

УТВЕРЖДАЮ  
Генеральный директор  
ООО «УК «ЭКОДОМ»



А. А. Воронин  
2019 г.

## ПОЛОЖЕНИЕ об обработке и защите персональных данных

### 1. ОБЩИЕ ПОЛОЖЕНИЯ

#### 1.1. Сфера действия настоящего Положения

Настоящее Положение определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в Обществе с ограниченной ответственностью «Управляющая компания «ЭКОДОМ» (далее - Организация) персональных данных, функции Организации при обработке персональных данных, права субъектов персональных данных, а также реализуемые в Организации требования к защите персональных данных и ответственность должностных лиц Организации, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, правила обработки персональных данных (ПД), порядок уничтожения ПД, правила осуществления внутреннего контроля соответствия обработки ПД требованиям законодательства, правила доступа субъектов ПД к своим персональным данным, находящимся в информационных системах персональных данных (ИСПД) и другие вопросы, возникающие при обработке ПД в Организации.

Действие настоящего Положения не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования, содержащих персональные данные архивных документов в соответствии с законодательством об архивном деле в Российской Федерации.

#### 1.2. Цель настоящего Положения

Целью данного Положения является обеспечение выполнения требований законодательства Российской Федерации в области защиты персональных данных и защита прав и свобод субъектов ПД при обработке их персональных данных.

#### 1.3. Основные понятия, используемые в настоящем Положении

В настоящем Положении используются следующие основные термины и определения.

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

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

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

*Обработка персональных данных* - любое действие (операция) или совокупность действий (операций), совершаемые 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.

*Автоматизированная обработка персональных данных* - обработка персональных данных с помощью средств вычислительной техники.

*Предоставление персональных данных* - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

*Распространение персональных данных* - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

*Трансграничная передача персональных данных* - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

*Блокирование персональных данных* - временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).

*Уничтожение персональных данных* - действия, в результате которых становится невозможным восстановить содержание ПД в ИСПД и (или) в результате которых уничтожаются материальные носители ПД.

*Обезличивание персональных данных* - действия, в результате которых становится невозможным без

использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

1.4. Нормативные правовые акты, на основании которых разработано настоящее Положение Настоящее Положение разработано в соответствии с Политикой обработки персональных данных в Организации с учетом требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Жилищного кодекса Российской Федерации, Трудового кодекса Российской Федерации, постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и других действующих нормативно-правовых актов Российской Федерации. Настоящее Положение вступает в действие с даты его утверждения руководителем организации и действует до отмены его Приказом руководителя организации. Работники Организации - ответственные за организацию обработки персональных данных в, администраторы информационных систем персональных данных, а также лица, допущенные к обработке персональных данных, должны быть ознакомлены с настоящим Положением под роспись.

## **2. ПРИНЦИПЫ, УСЛОВИЯ И ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ**

2.1. Принципы обработки персональных данных в Организации Обработка персональных данных в Организации осуществляется с учетом необходимости обеспечения защиты прав и свобод субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

а) обработка персональных данных осуществляется в Организации на законной и справедливой основе;

б) обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

в) не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

г) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

е) обработке подлежат только персональные данные, которые отвечают целям их обработки;

ж) содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

з) при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Организацией принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;

и) хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Условия обработки персональных данных в Организации

2.2.1. Обработка персональных данных в Организации осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

2.2.2. Организация без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральными законами.

2.2.3. Организация вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом,

осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2.2.4. В целях внутреннего информационного обеспечения Организация может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, должность, год и место рождения, адрес, адрес электронной почты, иные персональные данные, указанные в его письменном согласии.

2.3. Категории субъектов персональных данных, персональные данные которых подлежат обработке в Организации обрабатываются персональные данные, принадлежащие следующим категориям субъектов:

2.3.1. Работникам Организации.

2.3.2. Клиентам Организации.

