УТВЕРЖДАЮ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование должности руководителя Компании)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, Ф.И.О.)

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**ПОЛОЖЕНИЕ**

об организации обработки персональных данных общества с ограниченной ответственностью «Кировский Коммунальный Расчетный Центр»  
(ООО «ККРЦ»)

ОГЛАВЛЕНИЕ

[I. Общие положения 3](#_Toc513484718)

[II. Основные понятия и определения 3](#_Toc513484719)

[III. Содержание обрабатываемых персональных данных 4](#_Toc513484720)

[IV. Порядок обработки, хранения и уничтожения персональных данных 6](#_Toc513484721)

[V. Организация защиты персональных данных 9](#_Toc513484722)

[VI. Права субъектов персональных данных 10](#_Toc513484723)

[VII. Обязанности и ответственность Компании и работников за нарушение норм, регулирующих обработку и защиту персональных данных 12](#_Toc513484724)

[VIII. Контроль и надзор за обработкой персональных данных. Ответственность за нарушения требований настоящего положения 16](#_Toc513484725)

1. **Общие положения**
   1. Настоящее Положение об обработке и защите персональных данных (далее – Положение) ООО «ККРЦ» разработано во исполнение   
      ст. 18.1 ч. 1 Федерального Закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – 152-ФЗ) и ст. 1 п. б Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами», а также в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», п. 32 пп. «е» Постановления Правительства РФ от 06.05.2011 N 354 «О предоставлении коммунальных услуг собственникам и пользователям помещений в многоквартирных домах и жилых домов», а также другими нормативными правовыми актами Российской федерации в области защиты персональных данных.
   2. Положение является документом, определяющим политику оператора в отношение обработки персональных данных работников ООО «ККРЦ» (далее – Компания), а также иных субъектов персональных данных, персональные данные которых подлежат обработке, на основании полномочий оператора.
   3. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым Положением.

Все изменения в Положение вносятся приказом Генерального директора.

* 1. Все сотрудники компании должны быть ознакомлены с настоящим Положением под роспись.

1. **Основные понятия и определения**

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

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

**Машинный носитель информации (МНИ)** - материальный носитель, содержащий информацию, представленную в форме, приспособленной для обработки с использованием средств вычислительной техники.

**Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

**Оператор** - 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.

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

**Субъекты персональных данных** – лица, чьи данные хранятся и обрабатываются компанией в процессе осуществления ей своей деятельности.

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

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

1. **Содержание обрабатываемых персональных данных**
   1. Обработка персональных данных осуществляется на законной и справедливой основе.
   2. Обработка персональных данных в Компании осуществляется в следующих случаях:
      1. на основании договора с управляющей компанией (далее - заказчиком), предоставляющей потребителям (субъектам персональных данных) жилищно-коммунальные услуги. При этом оператором, несущим ответственность перед субъектом персональных данных, является заказчик.

Обязанности по соблюдению Компанией законодательства Российской Федерации в области обработки персональных данных прописываются в соответствующих договорах с заказчиком. За нарушения вышеуказанных требований компания несет ответственность перед заказчиком, в рамках исполнения договора;

* + 1. на основании заключенного с субъектом персональных данных трудового договора.
  1. Требования по организации обработки и защиты персональных данных, обрабатываемых в Компании на основании требований  
     пп. 3.2.1 и 3.2.2 определяются гл. IV-VIII настоящего положения.
  2. **Цели обработки персональных данных:**

В случаях, предусмотренных п. 3.2.1 настоящего положения, цели обработки персональных данных определяет оператор (заказчик). Оператор также устанавливает перечень действий (операций) с персональными данными, которые будут совершаться Компанией и обязанности по соблюдению конфиденциальности персональных данных при их обработке. Все вышеуказанные сведения прописываются в поручении (договоре) оператора (заказчика).

