор,
2. запись,
3. организацию,
4. структурирование,
5. хранение,
6. адаптацию или изменение,
7. загрузку,
8. просмотр,
9. использование,
10. раскрытие посредством передачи,
11. распространение или иной вид предоставления доступа,
12. сопоставление или комбинирование,
13. сокращение,
14. удаление или уничтожение.

Несмотря на множество перечисленных отдельных операций обработки, на практике они группируются в группы операций обработки для реализации определенной цели. Тем не менее осуществление контроля конкретным субъектом может распространяться как на всю обработку, так и быть ограничено одной отдельной операцией. В каждом из таких случаев субъект будет считаться контролером по смыслу GDPR.

2. Процессор

> ***«Процессор (processor)»*** *— физическое или юридическое лицо, государственный орган, учреждение или другой орган, который обрабатывает персональные данные от имени и по поручению контролера (абз. 8 п. 1 ст. 4 GDPR);*

В отличие от понятия «контролера» понятие «процессора» содержит только 2 основных элемента:

- ***«физическое или юридическое лицо, государственный орган, учреждение или другой орган»;***

  Так же, как и в отношении контролера GDPR не устанавливает ограничений, кто может быть процессором. Однако привлечение процессора к обработке персональных данных зависит от решения контролера, который может делегировать обработку или ее часть процессору.

  Из этого следует другая часть определения:

- ***«обрабатывает персональные данные от имени и по поручению контролера».***

  В контексте процессов обработки персональных данных процессор выполняет роль исполнителя, поскольку цели и основные средства обработки определяет контролер. Так, «обработка персональных данных от имени и по поручению контролера» означает обязанность процессора следовать установленным контролером целям и средствам обработки, и действовать исходя из его инструкций.

  Процессор в части своей компетенции может рекомендовать осуществлять обработку определенным образом, но только контролер будет принимать окончательное решение. В случае, если процессор превысит свои полномочия и станет самостоятельно определять цели и основные средства конкретной обработки, такое лицо станет классифицироваться в качестве контролера. Следовательно, будет самостоятельно нести ответственность за любые нарушения законодательства о персональных данных.

Контролер должен привлекать для осуществления обработки данных только процессоров, обладающих необходимыми знаниями и предоставляющих достаточные гарантии в отношении технических и организационных мер в соответствии с требованиями GDPR.

Любая обработка персональных данных процессором должна регулироваться договором или иным правовым актом, заключенным в письменной форме (или в электронной форме) и имеющим обязательную юридическую силу.

В GDPR содержится перечень условий, обязательных для включения в соглашение об обработке данных.

Важно: соглашение должно содержать конкретную информацию о том, как именно будут соблюдаться требования и какой уровень безопасности будет обеспечен при обработке персональных данных.

3. Субъект персональных данных

Субъектом персональных данных *по смыслу положений GDPR является физическое лицо (резидент или гражданин ЕЭЗ), которое может быть идентифицировано или поддается идентификации.*

*«**Поддающееся идентификации физическое лицо**» — это лицо, которое можно прямо или косвенно идентифицировать, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайновый идентификатор, либо на один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица.*

Таким образом, критерий идентифицируемости означает возможность отличить одного человека от другого. Как указывает определение, отличить одного человека от другого можно благодаря идентификаторам, т.е. информации, в той или иной степени характерной для конкретного человека. В данном контексте GDPR приводит ряд примеров подобных идентификаторов, поэтому далее предлагаем рассмотреть подробнее, какие идентификаторы являются прямыми, какие косвенными и всегда ли такой идентификатор как, например, имя будет персональным.

Прямые идентификаторы *— это фрагменты информации, которые можно использовать для непосредственной идентификации человека. Эти идентификаторы включают в себя такие данные, как имя, адрес, номер социального страхования и номер телефона.*

Прямые идентификаторы бывают разных видов. Так, полное имя человека в сочетании с датой его рождения может служить уникальным идентификатором. Аналогичным образом может работать комбинация адреса и номера телефона.

Однако на практике именно от контекста зависит то, действительно ли какой-либо потенциальный идентификатор, включая имя, позволяет идентифицировать человека. Например, одно только указание «И. Иванов» или «Дж. Смит» не всегда считается персональным идентификатором, поскольку существует множество людей с таким именем. В то же время, если имя сочетается с другой информацией (адресом, местом работы, номером телефона или описанием внешности человека), то таких данных зачастую достаточно для идентификации конкретного субъекта.

Косвенные идентификаторы *— это любые фрагменты информации, которые в сочетании с другой доступной информацией могут быть использованы для косвенной идентификации субъекта.*

Примерами косвенных идентификаторов являются данные, такие как возраст или пол, данные о местоположении, такие как почтовый индекс или IP-адрес, и даже некоторые характеристики, такие как род занятий или хобби. Хотя эти факторы сами по себе не могут однозначно определить личность человека, в сочетании с другими данными они потенциально могут привести к его идентификации.

Отдельно следует рассмотреть онлайновый (сетевой) идентификатор – информацию, позволяющую идентифицировать субъект в сети Интернет. К таким идентификаторам относится информация об используемом устройстве, приложениях, инструментах или протоколах, в частности (п. 30 Преамбулы):

- адреса интернет-протокола (IP);
- идентификаторы файлов cookie;
- другие идентификаторы, такие как метки радиочастотной идентификации (RFID).

Другие примеры сетевых идентификаторов, которые могут быть персональными данными, включают:

- MAC-адреса;
- рекламные идентификаторы;
- пиксельные теги;
- дескрипторы счетов;
- отпечатки пальцев устройства.

Их использование в сочетании с уникальными идентификаторами и другой информацией, полученной серверами, способно идентифицировать субъект, поэтому подлежит регулированию законодательством о персональных данных. Так, использование файлов cookie или аналогичных технологий для отслеживания действий субъекта на веб-сайтах подразумевает обработку персональных данных, если такое отслеживание включает в себя онлайн-идентификаторы, которые используются для создания профиля отдельного человека.

На этом основании GDPR устанавливает ряд требований для контролеров и процессоров в части обработки персональных данных в сети Интернет, среди которых специальные требования к оформлению cookie-баннера, обязательное наличие политики cookie и политики конфиденциальности.

В общем, система взаимоотношений между контролером, процессором и субъектом данных может быть представлена следующим образом:

Принципы обработки персональных данных

Принципы являются основополагающими нормами, на которых строится все законодательство о защите персональных данных в Европе.

Несмотря на то, что принципы не устанавливают четких правил обработки персональных данных, их понимание крайне важно, поскольку, во-первых, на принципах строится вся система правил, которым должны соответствовать компании при обработке персональных данных, а, во-вторых, нарушение принципов обработки попадает под действие максимально возможных штрафов, которые возможны в соответствии с GDPR.

Итак, GDPR устанавливает **7 принципов обработки персональных данных**:

(1) Законность, справедливость и прозрачность

Первый и один из основополагающих принципов состоит из трех элементов, каждый из которых имеет самостоятельное значение для целей обработки персональных данных:

- ***Законность***

Законность обработки в соответствии с требованиями GDPR рассматривается с двух сторон: (1) персональные данные должны обрабатываться без нарушений каких-либо законов, (2) персональные данные должны обрабатываться только при наличии правового основания обработки персональных данных (*подробнее о правовых основаниях см. раздел «Правовые основания обработки персональных данных» данного обзора*).

