REVERA

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. КЛЮЧЕВЫЕ ТЕЗИСЫ ДЛЯ БИЗНЕСА

ОГЛАВЛЕНИЕ

ПОЧЕМУ ЭТО ВАЖНО

Регулирование сбора и использования персональных данных берёт начало с защиты права на неприкосновенность частной жизни. С усилением влияния Интернета, ускорением распространения информации возникает проблема неконтролируемого использования данных о гражданах, их поведении и предпочтениях.

Получив доступ к персональным данным, бизнес стал использовать их в целях, не связанных с оказанием услуг — для анализа поведения пользователей, составления их рекламных профилей, разработки механизмов для манипулирования поведением. Вместе с этим набирают обороты нарушения в сфере защиты частной жизни, кибербезопасности, становятся распространёнными утечки персональных данных.

С целью ограничения неконтролируемого использования персональных данных и их защиты государства принимают специальные законы, решающие вопросы обработки персональных данных. Государства по-разному решают вопрос защиты персональных данных. Некоторые подробно регулируют вопросы использования персональных данных любыми компаниями (ЕС, РФ и пр.), другие закрепляют минимальный набор обязанностей и точечно вопросы защиты персональных данных (модель «лоскутного одеяла» в США).

В связи с неоднородным регулированием однозначно определить, что собой представляют персональные данные и какой объём обязанностей возлагается на оператора, практически невозможно. Ниже будут анализироваться наиболее популярные и распространённые подходы.

ЧТО ТАКОЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Единого понятия персональных данных не закреплено — каждое государство раскрывает его значение самостоятельно.

На международном уровне персональные данные были определены в Конвенции Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера, согласно которой «персональные данные» означают любую информацию об определенном или поддающемся определению физическом лице. Конвенция стала основой для развития законодательства членов Совета Европы, которые понимают «персональные данные» максимально широко.

Как правило, к персональным данным относят информацию о человеке (субъекте персональных данных), которая самостоятельно или вместе с использованием иной информации идентифицирует или может позволить идентифицировать такого человека.

К персональным данным может относиться практически любая информация, начиная с ФИО, места жительства, работы граждан, их идентификационного или налогового номера и пр., заканчивая данными о поведении, передвижении, взглядах, предпочтениях, убеждениях конкретного лица, его IP адресе, рекламном профиле и пр.

В то же время, законодательство конкретного государства может сужать или по-своему интерпретировать понятие «персональных данных», поэтому для определения объёма регулирования и требований к операторам персональных данных нужно изучать законодательство конкретного государства и его правоприменительные подходы.

КАКИМИ МОГУТ БЫТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Персональные можно разделить на виды по их характеру и степени «чувствительности», уязвимости. От вида персональных данных зависят условия их обработки, предоставления доступа к персональным данным, требования к их защите.

Как правило, выделяют следующие виды персональных данных:

1) **персональные данные**, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, половой жизни и пр.;

2) **биометрические данные**, касающиеся физических, физиологических или поведенческих характеристик человека, которые предоставляют их уникальную идентификацию (изображение лица человека, дактилоскопические данные и пр.);

3) **генетические данные** — данные в отношении унаследованных или приобретенных характеристик человека, которые получены в результате анализа его биологических материалов (например, в результате анализа хромосом, ДНК или РНК).

4) **персональные данные в общедоступных источниках**;

5) **иные данные** — остальные персональные данные, не относящиеся к вышеперечисленным.

Наиболее уязвимыми являются первые три вида персональных данных, которые, как правило, подлежат особой защите.

КАК ПОНЯТЬ, КАКИЕ ПРАВИЛА ПРИМЕНЯЮТСЯ К РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Под обработкой персональных данных, как правило, понимаются все действия, которые связаны с их сбором, хранением, изменением, использованием, передачей, распространением, систематизацией, удалением, уничтожением, обезличиванием и пр. Поэтому, если компания каким-либо образом связана с использованием персональных данных как в коммерческих, так и некоммерческих целях (в том числе при обработке данных своих работников), необходимо провести анализ законодательства государств, в которых работает компания и в которых находятся её клиенты.

После этого необходимо определить применимое международное и национальное регулирование, понять, какие из требований распространяются или могут распространяться на бизнес и проанализировать риски, связанные с возможностью продолжения работы на рынке (штрафные санкции, возможность блокировки ресурсов и пр.).