В случаях, предусмотренных п. 3.2.2 настоящего положения, целью обработки персональных данных является обеспечение исполнения трудового законодательства при оформлении трудовых отношений работников с Компанией;

* 1. **В Компании обрабатываются персональные данные следующих категорий субъектов:**

- работники Компании (в том числе бывшие);

- клиенты Компании;

* 1. Исходя из целей обработки, а также категорий субъектов персональных данных, в Компании обрабатываются следующие персональные данные (для каждой из целей):
     1. **В целях обеспечения исполнения трудового законодательства при оформлении трудовых отношений работников с Организацией:**

- паспортные данные работника;

- информация, содержащаяся в трудовой книжке;

- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;

- сведения, содержащиеся в документах воинского учета;

- сведения об образовании, квалификации или наличии специальных знаний или подготовки;

- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;

- сведения о семейном положении;

- информация о заработной плате;

- другая персональная информация (рабочий и личный номер телефона, адрес электронной почты и т.д.).

* + 1. **В целях осуществление основной деятельности Компании, выполняемой на основании договора с заказчиком:**

- паспортные данные (фамилия, имя, отчество, дата и место рождения, пол, номер паспорта и сведения о выдавшем его органе)

- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;

- сведения о месте работы, специальности и занимаемой должности;

- адрес регистрации и адрес фактического проживания;

- семейное положение, состав семьи;

- сведения о наличии движимого и (или) недвижимого имущества;

- сведения о праве владения помещением (собственник/наниматель);

- сведения о площади принадлежащего жилого помещения;

- сведения, содержащиеся в свидетельстве о постановке на учет в Пенсионном Фонде Российской Федерации (страховое свидетельство);

- сведения, содержащиеся в документах воинского учета;

-другая персональная информация, предоставленная лично (контактный телефон, адрес электронной почты, и др.).

1. **Порядок обработки, хранения и уничтожения персональных данных**
   1. Приказом Генерального директора Компании назначаются:

- работник, ответственный за организацию обработки персональных данных;

- работник, ответственный за обеспечение безопасности персональных данных;

- работники, допущенные к обработке персональных данных[[1]](#footnote-1);

- места хранения носителей персональных данных и ответственные за их сохранность[[2]](#footnote-2);

- комиссия по уничтожению персональных данных[[3]](#footnote-3).

- комиссия по определению уровня защищенности персональных данных.

Конкретные обязанности, права и ответственность должностных лиц по обработке защите персональных данных определены в разделе 7 настоящего положения.

* 1. Доступ к персональным данным разрешен только должностным лицам, которым персональные данные необходимы для выполнения конкретных трудовых функций.

Допуск сотрудников к обработке персональных данных осуществляется на основании «Перечня лиц, доступ которых к персональным данным необходим для выполнения ими трудовых обязанностей», утвержденного приказом Генерального директора. Изменения в вышеуказанный перечень также, вносятся соответствующим приказом.

Основанием для прекращения допуска сотрудника к персональным данным служит увольнение или изменение его трудовых обязанностей.

Работники Компании, в обязанности которых входит работа с персональными данными, обеспечивают их защиту, о чем дают письменную расписку (Приложение № 1 к настоящему положению).

Содержание расписки допускается включать в текст трудового договора, либо дополнением к трудовому договору.

* 1. На основании требований пунктов 1, 4 Федерального закона от 2006 г. № 152-ФЗ «О персональных данных», а также пункта 16 статьи 155 Жилищного кодекса Российской Федерации от 29.12.2004 г. № 188-ФЗ, согласие субъекта персональных данных на обработку его персональных данных в Компании не требуется.
  2. Все персональные данные, обрабатываемые в Компании, получаются либо от самого субъекта, либо от заказчика. При этом у заказчика, являющегося оператором, с субъектом должен быть заключен договор, стороной которого является субъект.
  3. Документы, содержащие персональные данные создаются путем:

- копирования оригиналов документов (паспорта, документа об образовании, пенсионного свидетельства и др.);

- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.);

- внесения сведений в учетные формы и проекты документов.

* 1. Для обработки и хранения персональных данных Компании используются следующие носители информации:

**встроенные (несъемные) машинные носители информации** – то есть не демонтируемые из средств вычислительной техники в процессе их использования (встроенные жесткие диски ПЭВМ, SSD и т.д.);

**отчуждаемые (съемные) машинные носители информации** – то есть демонтируемые из средств вычислительной техники в процессе их использования (USB-flash накопители, USB HDD, оптические диски, дискеты и т.д.);

**бумажные носители информации –** распечатки с печатающих устройств средств вычислительной техники (отдельные листы бумаги, графические материалы и т.д.).