2.4. Категории персональных данных, обрабатываемых в Организации. Общедоступные персональные данные, обрабатываемые в Организации, содержат сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом. Специальные категории персональных данных, к которым относится информация о национальной и расовой принадлежности субъекта, о религиозных, философских, либо политических убеждениях, информация о здоровье и интимной жизни субъекта и биометрические персональные данные в Организации не обрабатываются.

2.5. Цели обработки персональных данных в Организации

2.5.1. Персональные данные обрабатываются в Организации в целях:

а) выполнения требований действующего Законодательства Российской Федерации, нормативных актов органов государственной власти и местного самоуправления;

б) организации кадрового учета Организации, исполнения обязательств по трудовым и гражданско-правовым договорам с работниками;

в) обеспечения деятельности бухгалтерии Организации по начислению и регулярной выплате заработной платы работникам;

г) обеспечения деятельности отдела кадров Организации, в части организации учета и движения контингента, исполнения обязательств по договорам с Клиентами;

д) заключения, исполнения и прекращения гражданско-правовых договоров с физическими и юридическими лицами, в случаях, предусмотренных действующим законодательством и Уставом Организации;

е) выполнения требований по предоставлению обрабатываемых персональных данных субъектов в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, в иные государственные органы;

ж) защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных – работников Организации;

з) предоставление работникам Организации персонализированных информационных сервисов для осуществления видов деятельности, предусмотренных Уставом и иными локальными правовыми актами Организации;

и) обеспечения пропускного и внутриобъектового режимов на объектах Организации;

к) формирования справочных материалов для внутреннего информационного обеспечения деятельности Организации, предусмотренной Уставом;

л) исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве; о) в иных законных целях.

2.6. Действия, совершаемые с персональными данными в Организации. Организация осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, предоставление, обезличивание, уничтожение персональных данных.

2.7. Согласие субъекта персональных данных на обработку его персональных данных в Организации. Условием обработки персональных данных субъекта персональных данных является его письменное согласие.

В случае если Организация на основании договора поручает обработку персональных данных третьей стороне, существенным условием договора является обязанность обеспечения третьей стороной конфиденциальности персональных данных и безопасности персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных. Также такой договор должен содержать перечень действий (операций) с персональными данными, цели и сроки обработки.

Согласие физического лица не требуется в случаях:

а) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

б) обработка персональных данных необходима для исполнения договора, стороной, выгодоприобретателем или поручителем по которому является субъект персональных данных;

в) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

г) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

д) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем, при условии обязательного обезличивания персональных данных;

е) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

ж) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации.

### **3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ**

#### **3.1. Виды обработки персональных данных в Организации**

В Организации осуществляется:

а) автоматизированная обработка персональных данных в информационных системах персональных данных;

б) обработка персональных данных без использования средств автоматизации;

в) передача персональных данных другим операторам.

#### **3.2. Обработка персональных данных без использования средств автоматизации**

3.2.1. Для каждой категории субъектов персональных данных, обрабатываемых без использования средств автоматизации в Организации, определяются отдельные места хранения персональных данных (материальных носителей) в запирающихся на ключ помещениях, в металлических несгораемых шкафах (сейфах), иных шкафах, имеющих запираемые блок-секции. Ключи от этих помещений (шкафов) должны храниться у лиц, ответственных за обработку персональных данных данной категории субъектов персональных данных. Запрещается хранение носителей с персональными данными на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам. Запрещается вынос носителей с персональными данными из служебных помещений для работы с ними вне Организации.

3.2.2. Перечень лиц, ответственных за обработку персональных данных без использования средств автоматизации в Организации, осуществляющих обработку персональных данных или имеющих к ним доступ утверждается приказом генерального директора.

3.2.3. Персональные данные субъектов персональных данных, обрабатываемые без использования средств автоматизации в Организации (материальные носители), обработка которых осуществляется в различных целях, должны храниться отдельно.

3.2.4. При хранении материальных носителей в Организации должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ.

#### **3.3. Автоматизированная обработка персональных данных**

3.3.1. Автоматизированная обработка персональных данных в Организации осуществляется в информационных системах персональных данных, принятых в эксплуатацию на основании приказа генерального директора.

