**администрация**

**(исполнительно - распорядительный орган)**

**СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**“Село Фоминичи”**

**Кировского района Калужской области**

Утверждаю

Глава администрации сельского поселения «Село Фоминичи»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.А.Дедов

 «25» сентября 2017 г.

ПОЛОЖЕНИЕ
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2017

Содержание

[1. Термины и определения 3](#_Toc375565284)

[2. Общие положения 5](#_Toc375565285)

[3. Принципы защиты персональных данных субъектов 6](#_Toc375565286)

[4. Перечень мер по защите персональных данных при их автоматизированной обработке 7](#_Toc375565287)

[5. Перечень мер по защите персональных данных, обрабатываемых без использования средств автоматизации 8](#_Toc375565288)

[6. Контроль защищённости персональных данных субъектов 9](#_Toc375565289)

[7. Организационная структура и обязанности ответственных лиц 10](#_Toc375565290)

[8. Обязанности Оператора и субъектов персональных данных 11](#_Toc375565291)

[9. Права субъектов персональных данных 12](#_Toc375565292)

[10. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных сотрудника 14](#_Toc375565293)

#  Термины и определения

## Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

## Использование персональных данных – действия (операции) с персональными данными, совершаемые Оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом, затрагивающих права и свободы субъекта персональных данных или других лиц.

## Конфиденциальность персональных данных – обязательное для соблюдения Оператором требование не допускать распространения персональных данных без согласия субъекта персональных данных или наличия иного законного основания.

## 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.

## Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных данных либо по его просьбе.

## Оператор персональных данных (далее 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. В рамках настоящего Положения Оператором является Кировская районная администрация (исполнительно-распорядительный орган) муниципального района «Город Киров и Кировский район».

## Персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

## Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

## Сотрудник (работник) – физическое лицо, состоящее в трудовых отношениях с Оператором.

## Субъект – физическое лицо, обладатель собственных персональных данных.

## Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

#  Общие положения

* 1. Назначение документа

## Целью настоящего «Положения по обеспечению безопасности персональных данных» (далее - Положение) является регламентация технологического и организационного процесса защиты персональных данных в администрации (исполнительно-распорядительного органа) сельского поселения «Село Фоминичи» (далее - Администрации).

## Положение разработано в соответствии с частью 1 статьи 23, статьи 24 Конституции Российской Федерации, главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников» от 30.12.2001 № 197‑ФЗ, Федеральным законом от 27.07.2006 № 149‑ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152‑ФЗ «О персональных данных».

* 1. Вступление в силу документа
		1. Настоящее Положение вступает в силу с момента его утверждения распоряжением администрации и действует бессрочно.
		2. Действие настоящего Положения может быть отменено распоряжением администрации в связи с утратой актуальности, либо по иным причинам.
		3. Все изменения настоящего Положения утверждаются распоряжением администрации.
		4. Все сотрудники Администрации, допущенные к обработке персональных данных, должны быть ознакомлены с настоящим Положением под роспись в течение одного месяца с момента принятия настоящего Положения, а также, в аналогичный срок с момента принятия изменений, вносимых в настоящее Положение.
		5. Все вновь принимаемые на работу в Администрацию сотрудники, для исполнения должностных обязанностей которых необходим допуск к обработке персональных данных, должны быть ознакомлены (под роспись) с настоящим Положением до начала исполнения этих обязанностей.

# Принципы защиты персональных данных субъектов

## В целях защиты персональных данных субъектов создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение персональными данными. Целью и результатом несанкционированного доступа к персональным данным субъектов может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внедрение вредоносных программ, фальсификация содержания реквизитов документа и др.

## Основным источником несанкционированного доступа к персональным данным является персонал, работающий с документами, содержащими персональные данные.

## Посторонние лица не должны знать информацию о распределении функций, рабочих процессах, технологии составления, оформления, ведения и хранения документов, дел и рабочих материалов в информационных системах персональных данных. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Администрации, например, посетители, сотрудники других организационных структур.

## Для обеспечения защиты персональных данных необходимо соблюдать следующие организационно-технические меры:

1. регламентация состава сотрудников, функциональные обязанности которых требуют доступа к персональным данным, и процесса предоставления такого доступа;
2. регламентация порядка приёма, учёта и контроля деятельности посетителей;
3. поддержания порядка охраны зданий и помещений;
4. периодический контроль обеспечения защищённости персональных данных субъектов;
5. соблюдение требований к защите персональных данных субъектов при интервьюировании и собеседованиях.

## В случаях обнаружения несоблюдения условий хранения носителей ПДн и/или несоблюдения использования средств защиты информации, а также в случае обнаружения нарушения порядка предоставления персональных данных, должно производиться разбирательство и составляться заключение по выявленным фактам.

# Перечень мер по защите персональных данных при их автоматизированной обработке

## Для обеспечения защиты персональных данных при их обработке должны приниматься следующие меры:

1. определение угроз безопасности персональным данным при их обработке, формирование на их основе модели угроз;
2. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
3. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
4. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
5. учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
6. контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
7. разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

## Порядок доступа в помещения Администрации, в которых ведётся обработка персональных данных представлены в документе «Порядок доступа в помещения, в которых ведётся обработка персональных данных».