- ***Справедливость***

Справедливость предполагает, что персональные данные должны обрабатываться таким образом, как субъекты персональных данных разумно ожидают, чтобы такая обработка не была неоправданно пагубной, незаконно дискриминационной, вводящей в заблуждение субъекта персональных данных

- ***Прозрачность***

Прозрачность как принцип означает, что контролер должен открытым и ясным для субъекта персональных данных языком разъяснить субъекту, кем, каким образом, для чего и какие персональные данные обрабатываются. Минимальный перечень информации, которую необходимо предоставить субъекту, указан в ст. 13-14 GDPR. Для этого компании разрабатывают уведомления и (или) политики обработки персональных данных (Privacy Notices / Privacy Policies).

В марте 2020 года человек, предположительно представляющий Литовский национальный центр общественного здоровья (NVSC), обратился к разработчику мобильных приложений ITSS с просьбой создать приложение для отслеживания контактов с больными COVID-19.

NVSC и ITSS обменялись информацией о функциях приложения и сборе данных по электронной почте. Обе организации разработали политику конфиденциальности, указав себя в качестве «контролеров».

Приложение ITSS было выпущено в Google Play и App Store в апреле 2020 года. Около 3800 человек, скачавших приложение, ввели персональные данные, включая данные о местоположении и состоянии здоровья. В приложении была ссылка на веб-сайт NVSC.

К маю NVSC осознала, что не может финансировать приложение. В связи с этим проект был закрыт, и ITSS потребовала удалить из приложения любые упоминания NVSC.

В феврале следующего года литовский орган по защите данных оштрафовал NVSC на 12 000 евро и ITSS на 3 000 евро за нарушение GDPR, назвав их совместными контролерами, ответственными за персональные данные, незаконно обрабатываемые через приложение.

(2) Ограничение целью

Принцип ограничения целью заключается в том, что персональные данные должны собираться и обрабатываться только для конкретных, отчетливых и законных целей.

Например, если компания собирает адрес электронной почты пользователя мобильного приложения для создания аккаунта в игре. При этом компания решила осуществлять маркетинговую рассылку по этому адресу электронной почты. Такое использование будет грубым нарушением принципа ограничения целью.

В октябре 2024 года Суд ЕС вынес решение по делу Schrems v. Meta Platforms, касающегося того, как компания обрабатывает персональные данные для персонализированной рекламы.

Компания Meta ссылалась на договорную необходимость (статья 6(1)(b) GDPR) для обоснования своей практики поведенческой рекламы, утверждая, что таргетированная реклама является частью основного сервиса. В иске оспаривалось соответствие такого подхода принципам GDPR, касающимся законности, необходимости и согласия пользователя.

Суд постановил, что реклама не является объективно необходимой для исполнения договора между Meta и её пользователями. Таким образом, статья 6(1)(b) не может быть использована для обоснования обработки данных в целях персонализации рекламы.

Суд также усилил принцип минимизации данных (статья 5(1)(c)), заявив, что Meta собирает и обрабатывает больше данных, чем необходимо для этой цели.

В нем вновь подтверждено, что действительное согласие в соответствии со статьей 6(1)(a) должно быть дано свободно, быть конкретным, информированным и недвусмысленным и не может быть связано с общим доступом к услуге.

Также ирландская комиссия по защите данных наложила штраф в размере 310 миллионов евро на LinkedIn за незаконное использование договорной необходимости для обоснования обработки персональных данных для персонализированной рекламы.

(3) Минимизация данных

Принцип минимизации заключается в том, чтобы компании не хранили больше персональных данных, чем того требуют цели обработки. Для соблюдения данного принципа компаниям необходимо четко определить цели обработки персональных данных, а также перечень персональных данных, которые необходимы для достижения указанной цели и не допускать сбора и обработки персональных данных «на всякий случай».

В уже упоминавшемся деле Schrems v. Meta Platforms Суд ЕС разъяснил, что «хранение персональных данных пользователей платформы социальной сети в течение неограниченного периода времени в целях целевой рекламы должно считаться несоразмерным вмешательством в права, гарантированные этим пользователям GDPR». Так, принцип минимизации ограничивает персональные данные, которые могут быть использованы для целевой рекламы.

(4) Точность

GDPR требует, чтобы обрабатываемая компаниями информация была точной и актуальной и при необходимости должна обновляться. Более того, данный принцип в том числе нашел свое отражение в ст. 16 GDPR, закрепляющей право субъекта на уточнение персональных данных.

Для обеспечения данного принципа компаниям необходимо, во-первых, убедиться, что обрабатываемые персональные данные точны и актуальны, во-вторых, иметь действенные механизмы актуализации и исправления персональных данных, в случае если субъект запросил их исправление.

(5) Ограничение хранения

Указанный принцип заключается в том, что персональные данные могут храниться только в течение срока, необходимого для достижения целей их обработки. Иными словами, после истечения срока обработки персональные данные должны быть удалены или анонимизированы. Для этого, компании разрабатывают политику хранения персональных данных, а также вести реестр сроков хранения персональных данных.

В июне 2017 года берлинское Управление по защите данных провело проверку холдинговых компаний Deutsche Wohnen и подняло вопросы хранения персональных данных, в результате чего было установлено, что компании, среди прочего, нарушили принципы минимизации данных и ограничения хранения.

В 2019 году Управление провело дополнительную проверку и обнаружило, что, несмотря на внедрение новой системы хранения данных, компания продолжала хранить персональные данные как минимум 15 арендаторов без необходимости.

Управление наложило на DW несколько штрафов: один на сумму 14 385 000 евро и 15 других на сумму от 3 000 до 17 000 евро.

(6) Целостность и конфиденциальность

Данный принцип заключается в том, что компании должны предпринимать необходимые и достаточные технические и организационные меры для обеспечения защиты и целостности персональных данных, включая их защиту от случайного или несанкционированного доступа, потери, уничтожения или повреждения.

***Например,** компания имеет базу данных, где хранятся персональные данные. Права доступа к базе данных имеют все работники компании, при этом информация из базы данных необходима только некоторым работникам. Поэтому компания установила ограниченный порядок доступа к специальным персональным данным и обеспечила доступ к ним при наличии ключа доступа и пароля.*

(7) Подотчетность

Данный принцип заключается в том, что компании несут ответственность за соблюдение указанных принципов обработки и должны быть в состоянии продемонстрировать соблюдение правил обработки персональных данных.

Кроме того, данный принцип нашел отражение в иных нормах GDPR.

Например, ст. 7 GDPR устанавливает, что, если обработка производится на основании согласия, контролёр должен быть в состоянии продемонстрировать, что субъект данных дал согласие на обработку.

Согласно второму отчету Европейской комиссии о применении GDPR, опубликованному в 2024 году, с момента вступления GDPR в силу сумма штрафов за нарушение требований к обработке превысила 4,2 млрд евро. Это подчеркивает растущее внимание уполномоченных органов к соблюдению требований защиты данных и приверженность ЕС строгому правоприменению.

