Утверждено приказом
№ 78 от 01.09.2012

Положение по обработке и защите персональных данных

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с законодательством Российской Федерации о персональных данных (далее по тексту - ПДн) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в информационных системах ПДн (далее — ИСПДн).

1.2. В целях настоящего Положения используются следующие термины:

персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

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

автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники;

распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц;

предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и /или в результате которых уничтожаются материальные носители ПДн;

обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3. Настоящее Положение определяет порядок и условия обработки ПДн в ООО «Русский Стандарт» (далее по тексту - Оператора), включая порядок передачи ПДн третьим лицам, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн, систему защиту ПДн, порядок организации внутреннего контроля и ответственность за нарушения при обработке ПДн, иные вопросы.

1.4. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передачу), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.5. Настоящее Положение вступает в силу с момента его утверждения Генеральным директором Оператора и действует бессрочно, до замены его новым Положением.

1.6. Все изменения в Положение вносятся приказом.

1.7. Все работники Оператора должны быть ознакомлены с настоящим Положением под роспись.

2. Цели и задачи обработки ПДн

2.1. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

2.2. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

2.3. Обработке подлежат только ПДн, которые отвечают целям их обработки.

2.4. Содержание и объем, обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

2.5. Обработка ПДн сотрудников Оператора может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Оператора.

2.6. Основными целями обработки ПДн является: исполнение договорных обязательств, предусмотренных в трудовых контрактах с сотрудниками;

2.7. ИСПДн обеспечивает решение следующих задач: Формирование регламентированной отчетности.

3. Персональные данные, обрабатываемые в ИСПДн

3.1. В ИСПДн обрабатываются ПДн следующих субъектов ПДн:

3.1.1. сотрудники Оператора;

3.1.2. кандидаты для приема на работу;

3.1.3. индивидуальные предприниматели — контрагенты Оператора;

3.2. Данный перечень может пересматриваться по мере необходимости.

3.3. Персональные данные субъектов ПДн включают:

фамилия, имя, отчество ; дата рождения ; место рождения ; семейное положение ; профессия ; адрес проживания ; образование ; доходы ; месяц рождения ; год рождения ;

а также, специальные категории персональных данных: национальная принадлежность ;

3.4. Полные списки обрабатываемых ПДн формируются в перечне ПДн, подлежащих защите в ИСПДн Оператора.

4. Доступ к ПДн

4.1. Сотрудники Оператора, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают допуск к необходимым категориям ПДн на срок выполнения ими соответствующих должностных обязанностей на основании перечня лиц, допущенных к работе с ПДн, который утверждается Руководителем Оператора. Перечень составлен на основе Концепции информационной безопасности и Политики информационной безопасности.

4.2. Список лиц, имеющих доступ к ПДн для информационной системы, должен поддерживаться в актуальном состоянии.

4.3. Оператором установлен разрешительный порядок доступа к ПДн. Сотрудникам Оператора предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей на основании решения Руководителя

4.4. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником Оператора по согласованию Руководителя.

4.5. Доступ к ПДн третьих лиц, не являющихся сотрудниками Оператора без согласия субъекта ПДн, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с разрешения Руководителя Оператора.

4.6. В случае если сотруднику сторонней организации необходим доступ к ПДн Оператора, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней организации и ее сотрудников по соблюдению требований текущего законодательства в области защиты ПДн. Кроме того, в случае доступа к ПДн лиц, не являющихся сотрудниками Оператора, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Оператором с субъектом ПД.

4.7. Доступ сотрудника Оператора к ПДн прекращается с даты, прекращения трудовых отношений, либо даты изменения должностных обязанностей сотрудника и/или исключения сотрудника из списка лиц, имеющих право

доступа к ПДн. В случае увольнения все носители, содержащие ПДн, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы, должны быть переданы соответствующему должностному лицу.

5. Основные требования по защите ПДн

5.1. При обработке ПДн в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и/или передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к ПДн;

в) недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль над обеспечением уровня защищенности ПДн.

5.2. Оператор обязан принимать необходимые правовые, организационные, технические и другие меры для обеспечения безопасности ПДн.

5.3. Для разработки требований по обеспечению безопасности и внедрения системы обеспечения безопасности ПДн Оператором разработана "Модель угроз безопасности ПДн при их обработке в ИСПДн" на основе нормативно-методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

5.4. Оператором в соответствии с руководящим документом государственных органов - приказом ФСТЭК России, ФСБ России и Минсвязи России от 13 февраля 2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» осуществлена классификация ИСПДн Оператора.

