

ПОЛОЖЕНИЕ

о защите персональных данных

ПОЛ-009

обозначение документа

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Назначение	Настоящий документ устанавливает порядок защиты персональных данных субъектов в ИП Николаенко Оксана Викторовна от несанкционированного доступа и разглашения, предотвращения и выявления нарушений законодательства Российской Федерации, устранения последствий таких нарушений.
Периодичность пересмотра	По мере необходимости
Срок действия	С 25 ноября 2023 г. И прекращает свое действие в связи с: • утверждением новой редакции Положения; • изменением законодательства Российской Федерации, регулирующего работу с персональными данными и иные, тесно связанные с ними отношения; • отменой (признанием утратившими силу).
Выполнены требования нормативных документов внешнего происхождения	Реализация данного документа гарантирует выполнение Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и иных нормативно-правовых актов в области защиты персональных данных, действующих на территории Российской Федерации
Заменяет	-
Версия	Издание 01

СОДЕРЖАНИЕ

ИНФОРМАЦИЯ О ДОКУМЕНТЕ	2
1. Нормативные ссылки	5
2. Определения, сокращения и условные обозначения	6
2.1. Сокращения	6
2.2. Определения	7
3. Общие положения	10
4. Категории субъектов персональных данных	10
5. Цели обработки персональных данных, категории (перечни) обрабатываемых персональных данных	11
6. Порядок и условия обработки персональных данных	14
7. Сроки обработки и хранения персональных данных	16
8. Порядок блокирования и уничтожения персональных данных	18
9. Защита персональных данных. Процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений	20
10. Ответственность за нарушение норм, регулирующих обработку персональных данных	26
11. Трансграничная передача персональных данных	28

1. Нормативные ссылки

1.1. Настоящее Положение Компании ссылается на следующие нормативные документы:

- 1.1.1 Конституция Российской Федерации;
- 1.1.2 Гражданский кодекс Российской Федерации;
- 1.1.3 Трудовой кодекс Российской Федерации;
- 1.1.4 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- 1.1.5 Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 06 марта 1997 г. №188;
- 1.1.6 Кодекс Российской Федерации об административных правонарушениях;
- 1.1.7 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 1.1.8 Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 1.1.9 Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- 1.1.10 Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных

данных при их обработке в информационных системах персональных данных»;

1.1.11 Постановление Правительства Российской Федерации от 29 июня 2021 г. №1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных»;

1.1.12 Приказ ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.1.13 Приказ ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

2. Определения, сокращения и условные обозначения

2.1. Сокращения

Компания, Общество, Организация – Индивидуальный предприниматель Николаенко Оксана Викторовна.

Положение – Положение о защите персональных данных.

ПДн – персональные данные.

2.2. Определения

Оператор, Общество – государственный орган, муниципальный орган, юридическое или физическое лицо (в целях настоящего Положения), 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.

Субъект персональных данных – физическое лицо, обладающее персональными данными прямо или косвенно его определяющими.

Персональные данные – 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.

Обработка персональных данных – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных.

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

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства

органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Конфиденциальность персональных данных – обязательное для соблюдения назначенным ответственным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия работника или иного законного основания.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или представление доступа к персональным данным каким-либо иным способом.

Персональными данными, разрешенными субъектом персональных данных для распространения, являются персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных».

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

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

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.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Угрозы безопасности ПДн – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

Уровень защищенности ПДн – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПДн при их обработке в информационной системе.

3. Общие положения

3.1. Настоящее Положение является локальным нормативным актом Индивидуального предпринимателя Николаенко Оксаны Викторовны, принятым с учетом требований, в частности, гл. 14 Трудового кодекса РФ, Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

3.2. В Положении устанавливаются:

- цель, порядок и условия обработки персональных данных;
- категории субъектов, персональные данные которых обрабатываются, категории (перечни) обрабатываемых персональных данных, способы, сроки их обработки и хранения, порядок уничтожения таких данных при достижении целей обработки или при наступлении иных законных оснований;
- положения, касающиеся защиты персональных данных, процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в области персональных данных, а также на устранение последствий таких нарушений.