* 1. Все носители информации подлежат обязательному учету в делопроизводстве Компании.

Машинные носители информации (встроенные и отчуждаемые) учитываются в журнале учета машинных носителей информации (Приложение № 2 к настоящему положению).

* 1. При фиксации персональных данных на соответствующий носитель, не допускается фиксация на одном носителе персональных данных, цели обработки которых заведомо несовместимы.
  2. Необходимо обеспечить раздельное хранение носителей информации с персональными данными, для каждой из целей, предусмотренных п. 3.4 настоящего положения.
  3. При хранении носителей информации, содержащих персональные данные, должны соблюдаться условия, обеспечивающие сохранность таких данных и исключающие несанкционированный доступ к ним.
  4. Персональные данные, зафиксированные на бумажных носителях, а также съемных машинных носителях информации хранятся в запираемых шкафах (сейфах), закрепленных за соответствующими должностными лицами.
  5. Хранение персональных данных (в форме, позволяющей определить субъекта персональных данных) осуществляется не дольше, чем этого требуют цели их обработки, если иное не определено законодательством РФ.

Персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

* 1. Уничтожение документов (носителей), содержащих персональные данные производится путем сожжения, дробления (измельчения). Встроенные (несъемные) машинные носители информации уничтожаются после извлечения их из корпуса системного блока ПЭВМ. Для уничтожения бумажных документов допускается применение бумагорезательной машины (шреддера).
  2. Персональные данные на машинных носителях уничтожаются путем стирания или форматирования носителя.
  3. Уничтожение производится комиссией, указанной в п. 4.1 настоящего положения с составлением акта об уничтожении носителей персональных данных.

В акте об уничтожении носителей персональных данных указываются следующие сведения:

- состав комиссии;

- дата уничтожения;

- номер по порядку;

- тип носителя информации (машинный носитель информации, документ на бумажном носителе);

- Регистрационный номер носителя, количество листов и номера экземпляра (в случае уничтожения документов на бумажных носителях);

- категория персональных данных

В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых документов. Акт утверждается Генеральным директором Компании.

* 1. Передача персональных данных субъектов в пределах Компании осуществляется в соответствии с должностными инструкциями и распоряжениями Генерального директора.
  2. Передача персональных данных субъектов (за пределы Компании) разрешена только специально уполномоченным лицам. Передача персональных данных (без согласия субъекта) может осуществляться с целью обеспечения исполнения полномочий федеральных органов исполнительной власти, исполнительных органов государственной власти субъектов Российской Федерации и т.д., а также в иных случаях, предусмотренных Федеральным законом от 2006 г. № 152-ФЗ «О персональных данных».
  3. В соответствии договором, заключенным между заказчиком и ООО «ККРЦ», Компания обязана осуществлять доставку счет – квитанций до потребителей услуг. При этом, доставка указанных квитанций осуществляется через «Почту России».
  4. Передача персональных данных субъектов по телефону или факсу Запрещена.

1. **Организация защиты персональных данных**
   1. В соответствии с требованиями Федерального закона от 2006 г. № 152-ФЗ «О персональных данных» и других нормативных правовых актов Российской Федерации в Компании создана система защиты информации (далее – СЗИ), содержащей персональных данных.

СЗИ направлена на выявление, предотвращение и устранение последствий нарушений требований законодательства Российской Федерации в области персональных данных.

* 1. СЗИ состоит из подсистем правовой, организационной и технической защиты.
     1. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗИ.
     2. Подсистема организационной защиты включает в себя регламентацию деятельности Компании, а также взаимоотношений между сотрудниками и клиентами, на нормативно-правовой основе, исключающей (или существенно затрудняющей) неправомерное овладение персональными данными.
     3. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту персональных данных.
  2. Основными мерами защиты персональных данных Компании являются:

назначение лица ответственного за обработку персональных данных, которое организует обработку персональных данных, обучение, инструктаж и внутренний контроль за соблюдением работниками требований нормативных правовых актов РФ и внутренних организационно-распорядительных документов по защите персональных данных;

проведение в установленном порядке определения уровня защищенности персональных данных;

определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, и разработка мер и мероприятий по их защите;

оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных;

установление правил доступа к персональным данным, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

установление индивидуальных паролей доступа работников в информационную систему в соответствии с их должностными обязанностями;

применение, прошедших в установленном порядке процедуру оценки соответствия, средств защиты информации (средств разграничения доступа, антивирусной защиты и т.д.);

соблюдение условий, обеспечивающих сохранность персональных данных и исключение несанкционированного доступа к ним;

обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа;

осуществление внутреннего контроля и аудита.