Возможны ситуации, когда компания может подпадать под регулирование нескольких юрисдикций (например, при обработке информации о гражданах из нескольких государств). В таком случае нужно соответствовать требованиям нескольких юрисдикций.

КАК РЕГУЛИРУЕТСЯ РАБОТА С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

ЕВРОПЕЙСКИЙ СОЮЗ

ЗАКОНОДАТЕЛЬСТВО

Основным источником регулирования защиты персональных данных является General Data Protection Regulation (GDPR), который вступил в силу с 25 мая 2018 года.

ОСНОВЫ РЕГУЛИРОВАНИЯ

«Персональные данные» — любая информация, которая прямо идентифицирует лицо (ФИО, паспортные данные) или косвенно (пол, локация, онлайн идентификаторы), а также любая информация, которая относится к лицу, которое было или может быть идентифицировано (поведение, действия, передвижения и т.д.)

«Обработка персональных данных» — любые операции, которые выполняются с персональными данными.

«Процессор» — обрабатывает персональные данные от имени контроллера.

«Контролер» — самостоятельно определяет цели и средства обработки персональных данных.

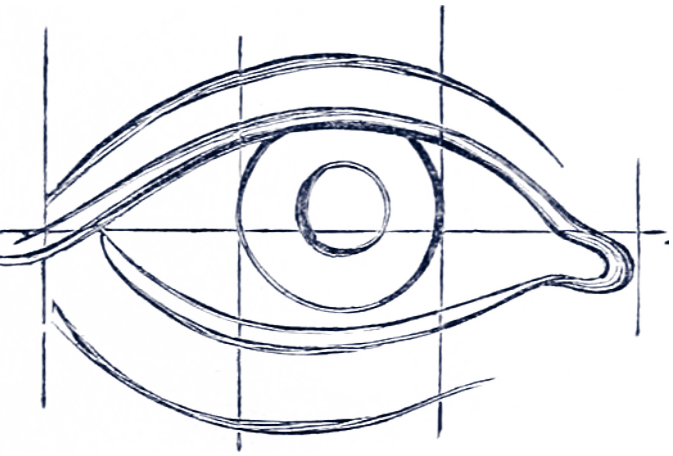
СФЕРА ДЕЙСТВИЯ GDPR

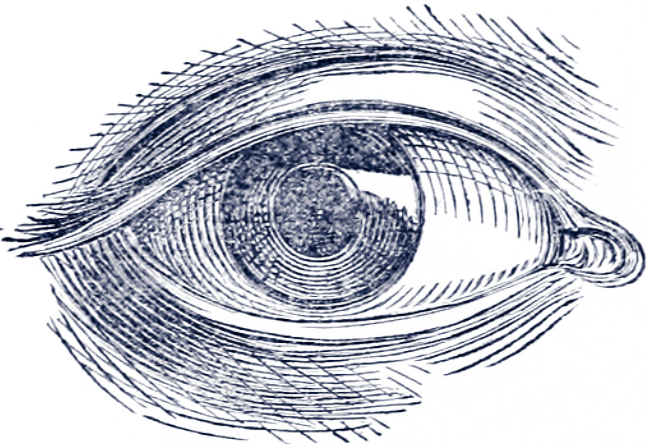
GDPR имеет экстерриториальное действие и применяется ко всем компаниям, обрабатывающим персональные данные лиц, которые находятся на территории ЕС, независимо от местонахождения такой компании.

ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для того, чтобы обрабатывать персональные данные согласно GDPR у компании должно быть хотя бы одно из 6 возможных оснований обработки:

1. Согласие субъекта персональных данных;
2. Необходимость исполнения договора с субъектом персональных данных;
3. Легитимный интерес;
4. Жизненно важный интерес;
5. Требования законодательства;
6. Выполнение задачи в общественных интересах или при осуществлении официальных полномочий контролера.