4. Категории субъектов персональных данных

4.1. К субъектам, персональные данные которых обрабатываются в Обществе в соответствии с Положением, относятся:

- кандидаты для приема на работу;
- работники Индивидуального предпринимателя;
- посетитель сайта;
- клиенты Индивидуального предпринимателя;
- бывшие работники Общества;
- члены семей работников Общества - в случаях, когда согласно законодательству сведения о них предоставляются работником;
- иные лица, персональные данные которых Индивидуальный предприниматель обязан обрабатывать в соответствии с трудовым законодательством и иными актами, содержащими нормы трудового права.

5. Цели обработки персональных данных, категории (перечни) обрабатываемых персональных данных

5.1. Согласно Положению, персональные данные обрабатываются с целью применения и исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ними отношений, в том числе:

- при содействии в трудоустройстве;
- ведении кадрового и бухгалтерского учета;
- содействии работникам в получении образования и продвижении по службе;
- оформлении награждений и поощрений;
- предоставлении со стороны Общества установленных законодательством условий труда, гарантий и компенсаций;
- заполнении и передаче в уполномоченные органы требуемых форм отчетности;
- обеспечении личной безопасности работников и сохранности имущества;
- осуществлении контроля за количеством и качеством выполняемой работы.

5.2. В соответствии с целью, указанной в п. 3.1 Положения, в Обществе обрабатываются следующие персональные данные:

- фамилия, имя, отчество (при наличии), а также прежние фамилия, имя, отчество (при наличии), дата и место их изменения (в случае изменения);
- пол;
- дата (число, месяц, год) и место рождения;
- фотографическое изображение;

- сведения о гражданстве;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- страховой номер индивидуального лицевого счета (СНИЛС);
- идентификационный номер налогоплательщика (ИНН);
- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;
- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и место рождения);
- сведения об образовании и (или) квалификации или наличии специальных знаний (в том числе наименование образовательной и (или) иной организации, год окончания, уровень образования, квалификация, реквизиты документа об образовании, обучении);
- информация о владении иностранными языками;
- сведения об отношении к воинской обязанности, о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документа, наименование органа, выдавшего его);
- сведения о трудовой деятельности, а также информация о предыдущих местах работы, периодах и стаже работы;
- сведения, содержащиеся в документах, дающих право на пребывание и трудовую деятельность на территории РФ (для иностранных граждан, пребывающих в РФ);
- сведения, содержащиеся в разрешении на временное проживание, разрешении на временное проживание в целях

получения образования (для иностранных граждан, временно проживающих в РФ), виде на жительство (для иностранных граждан, постоянно проживающих в РФ);

- сведения о доходах, обязательствах по исполнительным документам;

- номера расчетного счета, банковской карты;

- сведения о состоянии здоровья (для отдельных категорий работников);

- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (для отдельных категорий работников);

- иные персональные данные, содержащиеся в документах, представление которых предусмотрено законодательством, если обработка этих данных соответствует цели обработки, предусмотренной п. 3.1 Положения;

- иные персональные данные, которые работник пожелал сообщить о себе и обработка которых соответствует цели обработки, предусмотренной п. 3.1 Положения.

5.3. Общество не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

6. Порядок и условия обработки персональных данных

6.1. До начала обработки персональных данных Общество обязано уведомить Роскомнадзор о намерении осуществлять обработку персональных данных.

6.2. Обработка персональных данных осуществляется с соблюдением принципов и условий, предусмотренных законодательством в области персональных данных и настоящим Положением.

6.3. Обработка персональных данных в Обществе выполняется следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

6.4. Обработка персональных данных в Обществе осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством в области персональных данных.

6.4.1. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 Закона о персональных данных.

Согласие на обработку таких персональных данных оформляется отдельно от других согласий на обработку персональных данных. Согласие предоставляется субъектом персональных данных лично либо в форме электронного документа, подписанного электронной подписью, с использованием информационной системы Роскомнадзора.

6.4.2. Обработка биометрических персональных данных допускается только при наличии письменного согласия субъекта персональных данных. Исключение составляют ситуации, предусмотренные ч. 2 ст. 11 Закона о персональных данных.