3.3.2. Для принятия в эксплуатацию информационной системы персональных данных приказом генерального директора назначается комиссия по приему.

3.3.3. В приказе по вводу в эксплуатацию информационной системы персональных данных должны быть назначены:

а) ответственный за организацию обработки персональных данных в информационной системе персональных данных;

б) пользователи информационной системы персональных данных;

в) администратор информационной системы персональных данных;

г) администратор безопасности информационной системы персональных данных.

3.3.4. Ответственный за организацию обработки персональных данных в информационной системе персональных данных, пользователи, администратор и администратор безопасности должны быть

ознакомлены с приказом по вводу в эксплуатацию информационной системы персональных данных и своими должностными инструкциями под роспись.

3.3.5. Комиссия по приему составляет акт ввода в эксплуатацию информационной системы персональных данных, который утверждается генеральным директором. После утверждения акта ввода в эксплуатацию информационная система персональных данных считается принятой, а персонал, допущенный к обработке персональных данных субъектов персональных данных, приступает к выполнению своих должностных обязанностей.

#### 3.4. Порядок получения персональных данных

3.4.1. Организация получает сведения о персональных данных субъектов персональных данных из следующих документов:

- а) паспорт или иной документ, удостоверяющий личность;
- б) трудовая книжка;
- в) страховое свидетельство государственного пенсионного страхования;
- г) свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика;
- д) документы воинского учета, содержащие сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;
- е) документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки, содержащий сведения об образовании, профессии;
- ж) анкета, заполняемая при приеме на работу, поступлении на работу;
- з) иные документы и сведения, предоставляемые субъектом персональных данных при приеме на работу, а также в процессе работы.

3.4.2. Субъект персональных данных обязан представлять Организации достоверные сведения о себе. Организация имеет право проверять достоверность указанных сведений в порядке, не противоречащем законодательству РФ.

3.4.3. Все персональные данные субъекта персональных данных Организация получает непосредственно у указанных субъектов.

#### 3.5. Порядок передачи персональных данных

3.5.1. При передаче персональных данных работники Организации должны соблюдать следующие требования:

- а) не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается.
- б) осуществлять передачу персональных данных субъектов в пределах Организации в соответствии с настоящим Положением, локальными нормативными актами и должностными инструкциями.
- в) разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.
- г) передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и локальными нормативными актами и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

3.5.2. Организация не осуществляет трансграничную передачу персональных данных.

## **4. ОБЕСПЕЧЕНИЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБРАБОТКЕ ИХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ**

4.1. Права субъектов персональных данных Субъекты персональных данных имеют право на:

- а) полную информацию об их персональных данных, обрабатываемых в Организации;
- б) доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;
- в) уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- г) отзыв согласия на обработку персональных данных;
- д) принятие предусмотренных законом мер по защите своих прав;
- е) обжалование действия или бездействия Организации, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;
- з) осуществление иных прав, предусмотренных законодательством Российской Федерации.

4.2. Рассмотрение запросов на получение персональных данных субъектов

4.2.1. Доступ к своим персональным данным представляется субъекту персональных данных или его законному представителю лицом, ответственным за обработку персональных данных, при обращении субъекта персональных данных (законного представителя). В качестве формы обращения субъекта используется служебная записка на имя должностного лица, ответственного за обработку персональных данных, собственноручно подписанная субъектом (законным представителем), содержащая номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе.

4.2.2. Сведения о наличии персональных данных должны быть представлены субъекту персональных данных пользователем ИСПД в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

4.2.3. Субъект персональных данных имеет право на получение следующих сведений от пользователя ИСПД:

- а) подтверждение факта обработки персональных данных оператором;
- б) правовые основания и цели обработки персональных данных;
- в) цели и применяемые оператором способы обработки персональных данных;
- г) сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального законодательства Российской Федерации;
- д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством Российской Федерации;
- е) сроки обработки персональных данных, в том числе сроки их хранения;
- ж) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- з) наименование и юридический адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу; и) иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами Российской Федерации.