ТРЕБОВАНИЯ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

GDPR закрепляет ряд принципов, на которых должна основываться обработка персональных данных:

1) **Законность, справедливость, прозрачность —** персональные данные можно обрабатывать только при наличии одного из шести законных оснований.
2) **Целевое ограничение —** персональные данные могут обрабатываться только для конкретной цели, о которой должно быть известно субъекту персональных данных.
3) **Минимизация данных —** персональные данные могут обрабатываться только в объеме, необходимом для достижения заявленной цели..
4) **Точность —** данные должны быть точными и при необходимости обновляться; неактуальные данные должны быть удалены.
5) **Ограничение хранения данных —** персональные данные должны храниться не дольше срока, необходимого для достижения целей их использования.
6) **Целостность и безопасность —** при обработке персональных данных должна обеспечиваться защита от случайной потери, уничтожения или повреждения с использованием соответствующих технических или организационных мер.

ОТВЕТСТВЕННОСТЬ

GDPR предусматривает два вида штрафов в следующем размере:

1) **до 10 миллионов евро** или **2% от годового оборота** компании за прошлый финансовый год (в зависимости от того, что больше);

2) **до 20 миллионов евро** или **4% от годового оборота** компании за прошлый финансовый год (в зависимости от того, что больше). Повышенный размер штрафа предусмотрен, например, за нарушение принципов обработки данных, прав субъектов персональных данных и иные нарушения.

КАЛИФОРНИЯ

ЗАКОНОДАТЕЛЬСТВО

Основу законодательства штата Калифорния (США) о защите персональных данных составляет California Consumer Privacy Act (CCPA), который вступил в силу с 1 января 2020 года.

ОСНОВЫ РЕГУЛИРОВАНИЯ

«Персональные данные» — информация, которая прямо (имя, паспортные данные, водительское удостоверение) или косвенно (куки, номер телефона, IP) идентифицирует потребителя или домохозяйство, биометрические данные (внешность, отпечатки пальцев), геолокация, действия в интернете (история браузера, история поиска) и чувствительные данные (медицинские данные, данные о трудоустройстве, образовании).

СФЕРА ДЕЙСТВИЯ

CCPA применяется к компаниям, которые ведут бизнес и обрабатывают данные потребителей из штата Калифорния, если они соответствуют хотя бы одному из следующих условий:

a) Годовой валовый доход компании превышает 25 миллионов долларов США;
b) Компания ежегодно покупает, получает, либо продает персональные данные 50 000 и более потребителей, домохозяйств или устройств;
c) Компания получает не менее 50% своей прибыли от продажи персональных данных потребителей.

ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

CCPA обязывает компании при обработке персональных данных соблюдать следующие требования:

1. Предоставлять потребителям информацию о процессах обработки их персональных данных, их правах в отношении персональных данных, в том числе обновлять политику обработки персональных данных не реже, чем один раз в 12 месяцев;

2. Обеспечивать механизм реализации прав пользователей, в том числе обеспечивать технические средства (например, размещение соответствующей ссылки на веб-сайте или в мобильном приложении), чтобы потребитель мог запретить компании продавать его персональные данные. При этом потребителю не может быть отказано в предоставлении услуг или предложены другие условия их предоставления по причине того, что потребитель реализовал какие-либо права, предоставляемые ему CCPA, в том числе запретил продавать свои персональные данные.

3. Верифицировать личность потребителей, которые направляют запросы.

4. Хранить записи о полученных запросах и ответах на них в течение 24 месяцев.

На компании, которые обладают персональными данными более чем 4 миллионов потребителей, налагаются дополнительные обязанности.

ОТВЕТСТВЕННОСТЬ

Размер штрафов составляет 2,500 долларов США за каждое нарушение и 7,500 долларов США за каждое умышленное нарушение. То есть, за непреднамеренное нарушение требований CCPA в отношении 10 000 потребителей штраф достигнет 2,5 миллионов долларов США, а при наличии умысла — 7,5 миллионов долларов США.

Сам потребитель, чьи права были нарушены, может требовать от компании компенсации в размере от 100 до 750 долларов США.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ЗАКОНОДАТЕЛЬСТВО

Российская Федерация является участником Конвенции Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера и взяла на себя обязательства по её исполнению.

- Основными законами в сфере защиты персональных данных в Российской Федерации, являются:
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»);
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ.