5.5. Комиссией составлен Акт классификации ИСПДн, обрабатываемых с использованием средств автоматизации:

Акт классификации ИСПДн
Дата классификации ИСПДн
Класс ИСПДн

Акт классификации ИСПДн
13 января 2008 года
3

5.6. Оператором на основании Акта проверки ИСПДн и в соответствии с нормативно-методическим документом ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» разработан и внедрен комплекс мер по защите и обеспечению безопасности ПДн ("План мероприятий по обеспечению безопасности ПДн").

5.7. Оператором используется технические средства и программное оборудование для обработки и защиты ПДн.

5.8. Оператором при необходимости ведется журнал учета и хранения съемных носителей информации.

5.9. Вышеуказанные технические средства ИСПДн размещаются в офисе и помещениях Оператора.

5.10. Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн должны быть под роспись ознакомлены с требованиями настоящего Положения, а также должны подписать «Соглашение об обеспечении конфиденциальности персональных данных сотрудниками Оператора», приведенного в Приложении к настоящему Положению.

5.11. Оператором организован процесс обучения использования средств защиты ПДн, эксплуатируемых Оператором. Обучение по данному направлению рекомендовано лицам, имеющим постоянный доступ к ПДн, и лицам, эксплуатирующим технические и программные средства ИСПДн и средств защиты ИСПДн. В обязательном порядке обучение должны проходить лица, ответственные за эксплуатацию средств защиты информации ИСПДн.

5.12. Сотрудники обязаны незамедлительно сообщать соответствующему должностному лицу Оператора об утрате или недостаче носителей информации, составляющей ПДн, а также о причинах и условиях возможной

утечки ПДн. В случае попытки посторонних лиц получить от сотрудника ПДн, обрабатываемых Оператором незамедлительно известить об этом соответствующее должностное лицо Оператора.

6. Согласие на обработку ПДн

6.1. Субъект ПДн принимает решение о предоставлении своих ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством РФ. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Оператором. (ст.9 закона)

6.2. Получение письменного согласия на обработку ПДн осуществляется сотрудником Оператора, при получении ПДн от субъекта ПДн, путем оформления письменного согласия по форме, установленной у Оператора ИСПДн.

7. Права субъекта в отношении ПДн, обрабатываемых оператором

7.1. Субъект ПДн имеет право:

- на получение информации от Оператора, касающейся обработки его ПДн. Сведения должны быть предоставлены субъекту ПДн Оператором в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Перечень сведений и порядок получения сведений предусмотрен действующим законодательством РФ; (ч.1 ст.14 закона)

- требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством РФ меры по защите своих прав; (ч.1.ст.14 закона)

- на условие предварительного письменного согласия при обработки ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации; (ст.15 закона)

- на условие письменного согласия при принятии на основании исключительно автоматизированной обработки ПДн решений Оператора,

порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы; (ч.2. ст.16 закона)

- заявлять возражения на решения Оператора на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения; (ч.3 ст.16 закона)

- обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке. (ст. 17 закона)

8. Права и обязанности оператора ИСПДн

8.1. Оператор ИСПДн вправе:

8.1.1. Поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта. (ч.3 ст.6 закона)

8.1.2. В случае отзыва субъектом ПДн согласия на обработку ПДн, продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в законодательстве РФ. (ч.2 ст.9 закона)

8.1.3. Отказать субъекту ПДн в выполнении повторного запроса сведений, не соответствующего условиям, предусмотренным законодательством РФ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе. (ч.6 ст.14 закона)

8.1.4. Самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора ИСПДН, предусмотренных законодательством РФ. (ч.1 ст.18.1 закона)

8.2. Оператор ИСПДн обязан:

8.2.1. Оператор до начала обработки ПДн обязан уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных законодательством РФ.

8.2.2. При получения доступа к ПДн не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом. (ст.7 закона)

8.2.3. Представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия законных оснований, обработки ПДн без согласия субъекта ПДн.

8.2.4. До начала осуществления трансграничной передачи ПДн убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн.

8.2.5. Прекратить по требованию субъекта ПДн обработку его ПДн, в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации.

8.2.6. Разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов.

Оператор обязан рассмотреть возражение, в течение тридцати дней со дня его получения и уведомить субъекта ПДн о результатах рассмотрения такого возражения.

8.2.7. При сборе ПДн, предоставить субъекту ПДн по его просьбе информацию, предусмотренную законодательством РФ.

Если предоставление ПДн Оператору для субъекта ПДн является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

8.2.8. Если ПДн получены не от субъекта ПДн, Оператор, за исключением случаев, предусмотренных законодательством РФ, до начала обработки таких ПДн, предоставить субъекту ПДн следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки ПДн и ее правовое основание;

3) предполагаемые пользователи ПДн;

4) установленные настоящим Федеральным законом права субъекта ПДн;

5) источник получения ПДн.

