Защита персональных данных

Гаглоев Сергей Гивич,
заместитель руководителя
Управления Федеральной службы
по надзору в сфере связи,
информационных технологий и
массовых коммуникаций по
Омской области

Основные понятия

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

Субъект персональных данных – физическое лицо

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

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

Уполномоченный орган по защите прав субъектов персональных данных –

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

На территории Омской области функции уполномоченного органа по защите прав субъектов персональных данных осуществляет

Управление Роскомнадзора по Омской области

Нормативные правовые акты

Конституция Российской Федерации от 12.12.1993 г.

Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ

Кодекс РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»

Постановление Правительства РФ от 6.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Федеральный закон «О персональных данных»

не распространяется на отношения, возникающие при:

1. Обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушается права субъектов персональных данных;

2. Организации хранения, комплектования, учёта и использования содержащих персональные данные документов Архивного фонда РФ и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3. Обработке подлежащих включению в единый государственный реестр индивидуальных предпринимателей сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством Российской Федерации в связи с деятельностью физического лица в качестве индивидуального предпринимателя.

Принципы обработки персональных данных

1. Обработка ПД должна осуществляться на законной и справедливой основе.

2. Обработка ПД должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только ПД, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых ПД должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке ПД должны быть обеспечены точность ПД, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПД. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение ПД должно осуществляться в форме, позволяющей определить субъекта ПД, не дольше, чем этого требуют цели обработки ПД, если срок хранения ПД не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПД. Обрабатываемые ПД подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Условия обработки персональных данных

В соответствии с п. 1 ч. 1 ст. 6 Федерального закона «О персональных данных» обработка персональных данных может осуществляться с согласия субъекта персональных данных на обработку его персональных данных

Этой же статьёй предусмотрены случаи, когда обработка персональных данных возможна без согласия субъекта персональных данных, в том числе в случаях когда обработка персональных данных:

- необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом;
- осуществляется в связи с участием лица в судопроизводстве;
- необходима для исполнения полномочий федеральных органов исполнительной власти, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления;
- необходима для осуществления профессиональной деятельности журналиста;
- необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- в иных предусмотренных законом случаях.

Конфиденциальность персональных данных

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Меры, которые обязан принять оператор для обеспечения безопасности персональных данных

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Согласие субъекта персональных данных на обработку его персональных данных

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии предусмотренных законом оснований

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия предусмотренных законом оснований возлагается на оператора

Обязанности оператора по защите персональных данных

Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством о персональных данных. К таким мерам могут относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки ПД законодательству, политике оператора в отношении обработки ПД, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам ПД в случае нарушения законодательства о персональных данных;

6) ознакомление работников оператора, непосредственно осуществляющих обработку ПД, с положениями законодательства о ПД, в том числе требованиями к защите ПД, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Примерный перечень документации оператора по выполнению требований законодательства о персональных данных

Политика оператора в отношении обработки данных;
Приказ о назначении ответственного (ответственных) за обработку персональных данных;
Инструкция ответственного за организацию обработки персональных данных;
Приказ о допуске к обработке ПД (с указанием должностей и ФИО работников);
Приказ об утверждении перечня обрабатываемых ПД;
Приказ об утверждении перечня помещений, в которых ведется обработка ПД, и Положения о порядке доступа в помещения, в которых ведется обработка ПД;
Приказ об утверждении Положения об обработке ПД без использования средств автоматизации;
Приказ об утверждении перечня систем персональных данных;
Инструкция пользователя информационной системой персональных данных (ИСПДн);
Журнал учета прав доступа к ИСПДн;
Инструкция по учету лиц, допущенных к работе с ПД в ИСПДн;
Инструкция пользователя ИСПДн при возникновении нештатных ситуаций;
Приказ об определении границ конролируемой зоны;
Инструкция для проведения инструктажа лиц, допущенных к работе с ИСПДн, журнал прохождения первичного инструктажа работников, допущенных к работе с ПД и ИСПДн;
Инструкция по порядку уничтожения и обезличивания ПД в ИПДн, акты уничтожения;
Инструкция по антивирусной защите в ИСПДн;
Инструкция по проведению внутреннего контроля соответствия обработки ПД требованиям к защите ПД;
Формы документов (согласие на обработку ПД, соглашение о неразглашении информации, содержащей ПД, акт уничтожения ПД и т.п.).

Ответственность операторов за нарушения законодательства Российской Федерации в области персональных данных (согласно ст. 13.11 КоАП РФ)

Вид нарушения	Санкция			
	Преду-преждение	Штраф (в тыс. рублей) на:		
		граждан	Должн.лиц	Юр.лиц
Обработка ПД в случаях, не предусмотренных законодательством, либо обработка ПД, несовместимая с целями сбора персональных данных	возможно	1 – 3	5 – 10	30 – 50
Обработка ПД без согласия в письменной форме субъекта ПД в случаях, когда в соответствии с законодательством такое согласие должно быть получено, либо обработка ПД с нарушением требований к составу сведений, включаемых в такое согласие	нет	3 – 5	10 – 20	15 – 70
Невыполнение оператором обязанности по обеспечению неограниченного доступа к документу, определяющему политику оператора в отношении обработки ПД, или сведениям о реализуемых требованиях к защите ПД	возможно	0,7 – 1	3 – 6	15 – 30
Невыполнение оператором обязанности по предоставлению субъекту ПД информации об обработке его ПД	возможно	1 – 2	4 – 6	10 – 15
Невыполнение оператором требования об уточнении, блокировании или уничтожении ПД, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки	возможно	1 – 2	4 – 10	25 – 45
Невыполнение оператором при обработке ПД без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих сохранность ПД, если это повлекло неправомерные действия в отношении ПД	нет	0,7 - 2	4 - 10	25 - 50
Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию ПД либо несоблюдение установленных требований или методов по обезличиванию ПД	возможно	–	3 – 6	–

Благодарим за внимание