* 1. Состав и содержание конкретных организационно – технических мер по обеспечению безопасности персональных данных, при их обработке в информационной системе Компании определен инструкцией по защите информации, составленной на основании Акта установки уровня защищенности персональных данных и модели угроз безопасности информации.

1. **Права субъектов персональных данных**

Субъект персональных данных имеет право:

* 1. Получать доступ к своим персональным данным и ознакомление с ними.
  2. Требовать уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.
  3. Получать по запросу от субъекта персональных данных, или его представителя информацию, касающуюся обработки его персональных данных, в том числе содержащей:
     1. подтверждение факта обработки персональных данных Компанией;
     2. правовые основания и цели обработки персональных данных;
     3. цели и применяемые Организацией способы обработки персональных данных;
     4. наименование и место нахождения Компании, сведения о лицах (за исключением работников Компании), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Компанией 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 «О персональных данных»;
     6. сроки обработки персональных данных, в том числе сроки их хранения;
     7. порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Положением;
     8. информацию об осуществленной или о предполагаемой трансграничной передаче данных;
     9. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных;
     10. иные сведения, предусмотренные Федеральным законом «О персональных данных» и настоящим Положением.

Запрос должен содержать номер основного документа, удостоверяющего личность, сведения о дате выдачи документа и выдавшем его органе, сведения (номер) о договоре, заключенном субъектом с Компанией, либо подпись, или данные иным образом подтверждающие факт обработки персональных данных оператором.

* 1. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Компании, при обработке и защите его персональных данных.
  2. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Федерального закона «О персональных данных».
  3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено, в том числе если:
     1. обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
     2. доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
     3. 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;
  4. В случаях, предусмотренных п. 3.2.1 настоящего положения, субъект персональных, для соблюдения своих прав обращается непосредственно к оператору (заказчику), если иное не установлено договором с управляющей компанией.

1. **Обязанности и ответственность Компании и работников за нарушение норм, регулирующих обработку и защиту персональных данных**
   1. Компания обязана:
      1. предоставить субъекту персональных данных по его просьбе информацию, предусмотренную п. 6.3 настоящего Положения, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных (или его представителя) либо в течение тридцати дней с даты получения запроса субъекта персональных данных дать (в письменной форме) мотивированный ответ об отказе в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных;
      2. разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с Федеральным законом;
      3. осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к субъекту персональных данных в случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных, его представителя, уполномоченного органа по защите прав субъектов персональных данных, либо по требованию оператора;
      4. уточнить персональные данные и снять блокирование персональных данных в случае подтверждения факта неточности в течение семи рабочих дней со дня представления таких сведений субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных;
      5. прекратить обработку персональных данных в случае выявления фактов неправомерной обработки персональных данных, осуществляемой Организацией, в срок, не превышающий трех рабочих дней;
      6. прекратить обработку и уничтожить персональные данные в случае достижения цели обработки персональных данных в срок, не превышающий тридцати дней с даты достижения цели, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.
      7. прекратить обработку персональных данных в случае отзыва субъектом персональных данных согласия на обработку его персональных данных;
      8. применять правовые, организационные и технические меры по обеспечению безопасности персональных данных.
      9. осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, и настоящему положению;
      10. оценивать вред, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона «О персональных данных», настоящего Положения;
   2. Общая организация работы с персональными данными субъектов возлагается на Генерального директора
   3. В целях реализации статьи 18.1 части 1 Федерального Закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», приказом Генерального директора назначается ответственный за организацию обработки персональных данных.
      1. Он обязан:

разрабатывать проекты организационных документов, регламентирующих порядок обработки персональных данных;

осуществлять внутренний контроль за соблюдением работниками Компании законодательства Российской Федерации о персональных данных;

доводить до сведения работников положения законодательства Российской Федерации о персональных данных и локальных актов по вопросам обработки персональных данных;

организовывать прием и обработку обращений и запросов субъектов персональных данных (или их представителей) и осуществлять контроль за приемом и обработкой указанных запросов;

разъяснять субъектам персональных данных юридические последствия отказа предоставления его персональных данных.