Важно: в своей практике Суд ЕС отмечал, что GDPR не является законом «строгой ответственности». То есть для того, чтобы уполномоченный орган наложил административный штраф, необходимо наличие «намерения или халатности», приведших к нарушению.

Правовые основания обработки персональных данных

Важно: для обеспечения принципа законности для обработки любого объема персональных данных необходимо надлежащее правовое основание.

Неправильно определенное правовое основание = отсутствие правового основания.

Согласие – не панацея, а лишь одно из возможных правовых оснований. Суждение о том, что обработка персональных данных возможна только при наличии согласия субъекта – ошибочно.

GDPR предусматривает следующие **правовые основания обработки:**

a. **согласие** (активное действие субъекта в случае, когда отсутствует иное основание для обработки персональных данных);

b. **исполнение договора** (когда обработка необходима для исполнения договора, в котором субъект данных является стороной, или для реализации шагов, предшествующих заключению договора);

c. **требование законодательства** (когда обработка необходима для выполнения правового обязательства, возложенного на контролера);

d. **жизненно важный интерес** (когда обработка необходима для защиты жизненно важных интересов субъекта персональных данных);

e. **публичный интерес** (обработка необходима для выполнения задачи в публичном интересе или в рамках осуществления государственной власти, доверенной контролеру);

f. **законный интерес** (обработка необходима для целей, вытекающих из законных интересов, преследуемых контролером или третьим лицом, за исключением случаев, когда преимущество над такими интересами имеют интересы или фундаментальные права и свободы субъекта данных, требующие защиты персональных данных, в частности, когда субъектом данных является ребенок).

Как определить правовое основание?

Вероятно, один из первых вопросов, которым задаются компании при начале обработки персональных данных – это правовое обоснование такой обработки. **Правильное определение правового основания позволяет обеспечивать законность процессов обработки персональных данных и гарантировать, что такая обработка осуществляется только в рамках определенных целей и в соответствии с законодательством.**

Как уже отмечалось ранее, нельзя использовать согласие как правовое основание во всех случаях осуществления обработки, поэтому для определения корректного правового основания в соответствии с GDPR попробуйте ответить на вопросы ниже.

1. Данные субъекта обрабатываются ввиду заключенного с ним договора (или в процессе заключения договора)?

- **Основание:** «для исполнения договора, стороной которого является субъект данных, или для принятия мер по запросу субъекта данных до заключения договора» (ст. 6b GDPR).

2. Необходима ли обработка для выполнения обязательств, предусмотренных законом?

- **Основание**: «для соблюдения юридического обязательства, которому подчиняется контролер» (ст. 6c GDPR).

3. Происходит ли обработка для защиты жизненно важных интересов (к примеру, лицо без сознания, необходимо сообщить врачам информацию об этом лице для оказания ему помощи)?

- **Основание:** «для защиты жизненно важных интересов субъекта данных или другого физического лица» (ст. 6d GDPR).

4. Необходима ли обработка в целях общественного интереса, для осуществления официальных полномочий, возложенных государством / органами государственной власти?

- **Основание:** «обработка необходима для выполнения задачи, осуществляемой в общественных интересах или при осуществлении официальных полномочий, возложенных на контролера» (ст. 6e GDPR).

5. Данные обрабатываются в рамках вашего законного интереса (т.е. законного интереса контролера)?

- **Основание:** «для реализации законных интересов контролера или третьей стороны, за исключением случаев, когда такие интересы преобладают над интересами или основными правами и свободами субъекта данных, требующими защиты персональных данных, в частности, когда субъектом данных является ребенок» (ст. 6f GDPR).

Важно: использование законного интереса как правового основания требует проведения оценки и обоснования интересов компании и интересов субъекта в такой обработке. Так же, как и в отношении согласия не рекомендуем использовать его для обоснования каждого случая обработки данных.

6. Если не подходит ничего из вышеперечисленного, то надлежащим основанием является согласие субъекта персональных данных.

- **Основание:** «обработка необходима для выполнения задачи, осуществляемой в общественных интересах или при осуществлении официальных полномочий, возложенных на контролера» (ст. 6e GDPR).

Важно: Согласие субъекта на обработку персональных данных должно быть свободным, конкретным, осознанным и недвусмысленным.

Запрос о согласии должен быть представлен в понятной и легкодоступной форме, с использованием ясного и простого языка (ст. 7 GDPR).

Важно: документирование наличия правового основания (например, согласия субъекта, обоснования законного интереса) в дальнейшем может являться подтверждением законности осуществляемой проверки при проведении аудита или проверки контролирующего органа.

Ниже приведен краткий обзор правовых оснований и наиболее частых примеров их использования:

Правовое основание	Пример использования	Ключевые аспекты
Согласие	Маркетинговая рассылка, участие в мероприятиях компании	Согласие свободное, конкретное, осознанное и недвусмысленное; избегать избыточного применения.
Договор	Использование услуг / продуктов компании, доставка товара	Только при наличии заключенного или заключаемого договора

Правовое основание	Пример использования	Ключевые аспекты
Юридическое обязательство	Предоставление налоговой отчетности, соблюдение трудового законодательства	Обязательное требование законодательства
Жизненно важный интерес	Вызов скорой помощи	Только в ситуациях, представляющих угрозу жизни или здоровью.
Общественный интерес	Государственные услуги	Государственный сектор или государственные полномочия
Законный интерес	Ответы на запросы о товарах / услугах, предоставление информации	Соблюдение баланса интересов компании и субъекта

Права субъектов в области защиты персональных данных

Помимо того, что GDPR возлагает на компании ряд обязанностей, связанных с обработкой персональных данных, он также предоставляет субъектам персональных данных права, связанные с такой обработкой.

Мы настоятельно рекомендуем всем компаниям обращать внимание на то, какие права есть у субъектов данных в связи с обработкой их персональных данных. Дело в том, что в Европе многие субъекты трепетно относятся к конфиденциальности своих персональных данных. По статистике, одним из триггеров проверок, проводимых надзорными органами, являются жалобы субъектов персональных данных. И здесь алгоритм прост: хочешь избежать проверок надзорных органов и потенциальных штрафов – уважай права субъекта и выстраивай с ним доверительные отношения.

В частности, субъекты персональных данных имеют следующие права в связи с обработкой их персональных данных:

Право на получение информации об обработке (ст. 12 GDPR)

Право на получение информации об обработке предоставляет субъекту возможность получить от организации любые сведения, связанные со сбором, использованием, хранением его персональных данных.

По запросу субъекта такая информация должна предоставляться организацией письменно в краткой, прозрачной, понятной и легко доступной форме в течение месяца (с возможным продлением срока в некоторых случаях). Как правило, взимание платы недопустимо.

Право на получение информации об обработке непосредственно связано с иными правами, предусмотренными GDPR и закрепленными в ст. 15 – 22, 34 (*см. перечень ниже*).

Право на доступ (ст. 15 GDPR)

Право на доступ предоставляет субъекту право получить от компании подтверждение о том, обрабатываются ли его персональные данные, а также получить доступ к таким персональным данным. Важно обозначить, что право на доступ распространяется не только на персональные данные, которые субъект предоставил компании, но и на те персональные данные, которые компания получила от третьих лиц либо самостоятельно собрала автоматизированным способом.