4.2.4. Внесение изменений или уточнение персональных данных субъекта персональных данных пользователем ИСПД должны быть выполнены в течение 7 рабочих дней со дня предоставления таких сведений.

4.3. Порядок обеспечения конфиденциальности при обработке персональных данных

4.3.1. Должностным лицам Организации, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных.

4.3.2. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные, запрещается.

4.3.3. Должностные лица Организации, работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, указанных в согласии на обработку и передачу персональных данных субъектом персональных данных.

4.3.4. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством РФ, при заполнении согласия на передачу персональных данных третьей стороне, в соответствии с должностными инструкциями и иными локальными нормативными актами Организации.

4.3.5. Передача персональных данных осуществляется ответственным за обработку персональных данных должностным лицом Организации на основании письменного или устного поручения руководителя структурного подразделения.

4.3.6. Передача сведений и документов, содержащих персональные данные, оформляется путем внесения записи в Журнал учета передачи персональных данных.

4.3.7. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими в Организации локальными нормативными актами.

4.3.8. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

4.3.9. Должностные лица Организации, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю и (или) генеральному директору по режиму и безопасности Организации обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об

утрате или недостатке носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.

4.3.10. Должностные лица, осуществляющие обработку персональных данных, за невыполнение требований конфиденциальности, защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

## **5. ОБЯЗАННОСТИ ОРГАНИЗАЦИИ КАК ОПЕРАТОРА**

5.1. Меры, осуществляемые в Организации для обеспечения выполнения обязанностей оператора

5.1.1. Меры по обеспечению выполнения Организацией обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных, включают:

- а) назначение лиц, ответственных за организацию обработки персональных данных в Организации;
- б) принятие локальных нормативных актов и иных документов в области обработки и защиты персональных данных;
- в) организацию обучения и проведение методической работы с работниками Организации, осуществляющими обработку персональных данных;
- г) получение согласий субъектов персональных данных на обработку их персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;
- д) обособление персональных данных, обрабатываемых без использования средств автоматизации, от иной информации, в частности путем их фиксации на отдельных материальных носителях персональных данных, в специальных разделах;
- е) обеспечение отдельного хранения персональных данных и их материальных носителей, обработка которых осуществляется в разных целях и которые содержат разные категории персональных данных;
- ж) установление запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям и сетям Интернет без применения установленных в Организации мер по обеспечению безопасности персональных данных (за исключением общедоступных и (или) обезличенных персональных данных);
- и) хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;
- к) ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Порядок доступа в помещения, где происходит обработка персональных данных, в рабочее и нерабочее время, а также в нестандартных ситуациях приведен в Приложении;
- л) осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящему Положению, локальным нормативным актам Организации;
- м) ознакомление работников Организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов Организации в области персональных данных, в том числе с требованиями к защите персональных данных, и обучение указанных работников;
- н) опубликование или обеспечение неограниченного доступа к настоящему Положению иным образом;
- о) прекращение обработки и уничтожение персональных данных в случаях, предусмотренных законодательством Российской Федерации в области персональных данных; п) иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.

5.3. Меры, осуществляемые в Организации по обеспечению безопасности персональных данных при их автоматизированной обработке

5.3.2. Обеспечение безопасности ПД при их автоматизированной обработке в Организации осуществляется применением организационных и технических мер с целью предотвращения неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, разглашения, а также иных неправомерных действий в отношении ПД.