* + 1. Ответственный за организацию обработки персональных данных имеет право:

принимать решения в пределах совей компетенции и требовать от работников Компании соблюдения действующего законодательства, а также локальных нормативных актов о персональных данных;

контролировать в осуществление мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

взаимодействовать со структурными подразделениями Компании по вопросам обработки персональных данных;

давать свои предложения по совершенствованию системы обработки персональных.

* 1. В целях реализации статьи 14 Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных», приказом Генерального директора назначается ответственный за обеспечение безопасности персональных данных.
     1. Он обязан:

осуществлять внутренний контроль за соблюдением работниками Компании законодательства Российской Федерации о защите персональных данных;

разрабатывать организационно-планирующие документы и выполнять практические мероприятий по защите информации в информационных системах персональных данных Компании;

уточнять в установленном порядке обязанности всех групп пользователей информационных системах персональных данных по обеспечению безопасности персональных данных.

поддерживать необходимый уровень защищенности (режим безопасности) персональных данных при их обработке в информационной системе персональных данных;

обеспечивать антивирусную защиту информации в информационных системах персональных данных Компании;

обеспечивать безопасность персональных данных при проведении работ по сервисному техническому обслуживанию средств вычислительной техники;

генерировать, распределять и контролировать безопасность применения пользователями паролей, средств защиты информации (в том числе криптографических) и средств электронной подписи;

выявлять, устранять последствия и участвовать в проведении расследований фактов несанкционированного доступа к персональным данным или воздействия компьютерных вирусов;

анализировать состояние защиты информационных систем персональных данных и их отдельных подсистем;

контролировать неизменность состояния средств защиты информации, их параметров и режимов защиты;

В случае отказа работоспособности средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности

* + 1. Ответственный за обеспечение безопасности персональных данных имеет право:

принимать решения в пределах совей компетенции и требовать от работников Компании соблюдения действующего законодательства, а также локальных нормативных актов Компании о защите персональных данных;

блокировать доступ к персональным данным, при нарушении правил их обработки, неисправностях в работе средств защиты информации и с целью предотвращения несанкционированного доступа к персональным данным;

брать объяснения с работников Компании, в случае нарушения ими правил обработки и защиты персональных данных;

вносить предложения руководству по совершенствованию системы защиты персональных данных;

в пределах своей компетенции сообщать руководству о недостатках, выявленных в процессе исполнения должностных обязанностей, и вносить предложения по их устранению

* + 1. В случае необходимости разрешается совмещать обязанности ответственного за организацию обработки персональных данных и ответственного за обеспечение безопасности персональных данных.
  1. Работники, в соответствии со своими полномочиями владеющие информацией о субъектах персональных данных, получающие, хранящие и осуществляющие обработку персональных данных, несут персональную ответственность за нарушение режима защиты, обработки и порядка их использования.
     1. Работники Компании, допущенные в установленном порядке к обработке персональных данных обязаны:

знать цели и категории обрабатываемых ими персональных данных,

знать свои полномочия и права доступа к информации в информационной системе персональных данных;

знать и выполнять требования по защите и стиранию информации;

соблюдать установленный порядок учета, хранения и отправки машинных и бумажных носителей информации;

уметь самостоятельно применять средства защиты информации, антивирусной защиты и электронной подписи, установленные на рабочем месте;

соблюдать установленный порядок допуска к соответствующим категориям персональных данных лиц, не имеющих отношения к выполняемым работам;

запирать на замок помещения и хранилища носителей персональных данных при необходимости временного убытия;

сообщать ответственному за обеспечение безопасности персональных данных о фактах (или предпосылках) к несанкционированному доступу изменениях в конфигурации технических средств и программного обеспечения, компрометации (утрате) паролей, воздействии (подозрении воздействия) компьютерных вирусов;

предъявлять для проверки по требованию ответственного за организацию обработки и ответственного за обеспечение безопасности персональных данных все находящиеся на рабочем месте (в хранилище) носители информации.