Например, *человек получает рекламную рассылку от компании и направляет запрос на доступ. В ответ компания обязана подтвердить, что обрабатывает его персональные данные, указать для каких целей и какими способами производится обработка, и предоставить копию таких данных, а также сообщить, каким образом персональные данные были получены.*

Так, данное право предоставляет субъекту право запросить у компании:

(1) подтверждение, что его персональные данные обрабатываются,

(2) доступ к следующей информации:

- цели обработки,
- получатели или категории получателей, которым передаются персональные данные субъекта,
- срок хранения или критерии, используемые для определения указанного периода,
- наличие следующих прав: удаление, исправление, ограничение обработки и возражение против обработки, подать жалобу в надзорный орган,
- источник получения персональных данных субъекта персональных данных,
- имеется ли процесс автоматизированного принятия решения, включая профилирование,
- (*если персональные данные передаются в третью страну*) имеются ли надлежащие средства защиты персональных данных в третьей стране, куда передаются персональные данные.

Какой алгоритм реагирования на такой запрос?

Компания должна предоставить копию обрабатываемых персональных данных вне зависимости от источника их получения (от субъекта, автоматическим образом, от третьих лиц), а также иную информацию, указанную выше.

Стоимость предоставления. По общему правилу указанная информация предоставляется бесплатно. Вместе с тем, GDPR устанавливает, что за любые дополнительные копии данных, компании могут взимать разумную плату.

Форма предоставления. Согласно GDPR информация может предоставляться в любой форме. Однако необходимо отметить, что форма предоставления информации во многом зависит от формы подачи запроса о реализации данного права. Так, если субъект данных подает запрос электронным способом, информация должна быть представлена в общепринятой электронной форме, если субъект данных не запрашивает иное.

Совет!

Если процесс обработки предполагает наличие у субъекта данных личного кабинета, можно реализовать в личном кабинете механизм получения доступа к информации.

Право на уточнение данных (ст. 16 GDPR)

GDPR предоставляет субъектам право на внесение изменений в персональные данные, которые обрабатываются компанией в случае, если эти персональные данные являются неточными. Кроме того, данное право предполагает наличие у субъекта данных возможности внесения дополнений в неполные персональные данные.

Важно: Право на уточнение данных распространяется только на те случаи, когда некорректная или неактуальная информация вредит достижению заявленной цели.

Например, *компания предоставляет возможность регистрации личного кабинета по адресу электронной почты для создания фотоальбомов. Готовые фотоальбомы направляются субъекту по адресу электронной почты. Субъект запросил внести изменения в адрес электронной почты. Данные изменения имеют важное значение, поскольку направление фотоальбома и иной информации по неверному адресу приведет к несанкционированному доступу к персональным данным субъекта.*

Какой алгоритм реагирования на такой запрос?

1. Компания должна без неоправданной задержки исправить неточные персональные данные и (или) дополнить персональные данные.

2. Если для достижения целей обработки компания передавала персональные данные третьим лицам, она должна сообщить им об исправлении, если только это не окажется невозможным или не потребует несоразмерных усилий.

Совет!

Если процесс обработки предполагает наличие у субъекта данных личного кабинета, можно реализовать в личном кабинете механизм исправления персональных данных, привязанных к личному кабинету и (или) быстрого направления запроса на исправление.

Право на удаление («право быть забытым») (ст. 17 GDPR)

GDPR предоставляет субъектам право удаления их персональных данных, которые обрабатываются компанией, в следующих случаях:

- персональные данные больше не нужны для целей обработки;
- субъект данных отзывает согласие на обработку и нет других правовых оснований для обработки;
- субъект данных возражает против обработки;
- персональные данные были обработаны незаконно;
- персональные данные должны быть удалены для соблюдения обязательств в соответствии с законодательством;
- персональные данные были собраны в связи с предложением услуг информационного общества, указанных в статье 8 (1).

При поступлении запроса на удаление данных организация, хранящая данные, обязана удалить их «без неоправданной задержки».

Важно: если контролер ранее обнародовал данные, подлежащие удалению, он обязан принять необходимые разумные меры, чтобы проинформировать других лиц о том, что субъект данных потребовал от них удаление любых ссылок, копий или точных повторений указанных персональных данных.

Право на ограничение обработки (ст. 18 GDPR)

GDPR позволяет субъекту требовать ограничения обработки своих персональных данных в следующих случаях:

- субъект данных оспаривает точность персональных данных — обработка ограничивается на срок, позволяющий контролеру проверить точность персональных данных;
- обработка является незаконной и субъект вместо удаления требует ограничить использование своих персональных данных;
- контролер больше не нуждается в персональных данных для обработки, но они необходимы субъекту данных для заявления, осуществления или оспаривания правовых требований и исков;
- субъект данных подал возражение против обработки — ограничение производится до завершения проверки законного интереса контролера.

В данном случае контролер имеет право только на хранение указанных персональных данных. Любая иная обработка осуществляется только с согласия субъекта данных. Допустимые исключения из этого правила относятся к заявлению, осуществлению или оспариванию правовых требований и исков, защите прав другого физического или юридического лица, важному публичному интересу ЕС или государства-члена.

Важно: контролер обязан проинформировать субъекта данных перед снятием ограничения на обработку.

Право на переносимость данных (ст. 20 GDPR)

В соответствии с GDPR субъект имеет право получить относящиеся к нему персональные данные, которые он предоставил контролеру, и передать указанные данные другому контролеру.

Контролер, которому поступил такой запрос от субъекта, обязан предоставить персональные данные в структурированном, повсеместно используемом и машиночитаемом формате.

Реализация данного права субъекта осуществляется, если:

- обработка осуществляется на основании согласия или на основании договора;
- обработка осуществляется при помощи автоматизированных средств;
- передача данных непосредственно от одного контролера другому, если это технически осуществима.

Важно: данное право не применяется для обработки в публичном интересе или при исполнении официальных полномочий, возложенных на контролера.

Право на возражение (ст. 21 GDPR)

GDPR предоставляет субъекту право на возражение против обработки, которое заключается в требовании к контролеру прекратить обработку его персональных данных. Право на возражение применяется только в отношении тех персональных данных, обработка которых осуществляется на основании согласия субъекта.

Фактически право на возражение является отзывом субъекта своего согласия на обработку персональных данных.

Важно: если компания использует персональные данные субъекта в маркетинговых целях (включая профилирование), то после получения возражения компания обязана прекратить обработку до получения нового согласия.

Право не подвергаться решениям, основанным на автоматизированной обработке (ст. 22 GDPR)

В соответствии с GDPR субъект имеет право не подвергаться решениям, основанным исключительно на автоматизированной обработке, включая профилирование, которое влечет за собой юридические последствия в отношении субъекта или аналогичным образом существенно влияет на него.

В таких случаях субъект данных имеет право:

- на вмешательство человека в процессы обработки,
- на выражение своей точки зрения,
- на оспаривание решения и на его пересмотр.

Важно: применимость этой статьи ограничена автоматизированной обработкой данных, когда решения оказывают значительное (существенное) влияние на субъектов данных. Статья устанавливает общий запрет на принятие решений, основанных только на автоматизированной обработке, независимо от того, предпринимает ли субъект данных какие-либо действия.