5.3.3. Для обеспечения безопасности ПД при их автоматизированной обработке в Организации осуществляются следующие организационные меры:

- а) функционирование организационной структуры системы обработки ПД;
- б) ограничение доступа работников Организации к средствам обработки и защиты ПД

ИСПД Организации;

в) обеспечение невозможности визуального просмотра ПД, отображаемых на экранах мониторов и зафиксированных на бумажных носителях ПД, лицами, не имеющими прав доступа к этим ПД;

г) принятие работниками Организации-пользователями и администраторами информационных систем персональных данных, а также ответственных за организацию обработки персональных данных всех ИСПД Организации, перечисленных в п.3.5.1 настоящего Положения (далее – всех ИСПД), обязательства не разглашать ПД, ставшие им известными при выполнении ими своих функциональных обязанностей;

д) строгое соблюдение пользователями и администраторами информационных систем персональных данных, а также ответственными за организацию обработки персональных данных всех ИСПД соответствующих инструкций, утвержденных генеральным директором Организации;

е) учет отчуждаемых и съемных носителей ПД всех ИСПД;

ж) обеспечение условий хранения отчуждаемых и съемных носителей ПД всех ИСПД, исключающих возможность их утраты, несанкционированного доступа к ним и несанкционированного воздействия на них;

з) восстановление ПД, целостность которых была нарушена в результате несанкционированных и (или) непреднамеренных воздействий на них или их носитель;

и) установление правил доступа к ПД, обрабатываемым во всех ИСПД, персонала ИСПД;

к) учет всех ПД, обрабатываемых во всех ИСПД и передаваемых другим операторам (органам государственной власти и юридическим лицам);

л) контроль за принимаемыми мерами по обеспечению безопасности ПД при их обработке в ИСПД.

5.3.4. Для обеспечения безопасности ПД при их автоматизированной обработке в Организации осуществляются следующие технические меры:

а) функционирование в составе всех ИСПД средств защиты информации (СрЗИ), функционально объединенных в систему защиты информации (СЗИ) ИСПД, реализующую выполнение требований к защите ПД, установленных в проектной документации на ИСПД;

б) использование для обеспечения безопасности ПД во всех ИСПД сертифицированных по требованиям безопасности информации СрЗИ;

в) использование в составе СЗИ ИСПД СрЗИ, осуществляющих идентификацию и аутентификацию пользователей и администраторов информационных систем персональных данных;

г) оборудование помещений, в которых размещаются компоненты всех ИСПД, а также хранятся отчуждаемые и съемные носители ПД, техническими средствами охранной и пожарной сигнализации, средствами физической защиты информации в соответствии с требованиями, установленными в проектной документации на ИСПД и в документах ФСТЭК (Гостехкомиссии) России;

д) использование специальных средств гарантированного уничтожения ПД, подлежащих уничтожению в соответствии с законодательством Российской Федерации и локальными правовыми актами Организации;

5.4. Меры, осуществляемые в Организации, по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации

5.4.1. Обработка персональных данных без использования средств автоматизации осуществляется в Организации в следующих его структурных подразделениях:

а) администрация;

б) бухгалтерии;

в) абонентский отдел;

г) паспортный стол;

д) аварийная служба

5.4.2. Обеспечение безопасности ПД при их обработке без использования средств автоматизации в Организации осуществляется применением организационных и технических мер с целями предотвращения неправомерного доступа к ним и их носителям, разглашения их, обеспечения их целостности и сохранности их носителей.

5.4.3. Для обеспечения безопасности ПД при их обработке без использования средств автоматизации в Организации осуществляются следующие организационные меры:

а) функционирование организационной структуры системы обработки персональных данных;

б) обеспечение возможности определения места хранения ПД на носителях ПД для каждой категории ПД и субъектов ПД;

в) установление перечня работников Организации, осуществляющих обработку ПД или имеющих право доступа к ним и (или) их носителям;

г) раздельное хранение ПД на носителях ПД, обработка которых осуществляется в различных целях;

д) принятие работниками Организации, осуществляющими обработку ПД или имеющими право



доступа к ним или их носителям, обязательства не разглашать ПД, ставшие им известными при выполнении своих должностных обязанностей;

е) запрет на несанкционированное копирование, уничтожение и изменение ПД.

5.4.4. Для обеспечения безопасности ПД при их обработке без использования средств автоматизации в Организации осуществляется следующие технические меры:

а) оборудование помещений, где осуществляется хранение носителей ПД, техническими средствами охранной и пожарной сигнализации (при необходимости);

б) использование средств физической защиты информации (средств и систем контроля и управления доступом в помещения, защитных ограждений оконных проемов);

в) использованием специальных технических средств гарантированного уничтожения носителей ПД, ПД на которых подлежат уничтожению в соответствии с законодательством Российской Федерации и локальными правовыми актами Организации.