8.2.9. Принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей Оператора ИСПДН, предусмотренных законодательством РФ.

8.2.10. Опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн.

8.2.11. При осуществлении сбора ПДн с использованием информационно-телекоммуникационных сетей, опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

8.2.12. Представить документы и локальные акты, предусмотренные законодательством РФ, и/или иным образом подтвердить принятие мер, необходимых и достаточные для обеспечения выполнения обязанностей Оператора ИСПДН, по запросу уполномоченного органа по защите прав субъектов ПДн.

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

8.2.14. Сообщить в порядке, предусмотренном законодательством РФ, субъекту ПДн или его представителю информацию безвозмездно о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.

8.2.15. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение законодательства РФ, являющееся основанием для такого отказа, в срок, не превышающий

тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

8.2.16. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие ПДн. Оператор обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

8.2.17. Сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

8.2.18. В случае выявления неправомерной обработки ПДн, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки ПДн невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Оператор обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

8.2.19. В случае достижения цели обработки ПДн Оператор обязан прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн, иным соглашением между Оператором и субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.

8.2.20. В случае отзыва субъектом ПДн согласия на обработку его ПДн, прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.

8.2.21. Назначить лицо, ответственное за организацию обработки ПДн.

9. Порядок обработки и защиты ПДн

9.1. Обеспечение конфиденциальности ПДн, обрабатывающихся Оператором, является обязательным требованием для всех лиц, которым ПДн стали известны.

9.2. Сотрудники Оператора, осуществляющие оформление документов, обязаны получать в установленных случаях согласие субъектов ПДн на обработку.

9.3. В случае нарушения установленного порядка обработки ПДн сотрудники Оператора несут ответственность в соответствии с разделом 9 настоящего Положения.

9.4. ПДн субъектов на бумажных носителях, обрабатываемые Оператором, хранятся в отделах (у сотрудников), имеющих допуск к обработке соответствующих ПДн. Право допуска сотрудников к неавтоматизированной ИСПДн определяется приказом Руководителя. Носители ПДн не должны оставаться без присмотра. При покидании рабочего места, сотрудники, осуществляющие обработку ПДн должны, убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче ПДн осуществляется по возможности их восстановление.

9.5. Места хранения документов, содержащих ПДн:

9.5.1. ПДн клиентов Оператора (договоры, акты, соглашения, анкеты, копии паспортов, иные подобные документы, содержащие ПДн клиентов Оператора, носители информации (флеш-карты, CD-диски, и т.п.) хранятся в основном офисе Оператора, размещаются на полках и запираются на ключ.

Ответственное лицо, осуществляющее контроль определяется приказом Руководителя.

9.5.2. ПДн сотрудников Оператора — документы, носители информации (флеш-карты, CD-диски и т.п.) хранятся в сейфе организации и запираются на ключ. Ответственное лицо, осуществляющее контроль — Руководитель Оператора.

9.6. Выдача документов для ознакомления осуществляется лицам, допущенным к соответствующей информации в целях исполнения должностных обязанностей, на срок, не более одного рабочего дня.

9.7. Иные носители информации могут храниться в основном офисе Оператора, размещаются на полках и запираются на ключ или же в сейфе организации. Ответственное лицо, осуществляющее контроль за иными носителями информации определяется приказом Руководителя.

9.8. При работе с программными средствами автоматизированной системы Оператора, реализующей функции просмотра и редактирования ПДн, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

9.9. При получении ПДн сотрудником Оператора, который в соответствии с должностными обязанностями получает ПДн от клиента, сотрудника иного лица в обязательном порядке проводится проверка достоверности ПДн. Ввод ПДн, полученных Оператором, в информационную систему осуществляется сотрудниками имеющими доступ к соответствующим ПДн. Сотрудники, осуществляющие ввод информации, несут ответственность за достоверность и полноту введенной информации.

9.10.

9.11. При неавтоматизированной обработке различных категорий ПДн должен использоваться отдельный материальный носитель для каждой категории ПДн.

9.12. При неавтоматизированной обработке ПДн на бумажных носителях:

9.12.1. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы;

9.12.2. ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

9.13. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее — типовые формы), должны соблюдаться следующие условия:

9.13.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;

9.13.2. Типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, — при необходимости получения письменного согласия на обработку ПДн;

9.13.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

9.13.4. Типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

9.14. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

9.15. Случаи уничтожения, блокирования и уточнения ПДн:

9.16. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

9.17. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя — путем фиксации на том же

материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

9.18. Уничтожение носителей, содержащих ПДн, осуществляется в следующем порядке:

9.18.1. ПДн на бумажных носителях уничтожаются путем использования шредера (уничтожителя документов), установленного в офисе Оператора.