Совет!

Автоматизированный процесс может дать рекомендацию относительно субъекта данных. Если пользователь рассмотрит и примет во внимание другие элементы для принятия окончательного решения, это не будет решение, основанное только на автоматизированной обработке.

Контролер не может обойти требования статьи 22, создавая впечатление присутствия человека в процессе обработки.

Например, *если контролер постоянно использует автоматически созданные профили субъектов без фактического (реального) влияния на результат, это считается решением, основанным исключительно на автоматизированной обработке.*

Юридические последствия возникают, когда решение, основанное исключительно на автоматизированной обработке, затрагивает чьи-либо законные права, такие как свобода ассоциации, голосования и судебного иска, или создает юридические последствия, такие как расторжение контракта, предоставление социальных льгот/отказ в них, отказ во въезде в страну или отказ в гражданстве.

Право на подачу жалобу в надзорный орган (ст. 77 GDPR)

Право подать жалобу в надзорный орган в соответствии с GDPR выражается в возможности субъекта обратиться с возражениями в надзорный орган в государстве-члене по месту жительства субъекта, места работы или места предполагаемого нарушения, если субъект данных считает, что обработка его персональных данных осуществляется с нарушениями применимого законодательства.

Субъект также наделен правом обращения в судебный орган по вопросу нарушения его прав без ущерба для любых иных административных или внесудебных средств защиты.

Право на получение компенсации (ст. 82 GDPR)

Субъект персональных данных в случае, если ему был нанесен материальный или нематериальный ущерб, вправе требовать от контролера или процессора компенсации. Как правило, выплата компенсации возлагается на контролера.

Процессор несет ответственность за ущерб только если:

- не выполняет специальные требования GDPR в отношении процессоров,
- действует за рамками или в нарушение законных распоряжений контролера.

Если обработка осуществляется со-контролерами (или несколькими процессорами), каждый из них несет равную ответственность за весь ущерб. Если весь ущерб был возмещен одним контролером (процессором) из всех, то такое лицо может подать регрессный иск к другим контролерам (процессорам) для возмещения части выплаченной субъекту компенсации.

Освобождение от выплаты компенсации допускается в случае, если контролер (процессор) сможет доказать, что никоим образом не несет ответственность за событие, которое стало основанием для такой выплаты.

Трансграничная передача персональных данных

Передача персональных данных в иностранные государства и/или международные организации, согласно положениям GDPR, допускается только при соблюдении определенных условий:

- имеется решение Европейской комиссии об адекватности уровня защиты персональных данных в определенной юрисдикции;
- контролером или процессором обеспечиваются соответствующие гарантии защиты персональных данных за рубежом;
- субъект данных отчетливо согласился на предлагаемую передачу персональных данных, будучи проинформированным о возможных рисках такой передачи;
- передача необходима для выполнения договора между субъектом данных и контролером;
- передача необходима для заключения или исполнения договора, заключенного в интересах субъекта данных между контролёром и другим физическим или юридическим лицом;
- передача на основании публичного интереса;
- передача необходима для заявления, осуществления или оспаривания правовых требований и исков;
- передача необходима для защиты жизненно важных интересов субъекта данных или других лиц, если субъект данных физически или юридически не способен дать свое согласие;
- передача ведется из регистра, который согласно праву ЕС или государства-члена предназначен для предоставления информации общественности и который открыт для ознакомления широкой общественностью.

Схематично порядок трансграничной передачи персональных данных можно представить следующим образом (см. схему на стр. 32):

Далее рассмотрим особенности отдельных условий.

Передача данных на основании решения об адекватности (ст. 45 GDPR)

Решение об адекватности принимается Европейской комиссией. Европейская комиссия вправе пересмотреть или отменить свое решение при наличии оснований.

Трансграничная передача данных в таком случае не требует специальных разрешений. То есть передача данных в страну, в отношении которой имеется решение об адекватности, будет приравнена к передаче данных внутри ЕЭЗ.

На данный момент к таким государствам и международным организациям относятся:

- Андорра,
- Аргентина,
- Канада (есть исключения),
- Фарерские острова,
- Гернси,
- Израиль,
- Остров Мэн,
- Япония,
- Джерси,
- Новая Зеландия,
- Республика Корея,

- Швейцария,
- Великобритания,
- Соединенные Штаты (в рамках соглашения ЕС-США о защите персональных данных – EU-US Data Privacy Framework),
- Уругвай,
- а также Европейская патентная организация.

Передача данных при условии осуществления надлежащих гарантий (ст. 46 GDPR)

Если в отношении юрисдикции, куда необходимо передать данные, отсутствует решение об адекватности, GDPR допускает трансграничную передачу при условии осуществления надлежащих гарантий. Такие гарантии предоставляются с помощью:

- принятия обязательных корпоративных правил (ст. 47 GDPR);
- использования стандартных условий о защите данных, принятых Европейской комиссией или компетентным надзорным органом и утвержденных Комиссией;
- применения утвержденного кодекса поведения (ст. 40 GDPR);
- прохождения процедуры сертификации (ст. 42 GDPR).

Важно: указанные меры не освобождают контролера (процессора) от обязательств в третьей стране применить надлежащие меры для обеспечения безопасной передачи данных и реализации прав субъектов, включая эффективные средства правовой защиты.

Предоставление контролером (процессором) таких гарантий позволяет осуществлять передачу без дополнительного разрешения уполномоченного органа.

(1) Принятие обязательных корпоративных правил (ст. 47 GDPR)

Обязательные корпоративные правила – это политики защиты данных, которых придерживаются компании, зарегистрированные в ЕС, при передаче персональных данных за пределы ЕС внутри группы предприятий или организаций. Такие правила должны включать все общие принципы защиты данных и подлежащие исполнению права для обеспечения надлежащих гарантий при передаче данных. Они должны быть юридически обязательными и соблюдаться каждым заинтересованным членом группы.

Указанные правила утверждаются компетентным органом по защите данных в ЕС.

Совет!

Процедура утверждения может включать несколько надзорных органов, если группа компаний, подающая заявку на утверждение своих обязательных корпоративных правил, имеет филиалы в нескольких государствах-членах. Поэтому рекомендуется заранее изучить порядок утверждения правил в компетентных органах в каждой конкретной юрисдикции.

На заключительном этапе проект решения надзорного органа направляется в Европейский совет по защите данных, который выносит окончательное заключение по утверждению обязательных корпоративных правил.

Перечень компаний и утвержденных обязательных корпоративных правил размещены в реестре на сайте Европейского совета по защите данных.

(2) Использование стандартных условий о защите данных

Стандартные условия о защите данных или стандартные договорные положения (англ. standard contractual clauses (SCC)) – это стандартизированные положения, утвержденные Европейской комиссией, которые разрешают передачу данных за пределы ЕЭЗ.

Стандартные условия о защите данных могут быть добавлены в любое *«договорное соглашение»* между сторонами. Каждая из сторон, участвующая в трансграничной передаче, обязана подписать такое соглашение, содержащее указанные положения без каких-либо изменений.