5.5. Меры, осуществляемые в Организации по устранению нарушений законодательства, допущенных при обработке персональных данных

5.5.1. Работники Организации, непосредственно осуществляющие обработку ПД, могут случайно или преднамеренно допускать следующие нарушения законодательства Российской Федерации:

а) осуществлять неправомерную обработку ПД;

б) осуществлять обработку неточных ПД;

в) не прекращать обработку ПД в случае достижения цели обработки;

г) не прекращать обработку ПД в случае отзыва субъектом ПД согласия на обработку его ПД.

5.5.2. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных ответственный за организацию обработки этих ПД должен поручить администратору информационной системы персональных данных (если осуществлялась автоматизированная обработка этих ПД) или работнику Организации, неправомерно осуществлявшему обработку ПД, но имевшего право обрабатывать эти ПД (если осуществлялась обработка без использования средств автоматизации) осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки сроком не более трех дней, которая должна быть проведена под руководством названного ответственного. Если по результатам проверки выявлена невозможность обеспечить правомерную обработку ПД, ответственный обязан в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПД, организовать уничтожение этих ПД в установленном в Организации порядке.

5.5.3. Об устранении допущенных нарушений или об уничтожении персональных данных ответственный за организацию обработки персональных данных, организовавший проверку возможности правомерной обработки ПД, обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также орган.

5.5.4. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных ответственный за организацию обработки персональных данных этого субъекта должен поручить администратору информационной системы персональных данных (если осуществлялась автоматизированная обработка этих ПД) или работнику Организации, которому поручено осуществлять неавтоматизированную обработку ПД этого субъекта, осуществить блокирование этих неточных ПД с момента такого обращения или получения указанного запроса на период проверки, которую должен организовать названный ответственный, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

5.5.5. В случае подтверждения факта неточности ПД ответственный за организацию обработки персональных данных на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан обеспечить их уточнение в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных;

5.5.6. В случае достижения цели обработки персональных данных ответственный за организацию обработки этих ПД обязан организовывать прекращение обработки персональных данных и уничтожение персональных данных в срок, не превышающий тридцать дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Организацией и субъектом персональных данных либо если Организация не вправе осуществлять

обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

5.5.7. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных ответственный за организацию обработки этих персональных данных обязан обеспечить прекращение такой обработки и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, обеспечить их уничтожение 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 персональных данных, иным соглашением между Организацией и субъектом персональных данных либо если Организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

5.5.8. В случае отсутствия возможности уничтожения ПД в течение указанного в п.п. 5.5.4-

5.5.7 настоящего Положения срока, ответственный за организацию обработки этих персональных данных должен организовать блокирование таких ПД и обеспечить их уничтожение в установленном в Организации порядке в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.6 Меры, осуществляемые в Организации по уведомлению об обработке персональных данных

5.6.1. Организация до начала обработки персональных данных уведомляет Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Рязанской области (далее - Уполномоченный орган) о своем намерении осуществлять обработку персональных данных.

5.6.2. Уведомление готовят ответственные за организацию обработки персональных данных и главный специалист по защите информации. Руководит подготовкой уведомления и подписывает подготовленное уведомление координатор организации обработки персональных данных.