Также здесь принят ряд подзаконных нормативных актов, связанных с требованиям к защите персональных данных, информационным системам и пр., в том числе акты Правительства, ФСТЭК, ФСБ, Роскомнадзора и пр.-

ОСНОВЫ РЕГУЛИРОВАНИЯ

Российское законодательство выделяет следующие основные понятия:

- «Персональные данные» — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Российская практика толкует понятие персональных данных широко и включает в их число ФИО, налоговые и страховые номера, места проживания, работы, информацию о поведении пользователей, фото-, видеоизображения, файлы cookie, IP адреса и пр.;

- «Обработка персональных данных» — любое действие (операция) или их совокупность с использованием средств автоматизации или без их использования, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- «Оператор персональных данных» — лицо (государственный орган, муниципальный орган, юридическое или физическое лицо), самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие состав персональных данных, подлежащих обработке, цели обработки, действия (операции) с персональными данными.

СФЕРА ДЕЙСТВИЯ ЗАКОНОДАТЕЛЬСТВА

При определении сферы действия российские госорганы ориентируются на «таргетинговый» критерий, согласно которому иностранные сервисы, нацеленные на российский рынок, обязываются соблюдать основные требования российского законодательства о персональных данных. В этих целях на практике выработаны основные и дополнительные критерии, при совпадении которых Интернет-ресурсы и прочие операторы, работающие на российском рынке, признаются «таргетированными» на российский рынок и обязываются соблюдать требования российского законодательства.

ОСНОВАНИЯ ОБРАБОТКИ ПД

Российское законодательство закрепило основания, которые могут использоваться для обработки персональных данных. В их число входят:

- согласие субъекта персональных данных;
- исполнение договора, в котором субъект персональных данных является стороной, выгодоприобретателем или поручителем;
- осуществление прав и законных интересов оператора;
- достижение общественно значимых целей;
- выполнение обязанностей, возложенных на оператора законом;
- обработка в статистических или иных исследовательских целях при условии обезличивания персональных данных;
- защита жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение его согласия невозможно;
- иные основания, указанные в ФЗ «О персональных данных».

Наиболее распространённым и применимым основанием для обработки персональных данных считается получение согласия субъекта персональных данных. При этом в ряде случаев согласие должно быть оформлено только в письменной форме. К таким случаям относится трансграничная передача персональных данных в неадекватные юрисдикции, работа со специальными персональными данными и пр.

УВЕДОМЛЕНИЕ О НАЧАЛЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

До начала обработки персональных данных операторы обязаны направить уведомление о начале обработки персональных данных в специальный уполномоченный орган по защите прав субъектов персональных данных, функции которого осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Требование не распространяется в некоторых случаях (например, при обработке персональных данных в соответствии с трудовым законодательством и пр.).

Такие уведомления направляют как российские субъекты, так и иностранные компании в случае, если они попадают под «таргетинговый» критерий.

ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В Российской Федерации отдельно регламентируются вопросы методов и способов защиты персональных данных, которые должны в обязательном порядке предпринять операторы при обработке.

К числу таких мер, в том числе, относятся:
- назначение лица, ответственного за организацию обработки персональных данных;
- организация режима обеспечения безопасности помещений, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях;
- обеспечение сохранности носителей персональных данных;
- утверждение перечня лиц, доступ которых к персональным данным необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ, когда применение таких средств необходимо для нейтрализации актуальных угроз.

ТРЕБОВАНИЯ ЛОКАЛИЗАЦИИ

Операторы обязаны обеспечить при сборе персональных данных запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением некоторых случаев, указанных в ФЗ «О персональных данных».

В декабре 2019 года в КоАП Российской Федерации были внесены изменения, согласно которым установлена ответственность за невыполнение данного требования – штраф на юридическое лицо до 6 000 000 RUB (около 97 700 USD) за первое нарушение, и до 18 000 000 RUB (около 293 130 USD) за последующие нарушения.

ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА

Российское законодательство устанавливает особые правила передачи персональных данных в юрисдикции, не обеспечивающие адекватную защиту персональных данных. К таким странам относятся государства, не являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и не определённые Роскомнадзором в качестве стран, обеспечивающих адекватную защиту прав субъектов персональных данных.

Оператор может осуществлять трансграничную передачу персональных данных в «неадекватную» юрисдикцию по ограниченному перечню оснований. В их число входит получение согласия субъектов персональных данных в письменной форме (на бумажном носителе).

ОТВЕТСТВЕННОСТЬ

Российское законодательство предусматривает специальные меры воздействия на операторов персональных данных.