К настоящему моменту Европейская комиссия приняла два комплекта стандартных договорных положений (доступно по ссылке):

- Стандартные договорные положения, регулирующие взаимоотношения между контролерами и процессорами;
- Стандартные договорные положения для передачи данных за пределы ЕЭЗ.

Великобритания и Швейцария одобрили стандартные договорные положения ЕС в рамках их собственного национального законодательства о защите данных с ограниченными адаптациями.

(3) Применение утвержденного кодекса поведения

Кодекс поведения представляет собой свод правил, который призван помочь участникам этого Кодекса соблюдать требования GDPR по защите данных в конкретных секторах или в отношении конкретных операций по обработке данных.

Цель Кодекса поведения: обеспечить организациями соблюдение передовой практики и правил, разработанных специально для их отрасли или их процессов обработки данных, тем самым повышая соответствие законодательству о защите данных.

Кодексы разрабатываются и управляются ассоциацией или другим органом, так называемым «Владельцем кодекса»,

1. представляющим *определенную отрасль* (или категорию контролеров или процессоров),
2. обладающим *экспертными знаниями и опытом* в данной отрасли о том, как повысить уровень защиты данных в своем регионе.

Важно: Кодексы принимаются *только* от ассоциаций или других организаций, представляющих различные категории контролеров или обработчиков данных.

Кодексы поведения могут быть как «национальными» (охватывающими деятельность по обработке данных в одном государстве), так и «транснациональными» (охватывающими деятельность по обработке данных в нескольких государствах-членах).

«Национальные» кодексы утверждаются уполномоченным государственным органом по защите данных, «транснациональные» кодексы – Европейским советом по защите персональных данных.

GDPR обязывает Европейскую комиссию обеспечить доступ общественности к утвержденным кодексам, которые были определены как обладающие всеобщим действием.

На Европейский совет по защите персональных данных возлагаются функции перенести все утвержденные кодексы поведения, их изменения и дополнения в реестр и довести их до всеобщего сведения. Ознакомиться с утвержденными Европейским советом по защите персональных данных кодексами поведения можно на его официальном сайте.

Совет!

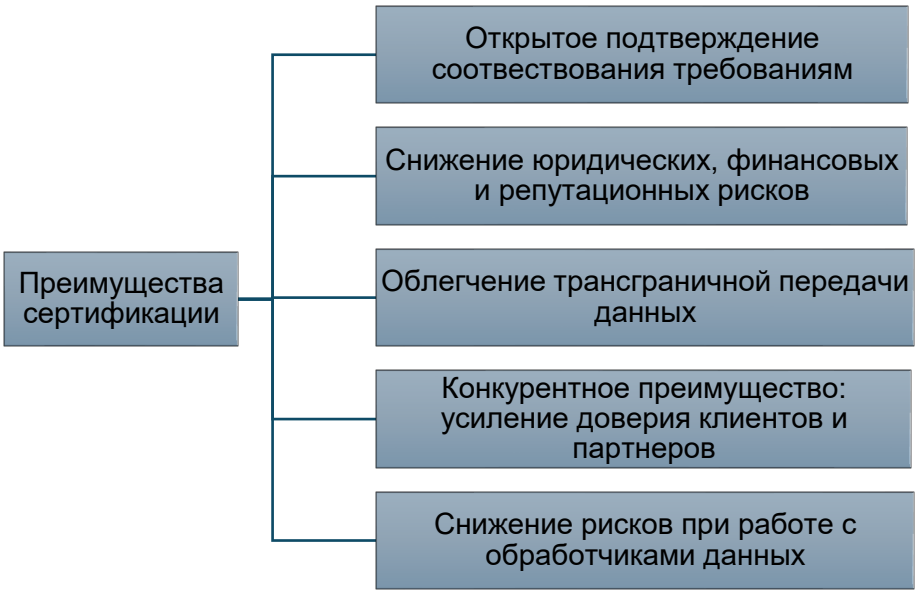
В случае ведения деятельности в нескольких государствах-членах ЕС целесообразно ориентироваться на транснациональные кодексы поведения, утвержденные Европейским советом по защите персональных данных и включенные в официальный реестр, поскольку их применение способствует унификации подходов к обработке данных и снижает риск расхождений в требованиях национальных надзорных органов. Регулярная проверка актуальности кодексов в реестре Европейского совета по защите персональных данных позволяет своевременно учитывать внесенные изменения и дополнения в практической деятельности.

(4) Прохождение процедуры сертификации

Сертификация позволяет компании демонстрировать меры соответствия законодательству о персональных данных как отдельным лицам, так и другим организациям, с которыми она сотрудничает, а также надзорным органам.

Цель сертификации: подтвердить соответствие деятельности компании в сфере персональных данных GDPR.

Важно отметить, что сертифицируется не сама компания, а разработанные и применяемые ею меры защиты данных.



Если компания решит пройти сертификацию, первое, что нужно сделать, — это убедиться, что деятельность компании действительно соответствует GDPR (подробнее об этом в разделе «*Минимум, чтобы соответствовать GDPR*»). На данном этапе рекомендуется выбрать приоритетные виды деятельности обработки данных, которые хотите сертифицировать.

Проверить соответствие можно следующими способами:

- Привлечь квалифицированных поставщиков услуг для проведения аудита;
- Самостоятельно оценить процессы компании.

Совет!

В обоих случаях необходимо документально подтвердить соответствие выбранной обработки данных критериям. Поэтому для ускорения и упрощения процесса подготовки документов можно воспользоваться услугами специалистов.

После документирования соответствия необходимо направить запрос и выбрать квалифицированный орган по сертификации для проведения аудита.

После аудита и проверки соответствия объекта оценки орган по сертификации примет решение о выдаче сертификата соответствия, действительного в течение трех лет с возможностью продления.

В случае с европейским знаком защиты данных «*Europrivacy*» сертификаты публикуются в онлайн-реестре, что позволяет проверить действительность и подлинность выданных сертификатов.

Важно: Сертификация не уменьшает ответственность контролера или процессора за допущенные нарушения GDPR.

Полномочия надзорных органов

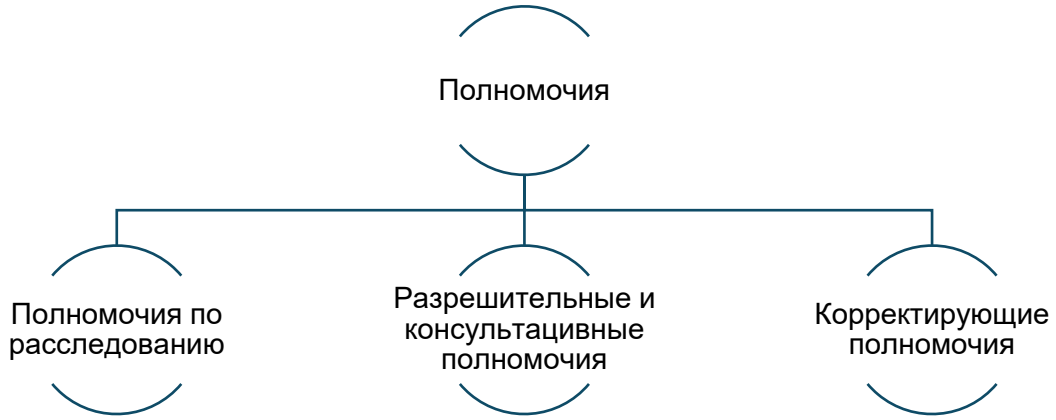
В Европейском Союзе двухуровневая система надзорных органов.