9.18.2. ПДн, размещенные в памяти ПЭВМ уничтожаются путем удаления её из памяти ПЭВМ.

9.18.3. ПДн, размещенные на флеш-карте, CD-диске, ином носителе информации уничтожаются путем удаления файла с носителя, при необходимости путем нарушения работоспособности флеш-карты или CD-диска.

9.19. Об уничтожении носителя информации составляется Акт (формы актов см. в приложениях).

9.20. Офис, помещения Оператора, по окончании рабочего дня и отсутствия сотрудников в офисе помещениях, должны запираться, окна должны быть закрыты, должна быть включена сигнализация (при наличии).

9.21. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

9.22. Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПДн.

9.23. В обязанности администраторов ИСПДн входит управление учетными записями пользователей ИСПДн, поддержание штатной работы ИСПДн, обеспечение резервного копирования данных, а также установка и конфигурирование аппаратного и программного обеспечения ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн. Также, в обязанности администраторов ИСПДн входит обеспечение соответствия порядка обработки и обеспечения безопасности ПДн в ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемых к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленных федеральным законодательством.

9.24. В обязанности администраторов ИСПДн также входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации ИСПДн, учет и хранение машинных носителей ПДн, периодический аудит журналов безопасности и анализ защищенности ИСПДн, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

9.25. В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения, критичных для безопасности ПДн, полномочий у одного лица не рекомендуется совмещать роли пользователя ИСПДн и администратора ИСПДн в лице одного сотрудника.

9.26. Квалификационные требования и детальный перечень прав и обязанностей администраторов ИСПДн закрепляются в соответствующих должностных инструкциях, с которыми сотрудники, назначаемые на данные роли, должны быть ознакомлены под роспись.

9.27. Организация внутреннего контроля процесса обработки ПДн у Оператора осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

9.28. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

9.28.1. Обеспечение соблюдения сотрудниками Оператора требований настоящего Положения и нормативно-правовых актов, регулирующих сферу ПДн.

9.28.2. Оценка компетентности персонала, задействованного в обработке ПДн.

9.28.3. Обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн.

9.28.4. Выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений.

9.28.5. Принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн.

9.28.6. Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий

9.28.7. Осуществление внутреннего контроля за исполнением рекомендаций и указаний по устранению нарушений.

9.29. Результаты контрольных мероприятий оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств ИСПДн и средств защиты ПДн, по обучению и повышению компетентности персонала, задействованного в обработке ПДн.
10. Особенности управления ПДн сотрудников оператора

10.1. В настоящем разделе установлены дополнительные права и обязанности Оператора и работников при обработке Пдн сотрудников Оператора.

10.2. ПДн сотрудника — информация, необходимая Оператору в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

10.3. Обработка ПДн работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудников в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

10.4. Оператор не имеет права получать и обрабатывать ПДн сотрудника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами;

10.5. При принятии решений, затрагивающих интересы сотрудника, Оператор не имеет права основываться на ПДн сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

10.6. Сотрудники не должны отказываться от своих прав на сохранение и защиту тайны;

10.7. Оператор обязуется не сообщать ПДн сотрудника в коммерческих целях без его письменного согласия;

10.8. Оператор обязуется предупредить сотрудников Оператора, третьих лиц, получающих ПДн сотрудника (при его согласии), о том, что эти данные

могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн сотрудника, обязаны соблюдать режим секретности (конфиденциальности). Режим конфиденциальности обеспечивается подписанием с лицом соглашения (Приложение к настоящему Положению). Данное положение не распространяется на обмен ПДн сотрудников в порядке, установленном законодательством РФ;

10.9. Доступ к ПДн сотрудников осуществляется на основании приказов и положений, утвержденных Оператором.

10.10. Оператор обязуется не запрашивать информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции;

10.11. Оператор обязуется передавать ПДн сотрудника представителям сотрудников в порядке, установленном законодательством РФ, и ограничивать эту информацию только теми ПДн сотрудника, которые необходимы для выполнения указанными представителями их функций.

10.12. Сотрудник имеет право на определение своих представителей для защиты своих ПДн.

11. Ответственность за нарушение настоящего положения

11.1. Руководство Оператора несет ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

11.2. Сотрудники Оператора несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

11.3. Сотрудник Оператора может быть привлечен к ответственности в случаях:

11.3.1. Умышленного или неосторожного раскрытия ПДн

11.3.2. Утраты материальных носителей ПДн;

11.3.3. Нарушения требований настоящего Положения и других нормативных документов Оператора в части вопросов доступа и работы с ПДн

11.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Оператору, его сотрудникам, клиентам и контрагентам материального или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.