* + 1. Работникам Компании, допущенных в установленном порядке к обработке персональных данных запрещается:

вносить изменения в состав, конструкцию, конфигурацию средств вычислительной техники и программного обеспечения;

обрабатывать категории персональных данных, к которым они не допущены;

осуществлять попытки несанкционированного доступа к защищаемой информации;

знакомить со значениями личных паролей и обрабатываемых персональных данных третьих лиц, и лиц, которые к ним не допущены;

устанавливать на средства вычислительной техники стороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

* 1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут ответственность в соответствии с действующим законодательством РФ:

- дисциплинарную;

- материальную;

- гражданско-правовую;

- административную;

- уголовную.

Состав мер административной и уголовной ответственности, для должностных и юридических лиц, предусмотренных за нарушения законодательства Российской Федерации в области персональных данных указан в приложении № 3 к настоящему положению.

1. **Контроль и надзор за обработкой персональных данных. Ответственность за нарушения требований настоящего положения**
   1. Ответственность за организацию и обеспечение выполнения требований законодательства Российской Федерации по защите персональных данных, а также настоящего положения возлагается на Генерального директора Компании.
   2. Контроль и надзор за обработкой персональных данных Компании осуществляет ответственный за обработку персональных данных. Он обязан:

осуществлять внутренний контроль за соблюдением Компанией и ее работниками законодательства Российской Федерации о персональных данных, настоящего положения, а также требований к защите персональных данных;

доводить до сведения работников Компании требования законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных и требования к защите персональных данных;

организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;

организовывать выполнение мероприятий, направленных на обеспечение безопасности персональных данных, обрабатываемых в информационной системе Компании;

инициировать проведение внутренних расследований по всем фактам нарушений законодательства Российской Федерации по защите персональных данных, а также настоящего положения.

|  |  |
| --- | --- |
| Ответственный за организацию обработки персональных данных | Ф.И.О. |

**Приложения:**

Приложение № 1: «Расписка работника о неразглашении персональных данных, ставших ему известными в ходе выполнения трудовых обязанностей».

Приложение № 2: «Журнал учета машинных носителей информации» (образец).

Приложение № 3: «Ответственность, предусмотренная, за нарушения, связанные с обработкой персональных данных».

Приложение № 1

к Положению об обработке и

защите персональных данных

РАСПИСКА

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, (Ф.И.О. полностью, должность)

паспорт серия \_\_\_\_№\_\_\_\_\_\_\_\_\_\_\_\_, выданный «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. \_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, (орган, выдавший документ)

проживающий по адресу:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

являясь работником общества с ограниченной ответственностью «Кировский коммунальный расчетный центр» (ООО «ККРЦ») (далее – Компания), находящейся по адресу: 610000, Кировская область, Киров г, Карла Либкнехта ул, дом 66 в период трудовых отношений с Компанией и после их окончания обязуюсь не разглашать сведения, составляющие персональные данные других работников и клиентов Компании, а также других лиц, которые будут мне доверены или станут мне известны в ходе выполнения трудовых обязанностей.

До моего сведения доведено действующее законодательство, нормативные акты и локальные акты Компании о безопасности персональных данных. Права и обязанности в области защиты персональных данных мне разъяснены.

Мне известно, что нарушение взятых на себя обязательств может повлечь дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством РФ.

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись и фамилия, имя, отчество прописью полностью)

Приложение № 2

к Положению об обработке и

защите персональных данных

**Ж У Р Н А Л**

учета машинных носителей информации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Учетный номер | Тип машинного носителя информации, его заводской номер, номер тома/количество томов | Принадлежность к средствам вычислительной техники | Дата постановки на учет | Учетный номер входящего документа, дата | Количество экземпляров | Номер экземпляра | Количество штук в экземпляре | Расписка в получении, дата | Расписка ответственного за учет в обратном приеме, дата | Отметка об уничтожении или номер исходящего документа, дата |
| 1 | 2 | 3 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 1 | CD-R зав.  № 38652В2 |  | *21.07.16* | - | 1 | 1 | 1 | *Иванов*  26.08.16 | *Петров*  26.08.16 | *Сидоров*  26.08.16 |
| 2 | USB – Flash «Transcend» 16 Gb зав. № 05RV2В2 |  | *22.07.16* | - | 1 | 1 | 1 | *Иванов*  26.08.16 | *Петров*  26.08.16 |  |
|  |  |  |  |  |  |  |  |  |  |  |

**Примечание:**

1. Каждый экземпляр машинного носителя информации одного учетного номера должен записываться отдельной строкой.
2. Регистрационный номер наносится на корпус (не рабочую поверхность) МНИ с использованием маркеров или механическим способом. Место маркировки должно обеспечить возможность его визуального обзора, а способ маркировки – ее сохранность с момента нанесения до окончания срока использования МНИ.