6.5. Общество не осуществляет трансграничную передачу персональных данных.

6.6. Обработка персональных данных осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, обезличивания, блокирования, удаления, уничтожения персональных данных, в том числе с помощью средств вычислительной техники.

6.6.1. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных в Обществе осуществляются посредством:

- получения оригиналов документов либо их копий;
- копирования оригиналов документов;
- внесения сведений в учетные формы на бумажных и электронных носителях;
- создания документов, содержащих персональные данные, на бумажных и электронных носителях;
- внесения персональных данных в информационные системы персональных данных.

6.6.2. Используются следующие информационные системы:

- корпоративная электронная почта;
- система электронного документооборота;
- система поддержки рабочего места пользователя;
- система нормативно-справочной информации;
- система управления персоналом;

- система контроля удаленным доступом;
- информационный портал.

6.7. Передача (распространение, предоставление, доступ) персональных данных субъектов персональных данных осуществляется в случаях и в порядке, предусмотренных законодательством в области персональных данных и Положением.

7. Сроки обработки и хранения персональных данных

7.1. Обработка персональных данных в Обществе прекращается в следующих случаях:

- при выявлении факта неправомерной обработки персональных данных. Срок прекращения обработки - в течение трех рабочих дней с даты выявления такого факта;
- при достижении целей их обработки (за некоторыми исключениями);
- по истечении срока действия или при отзыве субъектом персональных данных согласия на обработку его персональных данных (за некоторыми исключениями), если в соответствии с Законом о персональных данных их обработка допускается только с согласия;
- при обращении субъекта персональных данных к Обществу с требованием о прекращении обработки персональных данных (за исключением случаев, предусмотренных ч. 5.1 ст. 21 Закона о персональных данных). Срок прекращения обработки - не более десяти рабочих дней с даты получения требования (с возможностью продления не более чем на пять рабочих дней, если направлено уведомление о причинах продления).

7.2. Персональные данные хранятся в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Исключение - случаи, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных.

7.3. Персональные данные на бумажных носителях хранятся в Обществе в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 N 125-ФЗ "Об архивном деле в Российской Федерации", Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. Приказом Росархива от 20.12.2019 N 236)).

7.4. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

8. Порядок блокирования и уничтожения персональных данных

8.1. Общество блокирует персональные данные в порядке и на условиях, предусмотренных законодательством в области персональных данных.

8.2. При достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей персональные данные уничтожаются либо обезличиваются. Исключение может предусматривать федеральный закон.

8.3. Незаконно полученные персональные данные или те, которые не являются необходимыми для цели обработки, уничтожаются в течение семи рабочих дней со дня представления субъектом персональных данных (его представителем) подтверждающих сведений.

8.4. Персональные данные, обработка которых прекращена из-за ее неправомерности и правомерность обработки которых невозможно обеспечить, уничтожаются в течение 10 рабочих дней с даты выявления неправомерной обработки.

8.5. Персональные данные уничтожаются в течение 30 дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иным соглашением между ним и Обществом либо если Общество не вправе обрабатывать персональные данные без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

8.5.1. При достижении максимальных сроков хранения документов, содержащих персональные данные, персональные данные уничтожаются в течение 30 дней.

8.6. Персональные данные уничтожаются (если их сохранение не требуется для целей обработки персональных данных) в течение 30 дней с даты поступления отзыва субъектом персональных данных согласия на их обработку. Иное может предусматривать договор, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иное соглашение между ним и Обществом. Кроме того, персональные данные уничтожаются в указанный срок, если Общество не вправе обрабатывать их без согласия субъекта

персональных данных на основаниях, предусмотренных федеральными законами.

8.7. Отбор материальных носителей (документы, жесткие диски, флеш-накопители и т.п.) и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению, осуществляют подразделения Общества, обрабатывающие персональные данные.

8.8. Уничтожение персональных данных осуществляет комиссия, созданная приказом генерального директора.

8.8.1. Комиссия составляет акт с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

8.8.2. Персональные данные на бумажных носителях уничтожаются с использованием шредера. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

8.8.3. Непосредственно после уничтожения персональных данных оформляется акт об их уничтожении.