На уровне Европейского Союза действует надзорный орган European Data Protection Board, в чьи функции входит обеспечение последовательного применения законодательства ЕС в области защиты персональных данных во всех государствах, на которых оно распространяется, а также содействие сотрудничеству между национальными надзорными органами по защите данных.

Однако наибольший интерес для компаний представляют национальные органы по защите персональных данных, поскольку именно национальные органы рассматривают жалобы субъектов, применяют корректирующие меры, в т.ч. применяют штрафы на компании в случае выявления нарушений.

На уровне GDPR урегулирован порядок создания надзорных органов, их компетенция и полномочия, которые могут дополняться на уровне местного законодательства.

Все полномочия, предусмотренные GDPR, разделены на **три группы.**



Полномочия по расследованию

Первая группа полномочий – это полномочия по расследованию. Указанная группа полномочий направлена на обеспечение согласованного и единого подхода к рассмотрению жалоб субъектов персональных данных, проведении аудитов соблюдения компаниями требований GDPR и иного регулирования в сфере защиты персональных данных.

К полномочиям по расследованию относятся следующие полномочия надзорных органов:

a) требовать от компаний предоставления любой информации, необходимой для выполнения задач надзорных органов;

b) проводить расследования в форме аудитов защиты данных;

c) получить от компаний доступ ко всем персональным данным и всей информации, необходимой для выполнения задач надзорного органа;

d) получить доступ к любым помещениям компаний, а также к оборудованию и средствам для обработки данных;

e) иные полномочия.

Разрешительные и консультационные полномочия

Вторая группа полномочия – разрешительные и консультационные. Данная группа полномочий направлена на обеспечение единого подхода к применению правил GDPR и оказании компаниям содействия в толковании требований GDPR.

К данной группе полномочий относятся, в частности такие полномочия, как:

a) консультирование контролера в соответствии с порядком предварительной консультации;

b) принятие стандартных условий по защите данных в контексте заключения контролером договора с процессором или осуществления трансграничной передачи;

c) выдавать заключение и утверждать проекты кодексов поведения;

d) выдавать сертификаты и утверждать критерии сертификации;

e) утверждать обязательные корпоративные правила.

Корректирующие полномочия

Заключительная группа полномочий надзорных органов – корректирующие полномочия. Данная группа полномочий направлена на предотвращение дальнейших нарушений контролёрами. По своей сути корректирующие полномочия близки к мерам ответственности, которые применяются в случае несоблюдения установленных GDPR требований к обработке. Как правило, для компаний данная группа полномочий имеет одно из самых важных значений, поскольку данные полномочия могут связаны с какими-либо материальными потерями вследствие наложения штрафа или наложения каких-либо ограничений на обработку.

К корректирующим полномочиям относятся следующие полномочия надзорных органов:

a) делать предупреждения, если обработка данных нарушает положения GDPR;

b) потребовать от компании удовлетворения запроса субъекта данных относительно осуществления его прав согласно GDPR;

c) потребовать, при необходимости, от компаний приведения процесса обработки данных в соответствие с положениями GDPR в установленном порядке и в установленный срок;

d) наложить временное или окончательное ограничение на обработку данных, включая запрет обработки;

e) наложить административный штраф;

f) потребовать приостановить передачу данных получателю в третьей стране;

g) иные корректирующие полномочия.

Ответственность

В зависимости от серьезности нарушения GDPR устанавливает разные меры ответственности. Как правило, основной мерой ответственности является административный штраф. Такой штраф должен быть эффективным, сдерживающим и соразмерным.

При решении вопроса о наложении административного взыскания и установлении его размера надзорным органом принимается во внимание, в частности:

- характер, тяжесть и продолжительность нарушения с учетом характера, объема или цели обработки, количества пострадавших субъектов данных и размера причиненного им вреда;
- преднамеренный или непреднамеренный характер нарушения (умышленно или по неосторожности);
- любые действия, предпринятые контролером или процессором для уменьшения ущерба, причиненного субъектами данных;
- предыдущие нарушения со стороны контролёра или процессора;
- категории персональных данных, пострадавших в результате нарушения;
- любые другие отягчающие или смягчающие факторы, применимые к обстоятельствам дела.

1. Административный штраф в размере до 10 000 000 евро или 2% от годового мирового оборота, а в случае субъекта хозяйствования — до 2% от общего годового мирового оборота за предыдущий финансовый год (в зависимости от того, что выше) налагается за нарушения:

- обязанностей контролёра и процессора;
- обязанностей сертифицирующего лица;
- обязанностей контролирующего органа.

2. Административный штраф в размере до 20 000 000 евро или 4% от годового оборота, а в случае субъекта хозяйствования — до 4% от общего годового мирового оборота за предыдущий финансовый год (в зависимости от того, что выше) налагается за нарушения:

- основных принципов обработки, в том числе условий согласия;
- прав субъектов данных;
- передачи персональных данных получателю в третьей стране или международной организации;
- любых обязательств согласно законодательству государства-члена ЕЭЗ об отдельных случаях обработки;
- предписания о временном или постоянном ограничении на обработку либо о приостановке передачи данных, изданного надзорным органом.

Важно: в случае, если контролер или процессор умышленно или по неосторожности допускает несколько нарушений в пределах одной обработки (нескольких связанных операций обработки), общая сумма административного штрафа не должна превышать сумму штрафа за наиболее серьезное нарушение.

Важно: если законодательство государства-члена ЕЭЗ не содержит такой меры ответственности как административный штраф, он все равно может быть наложен решением компетентного национального суда по инициативе надзорного органа.

Минимум, чтобы соответствовать GDPR

Рассмотрев основные положения и требования GDPR, подведем итоги того, что минимально необходимо компании, чтобы соответствовать GDPR, если компания попадает под действие данного документа.

1. Провести анализ обрабатываемых персональных данных

Проведение аудита обрабатываемых персональных данных – первый шаг для приведения деятельности компании в соответствие с требованиями GDPR. Поскольку обработка должна быть законной, прозрачной и справедливой необходимо:

- определить объем (категории) всех обрабатываемых компаний персональных данных (т.е. определить какие именно данные собираются и у каких субъектов);
  Такие данные могут содержаться, например, в базах данных клиентов или заказов, во внутренних системах бизнес-процессов, в формах обратной связи или отзывах, заполненных клиентами, письмах в корпоративной электронной почте.
- определить для каких целей обрабатываются данные (цель обязательно должна быть четкой и конкретной, чтобы соблюсти принципы ограничения обработки целью и минимизации данных).

Важно: если в ходе анализа процессов обработки выявится, что компанией обрабатываются избыточные данные (т.е. данные, обработка которых не является необходимой для достижения указанных целей), такую обработку необходимо прекратить, а сами данные удалить во избежание штрафов за нарушения требований обработки.
Исходя из цели обработки определяется правовое основание, а также срок хранения персональных данных.