Блокировка интернет-ресурсов (сайтов, приложений и пр.), нарушающих права субъектов персональных данных.

Применение мер по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований закона.

Гражданско-правовая ответственность: взыскание убытков, компенсация морального вреда.

Применение административных взысканий: максимальный размер штрафа — до 18 000 000 RUB (около 293 130 USD) за нарушение требования о локализации. За другие нарушения в сфере защиты персональных данных – до 75 000 RUB (около 1 222 USD).

Уголовная ответственность: за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, а также за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

РЕСПУБЛИКА БЕЛАРУСЬ

ЗАКОНОДАТЕЛЬСТВО

Основным актом в сфере защиты персональных данных является Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» (Закон «Об информации, информатизации и защите информации»).

Также действуют иные акты в сфере обработки и защиты персональных данных, в том числе:

- Закон от 21.07.2008 № 418-З «О регистре населения» (Закон «О регистре населения»);
- Положение о технической и криптографической защите информации в Республике Беларусь, утверждено Указом Президента от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»;
- иные акты, которые связаны с обработкой персональных данных в отдельных сферах (архивное дело, перевозки и пр.).

По состоянию на февраль 2020 года Республика Беларусь не является участником Конвенции Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера и не приняла отдельного акта, регулирующего обработку персональных данных.

ОСНОВЫ РЕГУЛИРОВАНИЯ

Понятие персональных данных. Согласно абз.23 ст. 1 Закона «Об информации, информатизации и защите информации» к персональным данным относятся две категории данных:

- основные и дополнительные персональные данные, вносимые в регистр населения;
- иные данные, позволяющие идентифицировать физическое лицо;

К данным, вносимым в регистр населения, относятся (п.1 ст. 8, п.1 ст. 10 Закона «О регистре населения»):

- идентификационный номер;
- фамилия, собственное имя, отчество (если таковое имеется);
- пол;
- число, месяц, год рождения;
- место рождения;
- цифровой фотопортрет;
- данные о гражданстве (подданстве);
- данные о регистрации по месту жительства и (или) месту пребывания;
- данные о смерти или объявлении физического лица умершим, признании безвестно отсутствующим, недееспособным, ограниченно дееспособным.
- данные о родителях, опекунах, попечителях, семейном положении, супруге, ребенке (детях) физического лица;
- данные о высшем образовании, ученой степени, ученом звании;
- данные о роде занятий;
- данные о пенсии, ежемесячном денежном содержании по законодательству о государственной службе (далее — ежемесячное денежное содержание), ежемесячной страховой выплате по обязательному страхованию от несчастных случаев на производстве и профессиональных заболеваний;
- данные о налоговых обязательствах;
- данные об исполнении воинской обязанности;
- данные об инвалидности.

Белорусское законодательство не относит напрямую к персональным данным «косвенные» персональные данные и не регулирует вопросы использования «электронных» идентификаторов - следов, которые оставляют субъекты при использовании Интернета.

Не регулируется также обработка биометрических, генетических, специальных персональных данных, персональных данных в общедоступных источниках.

Операторы персональных данных. Понятие «оператора персональных данных» в белорусском законодательстве нет, при этом выделяются такие субъекты информационных отношений, как оператор информационной системы, владелец и собственник программно-технических средств, информационных ресурсов, информационных систем и информационных сетей, которые обязаны принимать меры по защите персональных данных и соблюдать права субъектов персональных данных.

Иные понятия, связанные с работой с персональными данными (обработчика персональных данных, обработки персональных данных, субъектов персональных данных и пр.) в белорусском законодательстве не закреплены.

ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Основное основание – получение письменного согласия физического лица. Отдельных требований к форме, содержанию, условиям предоставления такого согласия в законодательстве не установлено.

Случаи, когда сбор, обработка, хранение, использование персональных данных могут осуществляться без согласия субъекта персональных данных могут устанавливаться законодательными актами. Например, к таким случаям относится сбор, обработка, хранение, использование данных о владельцах доменных имён для формирования централизованной базы данных о доменных именах (подп. 1.2. Указа Президента от 18.09.2019 № 350 «Об особенностях использования национального сегмента сети Интернет»).

ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Закон «Об информации, информатизации и защите информации» закрепляет некоторые права субъектов персональных данных:

- право на недопустимость принуждения к предоставлению персональных данных (статья 18 Закона);
- право на ознакомление с персональными данными (статья 34 Закона);
- защита персональных данных с целью её сохранения и неразглашения (статья 27 Закона);
- право на предоставление согласия на последующую передачу персональных данных (статья 32 Закона);

ОТВЕТСТВЕННОСТЬ

Законодательство не исключает применение общей дисциплинарной, гражданско-правовой, административной, уголовной ответственности за нарушение требований в сфере обработки и защиты персональных данных.

Ответственность за разглашение персональных данных содержится в ст. 22.13 КоАП Республики Беларусь, согласно которой умышленное незаконное разглашение персональных данных лицом, которому персональные данные известны в связи с его профессиональной или служебной деятельностью, (если в этих деяниях нет состава преступления) влечёт наложение штрафа в размере от 4 до 20 базовых величин (приблизительно от 51 до 255 USD).

Статья 179 УК устанавливает ответственность за незаконное собирание либо распространение сведений о частной жизни, составляющих личную или семейную тайну, без его согласия, повлекшие причинение вреда правам, свободам и законным интересам потерпевшего. Статья 349 УК устанавливает ответственность за несанкционированный доступ к компьютерной информации.

ПЛАНИРУЕМЫЕ ИЗМЕНЕНИЯ В ЗАКОНОДАТЕЛЬСТВО РЕСПУБЛИКИ БЕЛАРУСЬ

В июне 2019 года в первом чтении был принят проект Закона «О персональных данных», который изменит подход к регулированию вопросов защиты персональных данных и закрепит новые права и обязанности, механизмы защиты субъектов персональных данных.

Основные изменения коснутся следующих вопросов.

ПОНЯТИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласно проекту **«персональные данные»** — любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано на основании такой информации.

«Физическое лицо, которое может быть идентифицировано» — физическое лицо, которое может быть прямо или косвенно определено, в частности, через идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Преимущество нового определения заключается в том, что оно конкретизирует основные признаки персональных данных и позволяет относить к таким данным информацию, косвенно идентифицирующую субъектов персональных данных, а также онлайн-идентификаторы.

НОВЫЕ ПОНЯТИЯ

Субъект персональных данных — физическое лицо, в отношении которого осуществляется сбор, обработка, распространение, предоставление персональных данных. Законопроект не указывает гражданство субъектов персональных данных, что позволяет защищать права всех лиц, обработка персональных данных которых производится операторами.

Оператор персональных данных — лицо (в т.ч. госорган, государственный орган, ИП, иные физлица, юрлица Республики Беларусь, иные организации), которое самостоятельно или совместно осуществляет одно или несколько действий с персональными данными, таких как сбор, обработка, распространение, предоставление персональных данных. Определение не устанавливает в качестве критерия для отнесения к «операторам персональных данных» установление состава, целей, объёма обработки персональных данных, что позволяет относить к операторам фактически любое лицо, которое осуществляет действия с персональными данными.

Законопроект выделяет также «лиц, осуществляющих сбор, обработку, распространение, предоставление персональных данных по поручению оператора» и обязывает Оператора заключать с ними договор на обработку персональных данных.

ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Законопроект разделяет следующие действия, которые могут осуществляться с персональными данными:

- сбор персональных данных — действия, направленные на получение персональных данных субъекта персональных данных, включая аудиозапись, фото- и видеосъемку;
- предоставление персональных данных — действия, направленные на ознакомление с персональными данными определенного лица или круга лиц;
- распространение персональных данных — действия, направленные на ознакомление с персональными данными неопределенного круга лиц;
- обработка персональных данных — любое иное действие или их совокупность, кроме вышеназванных, совершаемые с персональными данными, включая систематизацию, хранение, изменение, использование, обезличивание, блокирование, удаление персональных данных;

Таким образом, сама по себе «обработка» персональных данных интерпретируется уже, чем в странах ЕС и РФ.

ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Основным основанием для работы с персональными данными остаётся согласие субъекта персональных данных. Уточнено, что такое согласие должно быть свободным, конкретным и информированным.

Согласие может быть получено в письменной форме, в виде электронного документа или в иной электронной форме. Надлежащим согласием также будет считаться проставление «галочки» или ввод кода, полученного по СМС или по электронной почте. Могут быть установлены случаи, когда получение согласия возможно только в письменной форме. «Молчаливое» согласие не считается надлежащим.