5.6.3. Уведомление направляется в письменной форме и содержит следующие сведения:

- а) наименование, адрес Организации;
- б) цели обработки персональных данных;
- в) категории обрабатываемых персональных данных;
- г) категории субъектов, персональные данные которых обрабатываются;
- д) правовое основание обработки персональных данных;
- е) перечень действий, осуществляемых с персональными данными, общее описание используемых в Организации способов обработки персональных данных;
- ж) описание мер, которые Организация осуществляет по обеспечению безопасности персональных данных, в том числе сведения об используемых шифровальных (криптографических) средствах и наименовании этих средств;
- з) дата начала обработки персональных данных;
- и) срок или условие прекращения обработки персональных данных;
- к) сведения о наличии или отсутствии трансграничной передачи персональных данных в процессе их обработки;
- л) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

5.6.3. Организация вправе осуществлять без уведомления Уполномоченного органа обработку персональных данных:

- а) обрабатываемых в соответствии с трудовым законодательством;
- б) полученных Организацией в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются Организацией исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- в) сделанных субъектом персональных данных общедоступными;
- г) включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- д) необходимых в целях однократного пропуска субъекта персональных данных в Здания Организации;
- е) включенных в информационные системы персональных данных, имеющие в соответствии с Федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- ж) обрабатываемых без использования средств автоматизации в соответствии с Федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими

требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

з) обрабатываемых 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.

5.6.4. В случае изменения сведений, указанных в пункте 5.6.3 настоящего Положения, Организация уведомляет об изменениях Уполномоченный орган в течение десяти рабочих дней с даты возникновения таких изменений. Уведомление об изменениях готовят должностные лица, указанные в п. 5.6.2 настоящего Положения.

## **6. ОРГАНИЗАЦИОННАЯ СТРУКТУРА СИСТЕМЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

6.1. Должностные лица, составляющие организационную структуру системы обработки персональных данных

6.1.1. Организационную структуру системы обработки персональных данных составляют:

а) координатор организации обработки персональных данных (далее – Координатор);

б) ответственные за организацию обработки персональных данных (далее – Ответственные);

в) администраторы информационных систем персональных данных (далее – Администраторы);

г) пользователи информационных систем персональных данных (далее – Пользователи);

д) руководители структурных подразделений, в которых осуществляется обработка ПД любого вида (далее – Руководители);

е) работники Организации, правомочно осуществляющие обработку ПД без использования средств автоматизации или имеющие право доступа к таким ПД или их носителям (далее – Обработчики ПД);

6.1.2. Общее руководство организацией обработки ПД в Организации осуществляет Координатор, которым по должности является заместителем генерального директора (генеральный директор).

6.1.3. Непосредственное руководство обработкой ПД в Организации осуществляют Ответственные, назначаемые приказом генерального директора по представлению Координатора.

6.1.4 Администраторы обеспечивают функционирование в соответствии с проектной документацией на эти системы и назначаются приказом руководителя организации.

6.1.5 Пользователи осуществляют автоматизированную обработку ПД с использованием выделенных им средств и назначаются приказом руководителя Организации.

6.1.6 Руководители осуществляют контроль за обработкой ПД в возглавляемых ими структурных подразделениях Организации, готовят представления генеральному директору о назначении Пользователей и (или) представления о назначении Обработчиков ПД (при условии обработки в их структурных подразделениях ПД без использования средств автоматизации).

6.1.7 Обработчики ПД осуществляют обработку ПД без использования средств автоматизации и назначаются приказом генерального директора по представлению Руководителей, возглавляющих структурные подразделения, в которых осуществляется обработка ПД без использования средств автоматизации.

6.2. Ответственность должностных лиц, составляющих организационную структуру системы обработки персональных данных Должностные лица, составляющие организационную структуру системы обработки персональных данных и перечисленные в подразделе 6.1. настоящего Положения несут за нарушение законодательства Российской Федерации в области персональных данных, локальных правовых актов Организации и настоящего положения уголовную, административную и дисциплинарную ответственность в соответствии с Уголовным кодексом Российской Федерации от 13.06.96 № 63-ФЗ, Кодексом Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ, Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ.

## **7. ОРГАНИЗАЦИЯ КОНТРОЛЯ ЗА ОБРАБОТКОЙ И ЗАЩИТОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ**

7.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства

7.1.1. Контроль за соблюдением структурными подразделениями Организации законодательства Российской Федерации и локальных правовых актов Организации в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в структурных подразделениях Организации законодательству Российской Федерации и локальным правовым актам Организации в области персональных данных, в том числе требованиям к защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области

персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

7.1.2. Внутренний контроль за соблюдением структурными подразделениями Организации законодательства Российской Федерации и локальных правовых актов Организации в области персональных данных, в том числе требований к защите персональных данных, осуществляется заместителем генерального директора (генеральным директором) Организации.