2. Составить перечень всех третьих лиц, которые имеют доступ к персональным данным

После того, как все категории данных и цели их обработки были определены, необходимо проанализировать деятельность компании на предмет того, кто вне компании имеет доступ к персональным данным. Это могут быть:

- аффилированные лица,
- государственные органы (по требованию),
- подрядчики (например, хостинг-провайдеры или рекламные компании).

Если компания поручает кому-то обработку персональных данных, то следует удостовериться, что:

- компания имеет заключенное в письменной форме обязательное соглашение о порядке обработки данных с таким лицом (DPA).
- процессор соответствует требованиям GDPR (обеспечивает надлежащие организационные и технические меры, имеет соответствующие знания и опыт в сфере защиты персональных данных).

3. Проверить законность осуществления трансграничной передачи данных

Поскольку GDPR предъявляет достаточно строгие требования к трансграничной передаче данных, необходимо проверить, что компания не передает персональные данные за пределы ЕС или в страны, признанные Европейской комиссией странами, не обеспечивающими адекватный уровень защиты прав субъектов данных.

Важно: если, например, сервер, на котором находится сайт компании, расположен в стране, которая не находится в утвержденном Европейской комиссией перечне стран с надлежащими гарантиями прав субъектов данных, то это будет признано незаконной передачей данных, при условии того, что сайт может собирать персональные данные (формы обратной связи, отзывы).

В случае, если компанией была выявлена трансграничная передача данных в «небезопасные» страны, требуется наличие дополнительных мер и оснований для того, чтобы такая передача была признана законной. В частности:

- субъект данных отчетливо согласился на предлагаемую передачу персональных данных, будучи проинформированным о возможных рисках такой передачи;
- передача необходима для выполнения договора между субъектом данных и контролером.

Важно: контролером или процессором должны обеспечиваться соответствующие гарантии защиты персональных данных за рубежом. На практике это, как правило, означает заключение соглашения о передаче данных с «небезопасной» стороной. Под таким соглашением обычно понимаются Standard Contractual Clauses (SCC) – положения о защите данных, разработанные Европейской комиссией. SCC гарантируют, что передача и обработка персональных данных соответствуют нормативным актам ЕС, в частности GDPR.

4. Разработать необходимые документы

Ключевым документом, который необходимо разработать, в соответствии с GDPR является политика обработки персональных данных или политика конфиденциальности.

Политика конфиденциальности обязательно должна содержать информацию:

- о контролере,
- о целях обработки данных,
- о категориях обрабатываемых данных,
- о правовых основаниях обработки,
- о сроках хранения данных,
- о третьих лицах, кому передаются данные и для каких целей,
- о трансграничной передаче данных (если применимо),
- о перечне принимаемых мер для защиты данных,
- о правах субъектов данных и порядке их реализации,
- о назначенном DPO (корпоративный адрес электронной почты).

Политика конфиденциальности должна содержать положение о том, что компания не обрабатывает персональные данные лиц, моложе 16 лет, только если компания не работает целенаправленно с детской аудиторией или детским контентом.

Политика конфиденциальности компании обязательно должна быть представлена для ознакомления пользователям на официальном сайте компании (если применимо) или иным способом размещена в открытом доступе в целях соблюдения прав субъектов на информирование и сохранения прозрачности обработки.

Помимо политики конфиденциальности на сайте необходимо разместить политику обработки файлов-cookie (может быть как частью политики конфиденциальности, так и самостоятельным документом) и cookie-баннер, требования к которым регулируются e-Privacy Directive.

Также внутри компании следует:

- разработать порядок доступа сотрудников к персональным данным,
- хранить документы, подтверждающие согласие субъекта на обработку,
- составлять отчеты о создании, удалении, изменении персональных данных,
- вести учет обращений субъектов данных.

Всю информацию необходимо поддерживать в актуальном состоянии.

5. Принять соответствующие организационные и технические меры

Для соответствия GDPR требуется обязательное принятие организационных и технических мер. Конкретный комплекс мер определяется компанией индивидуально. Главное – они должны обеспечивать действительную эффективную защиту персональных данных.

Минимальный объем технических и организационных мер включает в себя:

- псевдонимизацию и шифрование персональных данных;
- способность обеспечить постоянную конфиденциальность, целостность, доступность и устойчивость систем и сервисов обработки;
- способность своевременно восстанавливать доступность персональных данных в случае возникновения физического или технического инцидента;
- регулярное тестирование, оценку и измерение эффективности технических и организационных мер по обеспечению безопасности обработки;
- оценку достаточности уровня безопасности и учет рисков, связанных с обработкой, в частности, рисков случайного или незаконного уничтожения, потери, изменения, несанкционированного раскрытия или доступа к переданным, хранимым, или другим образом обрабатываемым персональным данным.

6. Назначить DPO

Назначение DPO является обязательным в определенных случаях, в частности, если компания:

- обрабатывает данные значительного числа субъектов данных; или
- осуществляет систематический и широкомасштабный мониторинг их поведения.

Другие контролеры имеют право по своему усмотрению назначать DPO.

DPO в соответствии с GDPR обязано обладать соответствующими теоретическими и практическими знаниями в области защиты данных.

DPO обязан:

- информировать и консультировать контролера (процессора) и работников, которые обрабатывают персональные данные, о возложенных на них обязанностях в соответствии с GDPR и иными нормами ЕС в сфере защиты персональных данных;
- осуществлять мониторинг соблюдения GDPR, других норм ЕС в сфере защиты персональных данных, а также локальных нормативных правовых актов контролёра или процессора в области защиты персональных данных,
- осуществлять распределение обязанностей, повышение осведомленности, обучение персонала, участвующего в операциях по обработке, и соответствующие аудиторские проверки;
- предоставлять запрашиваемые рекомендации касательно оценки воздействия на защиту персональных данных и контролировать ее осуществление;
- сотрудничать с надзорным органом;
- выступать в качестве контактного лица для надзорного органа по вопросам, связанным с обработкой, и при необходимости консультировать по любому другому вопросу.

Важно: DPO должен осуществлять свои обязанности объективно и независимо. Подотчетен DPO только высшему должностному лицу компании.

Функции DPO могут выполняться сотрудником компании или другим лицом (лицами) на основании договора об оказании услуг.

Контролер и процессор обязаны обеспечить надлежащее вовлечение сотрудника по защите персональных данных в процесс принятия важных решений, касающихся обработки данных, предоставить ему/ей соответствующие ресурсы и обеспечить его/ее автономию при осуществлении деятельности.

Заключение

Мы рассмотрели ключевые теоретические и практические аспекты применения GDPR, начиная со сферы действия и понятия «обработки данных» и заканчивая положениями об ответственности, а также обязательным минимумом для соответствия GDPR. Особое внимание уделено разъяснениям европейских уполномоченных органов по защите данных, примерам и практическим кейсам.

Надеемся, что этот обзор станет для вас полезным инструментом, который не только ответит на ваши вопросы, но и позволит начать процесс по приведению деятельности вашей компании в соответствие с требованиями GDPR. Если у вас возникнут дополнительные вопросы или потребуется профессиональная поддержка, наша команда экспертов всегда готова помочь.

С уважением,

***Епихова Людмила**, юрист практики IT&IP REVERA law group.*

***Маглыш Александра**, юрист практики IT&IP REVERA law group.*