Законопроект устанавливает перечень случаев, когда операторы вправе осуществлять действия с персональными данными без согласия субъекта:

- заключение, исполнение договора, стороной которого является субъект персональных данных;
- при оформлении трудовых отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных;
- в научных или иных исследовательских целях при условии обязательного обезличивания персональных данных;
- обязательность действий в соответствии с требованиями законодательных актов;
- в случаях, когда законодательными актами прямо предусматривается возможность сбора, обработки, распространения, предоставления персональных данных без согласия субъекта персональных данных;
- иных целях, указанных в законопроекте (реализация норм по борьбе с коррупцией, ведение административного или уголовного процесса, назначение и выплаты пенсий, пособий и пр.).

ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

Законопроект разграничивает по типу государства, обеспечивающие и не обеспечивающие надлежащий уровень защиты персональных данных. Перечень «надлежащих» и «ненадлежащих» юрисдикций будет определён уполномоченным органом по защите прав субъектов персональных данных.

Проект закона запрещает передачу персональных данных в «ненадлежащие» юрисдикции, за исключением случаев если:

- дано согласие субъекта персональных данных;
- заключается или исполняется договор, стороной которого является субъект персональных данных;
- персональные данные могут быть получены любым лицом посредством направления запроса;
- персональные данные являются общедоступными;
- передача осуществляется в рамках исполнения международного договора Республики Беларусь;
- передача осуществляется органом финансового мониторинга в целях принятия мер по предотвращению легализации доходов;
- получено разрешение уполномоченного органа по защите прав субъектов персональных данных.

ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Законопроект уточняет и дополняет список прав субъектов персональных данных, а также устанавливает механизмы их реализации. В число таких прав входит:

- право на получение от операторов информации о правах, связанных с действиями с персональными данными;
- право давать согласие на действия с персональными данными;
- право на получение информации об обработке персональных данных (информация об операторах, персональных данных, источниках их получения, основаниях и целях сбора, иная информация, указанная в Законе и иных законодательных актах);
- право знакомиться с персональными данными;
- право изменять персональные данные;
- право на получение информации о предоставлении персональных данных третьим лицам;
- право на требование о прекращении обработки и удаление персональных данных при определённых обстоятельствах;
- право на отзыв согласия на действия с персональными данными;
- право на обжалование действий (бездействий), решений оператора.

ОБЯЗАННОСТИ ОПЕРАТОРОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Законопроект закрепляет новые обязанности операторов, которые будут обязаны:

- разъяснять права субъектам персональных данных;
- получать согласие субъектов персональных данных, прекращать обработку в случаях, когда это обязательно;
- обеспечивать защиту персональных данных, в том числе:
- назначить лицо или структурное подразделение, ответственное за действия с персональными данными;
- издать и опубликовать политику осуществления действий с персональными данными;
- установить процедуры, направленные на предотвращение нарушений законодательства о персональных данных, устранения их последствий;
- установить порядок доступа к персональным данным;
- обучать сотрудников, работающих с персональными данными;
- осуществлять техническую и криптографическую защиту информации;
- уведомлять уполномоченный орган о нарушениях систем защиты ПД.

УПОЛНОМОЧЕННЫЙ ОРГАН

Законопроект предусматривает создание уполномоченного органа по защите прав субъектов персональных данных. В число полномочий такого органа будет входить:

- контроль сбора, обработки, распространения, предоставления персональных данных операторами в порядке, установленном законодательством о контрольной (надзорной) деятельности;
- рассмотрение жалоб субъектов персональных данных по вопросам сбора, обработки, распространения, предоставления персональных данных;
- правомочие требовать от оператора изменения, удаления или блокирования недостоверных или полученных незаконным путем персональных данных, устранения иных нарушений;
- предоставление разрешения на трансграничную передачу персональных данных, если в другом государстве не обеспечивается надлежащий уровень их защиты;
- разъяснения по вопросам применения законодательства о персональных данных;
- участие в работе международных организаций по вопросам защиты персональных данных;
- иные полномочия, предусмотренные законопроектом и иными законодательными актами.

Уполномоченный орган будет определяться Президентом Республики Беларусь.