«УТВЕРЖДАЮ»
Директор казенного
учреждения Воронежской области
«Управление социальной защиты
населения Левобережного района г.
Воронежа»

_____ С.В. Паршин

«10» октября 2016 г.

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в казенном учреждении Воронежской области «Управление социальной защиты населения Левобережного района г. Воронежа»

Воронеж 2016

Содержание

Настоящее положение разработано в соответствии с федеральным законом от 27 июля 2006 года №152 ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Концепции и Политики информационной безопасности при обработке персональных данных населения в органах социальной защиты Воронежской области утвержденных приказом департамента труда и социального развития Воронежской области от 25.09.2012 г. № 3648/ОД.

Целью настоящего положения является систематизация основных принципов и условий обработки персональных данных, установления основных правил работы с персональными данными в казенном учреждении Воронежской области «Управление социальной защиты населения Левобережного района г. Воронежа» (далее КУВО «УСЗН Левобережного района»).

Термины и определения

В настоящем документе используются следующие основные термины и их определения:

Безо́пасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью работников, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных и без использования средств автоматизации.

Доступ к информации – возможность получения информации и ее использования.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Конфиденциальная информация – требующая защиты информация, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ к информации (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие установленные правила разграничения доступа.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Объект защиты – персональные данные, информация, обрабатываемая в информационных системах персональных данных, технические средства обработки и защиты персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

1. Общие положения

Персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

ПДн, обрабатываемые в КУВО «УСЗН Левобережного района» необходимы для оказания мер социальной поддержки субъекту персональных данных.

Обработка персональных данных граждан осуществляется как в информационных системах, так и без использования средств автоматизации.

Обязательным условием работы с персональными данными является обеспечение лицами, получающими доступ к персональным данным,

конфиденциальности таких данных, за исключением случаев, предусмотренных федеральными законами.

2. Правовое регулирование

Правовое регулирование вопросов обработки персональных данных осуществляется в соответствии с Конституцией Российской Федерации и международными договорами Российской Федерации следующими федеральными законами и нормативными правовыми актами:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Трудовой кодекс Российской Федерации;
- постановление Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- методические рекомендации ФСТЭК России;
- методические рекомендации Министерства здравоохранения и социального развития РФ;
- Концепция и Политика информационной безопасности при обработке персональных данных в органах социальной защиты населения Воронежской области.

3. Состав персональных данных

Состав (объем и содержание) персональных данных определяется нормативными правовыми актами, устанавливающими порядок предоставления мер социальной поддержки, социального обслуживания, иными документами, регламентирующими порядок осуществления функций органов социальной защиты населения. Состав персональных данных не должен превышать перечень информации, необходимой для реализации конкретных полномочий.

4. Область применения

Требования настоящего положения распространяются на всех сотрудников КУВО «УСЗН Левобережного района» (штатных, временных, работающих по контракту и т.п.), имеющих доступ к персональным данным граждан, включая персональные данные самих работников.

5. Основные принципы работы с персональными данными

Обработка персональных данных должна осуществляться на основе принципов:

1) законности целей и способов обработки персональных данных и добросовестности;

2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

6. Основные правила обработки персональных данных

Обработка персональных данных включает в себя – сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Система обработки информации – совокупность средств и методов получения и преобразования информации, позволяющая на основе исходного массива данных получить совокупность выходных показателей, необходимых для анализа, контроля, планирования, управления.

7. Обеспечение информационной безопасности при обработке персональных данных

Безопасность персональных данных при обработке достигается путем исключения всех возможностей несанкционированного доступа, случайного либо умышленного, в результате которого может произойти копирование, блокирование, удаление либо изменение персональных данных.

Уровень безопасности, соответствующий требованиям нормативно-правовой базы, достигается путем применения мер различного характера, в целом образующих комплексную систему информационной безопасности.

8. Правовые меры обеспечения информационной безопасности

Для реализации правовых мер обеспечения информационной безопасности необходимо опираться на нормативно правовые акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию персональных данных и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с лицами, осуществляющими обработку персональных данных.

9. Административные меры обеспечения информационной безопасности

Административными мерами устанавливается сфера влияния и ограничения при определении целей информационной безопасности, ресурсы (материальные, персонал) которыми они будут достигнуты и определен разумный компромисс между приемлемым уровнем безопасности и функциональностью информационных систем обработки персональных данных.

10. Организационные меры обеспечения информационной безопасности

При проведении организационных мер информационной безопасности регламентируются требования к персоналу, степень ответственности, статус и должностные обязанности сотрудников, ответственных за обеспечение информационной безопасности, устанавливается порядок обработки персональных данных, организуется взаимодействие специалистов в целях максимального затруднения или исключения возможности реализации угроз безопасности.

Организационные меры состоят из:

- регламента доступа в помещения, в которых осуществляется обработка персональных данных;

- порядка хранения персональных данных;

- порядка допуска сотрудников к работе с персональными данными, использованию ресурсов информационных систем персональных данных;

- регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов, с помощью которых осуществляется обработка персональных данных;

- порядка обработки персональных данных без использования средств автоматизации;

- инструкций пользователей информационных систем персональных данных (администратора информационной системы, администратора безопасности, оператора информационной системы);

- порядка действий при возникновении внештатных ситуаций.

11. Технические меры обеспечения информационной безопасности

Для реализации технических мер обеспечения информационной безопасности, КУВО «УСЗН Левобережного района» применяются различные электронные устройства и специальное программное обеспечение, входящие в состав информационных систем персональных данных или функционирующих автономно, выполняющих функции защиты, в том числе идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам.

Успешное применение технических средств защиты обеспечивается организационными (административными) мерами и используемыми физическими средствами защиты, направленными на выполнение следующих требований:

- каждый сотрудник – пользователь информационной системы персональных данных или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).

Осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

12. Требования к организации рабочих мест

Помещения, в которых размещается оборудование, предназначенное для обработки информационных ресурсов, хранятся машиночитаемые носители и документы, содержащие конфиденциальную информацию, расположены рабочие места специалистов, осуществляющих обработку персональных данных, должны исключать возможность бесконтрольного проникновения в них посторонних лиц, обеспечивать сохранность оборудования, машиночитаемых носителей информации и документов и защиту конфиденциальной информации от несанкционированного доступа.

Для этого входные двери этих помещений должны быть прочными, оборудованными надежными замками. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, должны быть защищены металлическими решетками.

Нахождение посторонних лиц и лиц, не имеющих права доступа к персональным данным, в этих помещениях допускается только в присутствии работников, ответственных за расположенные в них рабочие места.

Для проведения регламентных (наладочных), ремонтных и других работ во время обработки конфиденциальной информации посторонние лица могут быть допущены в эти помещения только в экстренных случаях по согласованию с руководителем учреждения и в присутствии лиц, ответственных за обработку персональных данных, при условии исключения несанкционированного доступа к персональным данным и иной конфиденциальной информации и контроля за порядком осуществления проводимых работ.

Средства вычислительной техники, с помощью которых осуществляется обработка персональных данных и другой конфиденциальной информации, должны быть расположены таким образом, чтобы был исключен несанкционированный просмотр информации, выводимой на экраны мониторов и на другие средства отображения информации.

13. Права субъектов персональных данных на доступ к своим персональным данным

Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных

данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

- способы обработки персональных данных, применяемые оператором;

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

- перечень обрабатываемых персональных данных и источник их получения;

- сроки обработки персональных данных, в том числе сроки их хранения;

- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

14. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

14.1. Операторы ИСПДн, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.