9. Защита персональных данных. Процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений

9.1. Защита персональных данных представляет собой процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в

конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Компании.

9.2. Защита персональных данных субъектов от неправомерного их использования или утраты должна быть обеспечена Обществом за счет его средств в порядке, установленном законодательством.

9.3. Компания принимает следующие меры по защите ПДн:

9.3.1. Назначение лица, ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите ПДн.

9.3.2. Разработка политики в отношении обработки ПДн.

9.3.3. Установление правил доступа к ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн.

9.3.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

9.3.5. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

9.3.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

9.3.7. Соблюдение условий, обеспечивающих сохранность ПДн и исключающих несанкционированный к ним доступ.

9.3.8. Обнаружение фактов несанкционированного доступа к ПДн.

9.3.9. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

9.3.10. Обучение работников, непосредственно осуществляющих обработку ПДн, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Работодателя в отношении обработки ПДн, локальным актам по вопросам обработки персональных данных.

9.3.11. Осуществление внутреннего контроля и аудита за работой с ПДн.

9.3.12. Определение типа угроз безопасности и уровней защищенности ПДн, которые хранятся в информационных системах.

9.3.13. Назначение лица ответственного за безопасность ПДн.

9.3.14. Разработка документа, фиксирующего перечень форм, содержащих персональные данные.

9.3.15. Определение перечня должностей, доступ которых к персональным данным необходим для выполнения ими служебных обязанностей.

9.3.16. Утверждение перечня ИСПДн.

9.3.17. Разработка инструкций для организации системы защиты ПДн.

9.3.18. Разработка мер оперативного реагирования на внештатные ситуации при работе с ПДн.

9.3.19. Своевременное уведомление государственных органов о случаях утечек данных.

9.3.20. Устранение в короткие сроки неисправностей оборудования, обеспечивающего сохранность ПДн.

9.3.21. Выявление и фиксация категорий субъектов ПДн и перечня данных, которые обрабатываются оператором в отношении ПДн.

9.3.22. Определение ограниченного списка лиц, допущенных, в силу исполняемыми ими обязанностями, к обработке ПДн.

9.3.23. Закрепление в документах, регулирующих трудовые отношения обязанности по обработке и ответственность за обработку ПДн.

9.3.24. Обеспечение фиксации случаев нарушения работы с ПДн, выявленных угроз и принятых мер по их устранению.

9.3.25. Контроль исполнения требований договоров поручения обработки ПДн третьими лицами, а также обеспечение исполнения требования по неразглашению ПДн.

9.3.26. Заключение с лицами, допущенными к обработке ПДн соглашение о неразглашении полученных в процессе исполнения обязанностей ПДн.

9.3.27. Обеспечение рабочего пространства сотрудников, способствующее сохранению безопасности обрабатываемых ПДн.

9.3.28. Определение мест хранения документов, форм и иных материальных носителей, содержащих ПДн.

9.3.29. Разработка плана мероприятий по организации защиты персональных данных.

9.3.30. Разработка инструкций пользователя ИСПДн.

9.3.31. Обеспечение порядка резервного копирования данных.

9.3.32. Обеспечение учета, хранения и уничтожения носителей персональных данных.

9.3.33. Организация хранения и уничтожения информации, содержащей в себе персональные данные субъектов персональных данных.

9.3.34. Ведение учета реагирования на запросы субъектов персональных данных.

9.4. Угрозы защищенности персональных данных.

9.4.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

9.4.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.

9.4.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

9.5. Уровни защищенности персональных данных.

9.5.1. Первый уровень защищенности. Если Оператор отнес информационную систему к первому типу угрозы или если тип угрозы второй, но Оператор обрабатывает специальные категории ПДн более 100 тыс. физических лиц без учета работников.

9.5.2. Второй уровень защищенности. Если тип угрозы второй и Оператор обрабатывает специальные категории ПДн работников вне зависимости от их количества или специальные категории ПДн менее чем 100 тыс. физических лиц, или любые другие категории ПДн более чем 100 тыс. физических лиц, или при третьем типе угрозы Оператор обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

9.5.3. Третий уровень защищенности. Если при втором типе угрозы Оператор обрабатывает общие ПДн работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы Оператор обрабатывает специальные категории ПДн работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы Оператор обрабатывает биометрические ПДн, или при

третьем типе угрозы Оператор обрабатывает общие ПДн более чем 100 тыс. физических лиц.