7.1.3. Внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящему Положению, локальным правовым актам Организации осуществляет ответственный за обработку персональных данных, назначенный приказом генерального директора.

7.1.4. Персональная ответственность за соблюдение требований законодательства Российской Федерации и локальных правовых актов Организации в области персональных данных в структурном подразделении Организации, а также за обеспечение безопасности персональных данных в указанных подразделениях Организации возлагается на их руководителей.

7.2. Организация контроля за автоматизированной обработкой персональных данных

7.2.1. Контроль за автоматизированной обработкой персональных данных субъектов персональных данных осуществляется администратором.

7.2.2. При обнаружении несанкционированного доступа к персональным данным субъектов персональных данных в, утечки персональных данных субъектов, а также нарушении установленного режима работы системы защиты информации, администратор обязан прекратить эксплуатацию ИСПД и доложить о случившемся администратору безопасности данной ИСПД.

7.2.3. Администратор безопасности ИСПД обязан принять меры по защите персональных данных субъектов, обрабатываемых в ИСПД, а в случае невозможности выполнения своих обязательств – доложить об этом Главному специалисту по защите информации.

7.2.4. На основании полученной информации, Главный специалист по защите информации с уведомлением генерального директора и Координатора имеет право приостановить эксплуатацию ИСПД до выяснения обстоятельств и устранения причин выявленных нарушений безопасности при обработке персональных данных субъектов персональных данных в ИСПД.

7.3. Организация защиты персональных данных при их автоматизированной обработке

7.3.1. Для автоматизированной обработки персональных данных в Организации по приказу генерального директора создается ИСПД.

7.4. Организация защиты персональных данных при их обработке без использования средств автоматизации

7.4.1. Организация защиты персональных данных при их обработке без использования средств автоматизации осуществляется ответственными за организацию обработки персональных данных.

7.4.2. Помощь Ответственным при организации защиты ПД при их обработке без использования средств автоматизации осуществляют работники Организации.

7.4.3. Ответственный в зависимости от конкретных условий обработки ПД выбирает необходимые организационные и технические меры, перечисленные в подразделе 5.4 Настоящего Положения.

7.4.4. Ответственный несет персональную ответственность за организацию защиты обрабатываемых ПД.

7.4.5. Координатор организации обработки персональных данных организует периодические проверки обеспечения безопасности ПД при их обработке без использования средств автоматизации, издавая соответствующие распоряжения по Организации.

7.5. Организация уничтожения персональных данных

7.5.1. Уничтожение персональных данных осуществляется:

а) по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом - в течение 30 дней;

б) при предоставлении субъектом персональных данных сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки – в течение 7 дней;

в) если невозможно обеспечить правомерность обработки персональных данных – в течение 10 дней;

г) в случае отзыва субъектом персональных данных согласия на обработку персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных – в течение 30 дней.

7.5.2. При невозможности уничтожения персональных данных в сроки, определенные Федеральным законом №152-ФЗ «О персональных данных» для случаев, когда невозможно обеспечить правомерность обработки персональных данных, при достижении целей обработки персональных данных, а также при

отзыве субъектом согласия на обработку персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных, Организация осуществляет блокирование персональных данных и уничтожает персональные данные в течение 6 месяцев, если иной срок не установлен федеральным законодательством Российской Федерации.

7.5.3. Уничтожение персональных данных в Организации производится способом, исключающим возможность восстановления этих персональных данных на материальном носителе.

7.5.4. Уничтожение носителей персональных данных в Организации производится комиссией, назначаемой распоряжением заместителя генерального директора(генерального директора) Организации. Комиссия составляет акт об уничтожении персональных данных, который утверждает заместитель генерального директора (директор).