Приложение № 3

к Положению об обработке и

защите персональных данных

**Административная ответственность, предусмотренная, за нарушения, связанные с обработкой персональных данных.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Состав административного правонарушения | Нарушаемая статья законодательства | Штраф для должностных лиц | Штраф для юридических лиц |
|  | **Обработка персональных данных в случаях, не предусмотренных законодательством**, либо обработка персональных данных, **несовместимая с целями сбора** персональных данных | Ст. 5, ст. 6  ФЗ № 152 | 5 – 10 тысяч рублей | 30 – 50 тысяч рублей |
|  | **Обработка персональных данных без согласия** в письменной форме субъекта, на обработку его персональных данных,  Обработка персональных данных, **не включенных в согласие** в письменной форме субъекта, на обработку его персональных данных. | Ст. 9  ФЗ № 152 | 10 – 20 тысяч рублей | 15 – 75 тысяч рублей |
|  | **Невыполнение оператором обязанности по опубликованию** (или обеспечению неограниченного доступа) документа, определяющего **политику оператора в отношении обработки персональных данных**, или сведениям о реализуемых требованиях к защите персональных данных. | Ст. 18.2  ФЗ № 152 | 3 – 6 тысяч рублей | 15 – 30 тысяч рублей |
|  | **Невыполнение оператором обязанности по предоставлению** **субъекту** персональных данных **информации, касающейся обработки его персональных данных.** | Ст. 14, ст. 20  ФЗ № 152 | 4 – 6 тысяч рублей | 20 – 40 тысяч рублей (для ИП 10 – 15 тысяч рублей) |
|  | **Невыполнение оператором** в сроки, установленные законодательством Российской Федерации, **требования субъекта** персональных данных (его представителя или уполномоченного органа по защите прав субъектов персональных данных) **об уточнении** персональных данных, **их блокировании или уничтожении** в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки. | Ст. 21  ФЗ № 152 | 4 – 10 тысяч рублей | 25 – 45 тысяч рублей (для ИП 10 – 20 тысяч рублей) |
|  | **Невыполнение оператором** (при обработке персональных данных без использования средств автоматизации) **обязанности по соблюдению условий**, **обеспечивающих** **сохранность** **персональных данных** при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных. | ПП № 687 | 4– 6 тысяч рублей | 25 – 50 тысяч рублей (для ИП 10 – 20 тысяч рублей) |
|  | **Невыполнение оператором**, являющимся государственным или муниципальным органом, **обязанности по обезличиванию персональных данных** либо несоблюдение установленных требований или методов по обезличиванию персональных данных. | ПП № 211  Приказ РКН №996 | 3 – 6 тысяч рублей | Ответственность предусмотрена только для должностных лиц, |

**Статья 137 «Уголовного кодекса Российской Федерации»**

**от 13.06.1996 г. № 63-ФЗ**

**Нарушение неприкосновенности частной жизни**

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации -наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2. Те же деяния, совершенные лицом с использованием своего служебного положения - наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

3. Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия, - наказывается штрафом в размере от ста пятидесяти тысяч до трехсот пятидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от восемнадцати месяцев до трех лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от трех до пяти лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет.

1. В приказе указывается, какой работник, к каким данным имеет доступ, а также способ обработки этих данных (с помощью средств автоматизации или нет). В случае автоматизированной обработки персональных данных – дополнительно указывается роль пользователя в информационной системе персональных данных (пользователь, администратор и т.д.) [↑](#footnote-ref-1)
2. В приказе указываются номера помещений, места хранения носителей персональных данных (сейф, шкаф и т.д.) и фамилии ответственных должностных лиц. [↑](#footnote-ref-2)
3. Комиссия назначается из числа лиц, допущенных к обработке соответствующих персональных данных. [↑](#footnote-ref-3)