9.5.4. Четвертый уровень защищенности. Если при третьем типе угрозы Оператор обрабатывает только общие ПДн работников или менее чем 100 тыс. физических лиц.

9.6. При четвертом уровне защищенности персональных данных Оператор:

9.6.1. обеспечивает режим безопасности помещений, в которых размещаете информационную систему;

9.6.2. обеспечивает сохранность носителей информации;

9.6.3. утверждает перечень работников, допущенных до ПДн;

9.6.4. использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

9.7. При третьем уровне защищенности ПДн дополнительно к мерам, перечисленным в пункте 4.4 настоящего Положения, Оператор назначает ответственного за обеспечение безопасности ПДн в информационной системе.

9.8. При втором уровне защищенности ПДн дополнительно к мерам, перечисленным в пунктах 4.4, 4.5 настоящего Положения, Оператор ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

9.9. При первом уровне защищенности ПДн дополнительно к мерам, перечисленным в пунктах 4.4-4.6 настоящего Положения, Оператор:

9.9.1. обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к ПДн в системе;

9.9.2. создает отдел, ответственный за безопасность ПДн в системе, либо возлагает такую обязанность на один из существующих отделов Оператора.

9.10. В целях защиты ПДн на бумажных носителях Оператор:

9.10.1. приказом назначает ответственного за обработку ПДн;

9.10.2. ограничивает допуск в помещения, где хранятся документы, которые содержат ПДн работников;

9.10.3. хранит документы, содержащие ПДн работников в шкафах, запирающихся на ключ;

9.10.4. хранит трудовые книжки работников в сейфе.

9.11. В целях обеспечения конфиденциальности документы, содержащие ПДн субъектов, оформляются, ведутся и хранятся только работниками, допущенными к ПДн работников.

9.12. Работники, допущенные к ПДн субъектов, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПДн не допускаются.

9.13 Допуск к документам, содержащим ПДн, внутри организации осуществляется исключительно работниками, допущенными к ПДн.

9.14. Передача ПДн по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия субъекта на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

9.15. Передача информации, содержащей сведения о ПДн работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

10. Ответственность за нарушение норм, регулирующих обработку персональных данных

10.1. Должностные лица, имеющие доступ к персональным данным, несут личную ответственность за нарушение режима защиты персональных данных в соответствии с законодательством РФ в области персональных данных.

10.2. Каждый сотрудник Компании, получающий для работы носитель персональных данных, несет единоличную ответственность за сохранность носителя и обеспечение конфиденциальности персональных данных.

10.3. Сотрудники Компании, которым стали известны персональные данные в силу их служебного положения, несут ответственность за их разглашение.

10.4. Обязательства по соблюдению конфиденциальности персональных данных остаются в силе и после окончания работы с ними вышеуказанных лиц.

10.5. За неисполнение или ненадлежащее исполнение сотрудником Компании, возложенных на него обязанностей по соблюдению установленного порядка работы с персональными данными, Компания вправе применять предусмотренные Трудовым Кодексом РФ дисциплинарные взыскания.

10.6. Ответственность за соблюдение порядка защиты персональных данных несет сотрудник, а также руководитель структурного подразделения, осуществляющего обработку персональных данных.

10.7. Должностные лица, в обязанность которых входит обработка персональных данных, обеспечивают, при необходимости, каждому субъекту персональных данных

возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

10.7.1. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законодательством РФ в области персональных данных, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях РФ.

10.8. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом РФ и иными федеральными законами РФ в области персональных данных, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном законодательством.

11. Трансграничная передача персональных данных

11.1. В случае осуществления трансграничной передачи персональных данных Оператор до начала осуществления такой деятельности уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных.

11.2. Оператор по запросу уполномоченного органа по защите прав субъектов персональных данных в целях оценки

достоверности сведений предоставляет такие сведения в течение десяти рабочих дней с даты получения такого запроса.