# Перечень мер по защите персональных данных, обрабатываемых без использования средств автоматизации

## Для обеспечения защиты материальных носителей, содержащих персональные данные субъектов, обрабатываемых в Администрации, Оператор обязан:

## Довести до сотрудников, осуществляющих обработку персональных данных субъектов на материальных носителях, информацию об особенностях и правилах осуществления такой обработки.

## Запретить вынос за пределы Администрации носителей, содержащих персональные данные субъектов, за исключением случаев, установленных законодательством.

## Хранить носители, содержащие персональные данные, только в сейфах (шкафах), с надёжными средствами защиты, предотвращающими неконтролируемый доступ к ним. Места хранения носителей определяются распоряжением Кировской районной администрации «Об утверждении мест хранения материальных носителей персональных данных».

## Обеспечить учёт материальных носителей, содержащих персональные данные. Система учёта должна предоставлять возможность контроля над местонахождением каждого материального носителя.

## Организационно исключить необоснованное ознакомление с персональными данными лиц, не имеющих соответствующих полномочий.

## Обеспечить защиту от несанкционированного доступа и копирования персональных данных на материальных носителях, согласно организационным и распорядительным документам, принятым в Администрации.

# Контроль защищённости персональных данных субъектов

## Необходимо производить периодический контроль выполнения организационно-технических мер, а также контроль защищённости информационных ресурсов, содержащих персональные данные.

## Виды контроля состояния защищённости персональных данных субъектов, обрабатываемых в Администрации:

1. предварительный контроль (оценочная проверка обоснованности мер защиты персональных данных до начала их обработки). Осуществляется с целью своевременного выявления и предотвращения предпосылок возможных нарушений требований или норм защиты персональных данных;
2. текущий контроль (проверка в процессе обработки персональных данных). Осуществляется с целью своевременного выявления возникающих трудностей и недостатков реализации, принятых мер защиты персональных данных и выработки мероприятий по их устранению. Текущий контроль может быть периодическим, повседневным или непрерывным;
3. контроль устранения недостатков (проверка, проводимая после устранения ранее допущенных нарушений норм и требований защиты персональных данных, вследствие которых были приостановлены или ограничены работы с защищаемыми персональными данными субъектов). Осуществляется с целью выдачи разрешения на продолжение обработки персональных данных субъектов;
4. внутренний контроль. Проводится силами уполномоченных сотрудников Администрации;
5. организационный контроль. Подразумевает проверку состояния полноты и обоснованности мероприятий, по защите защищаемых информационных ресурсов требованиям соответствующих руководящих и нормативных документов;
6. контроль эффективности. Проводится с целью проверки соответствия количественных или качественных показателей эффективности мероприятий по защите персональных данных установленным требованиям или нормам эффективности защиты;
7. технический контроль. Обеспечивает проверку эффективности защиты персональных данных с использованием технических и (или) программных средств контроля и в дальнейшем получение наиболее объективной и достоверной информации о состоянии объектов контроля.

# Обязанности Оператора и субъектов персональных данных

## Сотрудники Администрации обязаны использовать персональные данные только в соответствии с целями обработки, определившими их получение.

## Сотрудники Администрации обязаны не отвечать на запросы, связанные с передачей персональных данных, по телефону или факсу.

## Для защиты персональных данных субъектов Администрации обязано:

1. за свой счёт, в порядке, установленном законодательством РФ, обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты;
2. ознакомить сотрудника или его представителей с настоящим Положением под расписку;
3. по запросу ознакомить субъекта персональных данных, не являющегося сотрудником, или в случае недееспособности либо несовершеннолетия субъекта, его законного представителя с настоящим Положением под расписку;
4. осуществлять передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;
5. предоставлять персональные данные субъекта только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим Положением и законодательством Российской Федерации;
6. по требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и порядке обработки этих данных.

## При обнаружении нарушений порядка предоставления персональных данных сотрудники Администрации обязаны незамедлительно приостановить предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

## Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности.

# Права субъектов персональных данных

## Субъекты персональных данных имеют право:

## На получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1. подтверждение факта обработки персональных данных оператором;
2. правовые основания и цели обработки персональных данных;
3. цели и применяемые оператором способы обработки персональных данных;
4. наименование и место нахождения оператора, сведения о лицах (за исключением сотрудников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6. сроки обработки персональных данных, в том числе сроки их хранения;
7. порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
8. информацию об осуществлённой или о предполагаемой трансграничной передаче данных;
9. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
10. иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

## Получать доступ к своим персональным данным, включая право получать копии любой записи, содержащей собственные персональные данные, за исключением случаев, предусмотренных федеральным законом;

## Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;

## При отказе Оператора или уполномоченного им лица исключить или исправить персональные данные субъекта – заявить в письменной форме о своём несогласии, представив соответствующее обоснование;

## Требовать от Оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них изменениях.

## Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1. обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
2. обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
3. обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма;
4. доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
5. обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

#  Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных сотрудника

## Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несёт персональную ответственность за данное разрешение.

## Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, материальную, административную, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации.

## Каждый сотрудник несёт единоличную ответственность за сохранность и конфиденциальность полученных в процессе работы персональных данных субъектов.

## За неисполнение или ненадлежащее исполнение сотрудником возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера руководство Оператора вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

## Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечёт наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

Лист ознакомления

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Ф.И.О. | Должность | Дата | Подпись |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |