

КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ «ТРОИЦКАЯ ЦЕНТРАЛЬНАЯ РАЙОННАЯ
БОЛЬНИЦА» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ ХАБАРОВСКОГО
КРАЯ

ПРИКАЗ

от 17.12.2019 г.

№ 212

«Об утверждении положения об обработке и защите персональных данных работников краевого государственного бюджетного учреждения здравоохранения «Троицкая центральная районная больница» министерства здравоохранения Хабаровского края»

В соответствии с положениями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" в целях организации защиты персональных данных работников краевого государственного бюджетного учреждения здравоохранения «Троицкая центральная районная больница» министерства здравоохранения Хабаровского края от несанкционированного доступа и разглашения,

ПРИКАЗЫВАЮ:

1. Утвердить – Положение об обработке и защите персональных данных работников краевого государственного бюджетного учреждения здравоохранения «Троицкая центральная районная больница» министерства здравоохранения Хабаровского края, согласно приложению № 1 к настоящему приказу.
2. Начальнику отдела кадров - в срок до 31.12.2019 г. довести настоящий приказ до всех работников (по трудовым и гражданско-правовым договорам) краевого государственного бюджетного учреждения здравоохранения «Троицкая центральная районная больница» министерства здравоохранения Хабаровского края.
3. Положение об обработке и защите персональных данных работников краевого государственного бюджетного учреждения здравоохранения «Троицкая центральная районная больница» министерства здравоохранения Хабаровского края действует в учреждении - с 01.01.2020 г.
4. Контроль исполнения настоящего приказа оставляю за собой.

Основание:

- Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"


Главный врач
КГБУЗ «Троицкая ЦРБ»



С.Е. Кирдяшова

Приложение № 1
к приказу № 212 от 17.12.2019 г.
«Об утверждении положения об
обработке и защите персональных
данных работников краевого
государственного бюджетного
учреждения здравоохранения «Троицкая
центральная районная больница»
министерства здравоохранения
Хабаровского края»

УТВЕРЖДАЮ
главный врач КГБУЗ «Троицкая ЦРБ»

 /С.Е. Кирдяшова/
«17» декабря 2019 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников
краевого государственного бюджетного учреждения здравоохранения
«Троицкая центральная районная больница» министерства здравоохранения
Хабаровского края

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об обработке и защите персональных данных работников краевого государственного бюджетного учреждения здравоохранения «Троицкая центральная районная больница» министерства здравоохранения Хабаровского края (далее - Положение) разработано в целях обеспечения защиты прав работников при обработке их персональных данных, и устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников.

Под работниками подразумеваются лица, заключившие трудовой договор (и/или гражданско-правовой договор) с краевым государственным бюджетным

учреждением здравоохранения «Троицкая центральная районная больница» министерства здравоохранения Хабаровского края (далее – Учреждение).

1.2. Цель настоящего Положения - защита персональных данных работников Учреждения от несанкционированного доступа и разглашения. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

1.3. Настоящее Положение разработано на основании:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации от 30.12.2001 N 197-ФЗ;
- Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных";
- Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

- Постановления Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

- иных нормативно-правовых актов Российской Федерации.

1.4. Настоящее Положение и изменения к нему утверждается руководителем Учреждения и вводится соответствующим приказом.

На основе настоящего Положения учреждение разрабатывает инструкции по работе с персональными данными, которые носят обязательный характер для всех работников, занятых работой с персональными данными и/или кому такие данные стали известными в результате исполнения трудовых обязанностей.

1.5. Настоящее Положение являются обязательными для всех работников Учреждения. Работники Учреждения должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

1.6. Положение об обработке и защите персональных данных работников краевого государственного бюджетного учреждения здравоохранения «Троицкая центральная районная больница» министерства здравоохранения Хабаровского края действует в учреждении - с 01.01.2020 г.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. В настоящем Положении используются следующие основные понятия:

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

2) **оператор** - Краевое государственное бюджетное учреждение здравоохранения «Троицкая центральная районная больница» министерства здравоохранения Хабаровского края, 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;

3) **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

5) **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) **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;

9) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

2.2. Состав персональных данных работника:

- анкета;
- автобиография;
- образование;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;

- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- размер заработной платы;
- наличие судимостей;
- адрес места жительства;
- домашний (сотовый) телефон;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным работника;
- рекомендации, характеристики;
- принадлежность лица к конкретной нации, этнической группе, расе;
- привычки и увлечения, в том числе вредные (алкоголь, наркотики и др.);
- семейное положение, наличие детей, родственные связи;
- религиозные и политические убеждения (принадлежность к религиозной конфессии, членство в политической партии, участие в общественных объединениях, в том числе в профсоюзе, и др.);
- финансовое положение (доходы, долги, владение недвижимым имуществом, денежные вклады и др.);
- деловые и иные личные качества, которые носят оценочный характер;
- прочие сведения, которые могут идентифицировать человека.

Из указанного списка Учреждение вправе получать и использовать только те сведения, которые характеризуют физическое лицо, как сторону трудового договора (и/или гражданско-правового договора).

2.3. Персональные данные являются конфиденциальными.

Режим конфиденциальности персональных данных снимается в случаях их обезличивания, если иное не определено законом.

3. ОБЯЗАННОСТИ УЧРЕЖДЕНИЯ (РАБОТОДАТЕЛЯ)

3.1. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.1.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.1.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

3.1.3. Все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.1.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.1.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.1.6. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.1.7. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном законом и локальными актами Учреждения.

3.1.8. Работники и их представители должны быть ознакомлены под роспись с документами Учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.1.9. Лица, осуществляющие обработку персональных данных без использования средств автоматизации должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации.

4. ОБЯЗАННОСТИ РАБОТНИКА

Работник обязан:

4.1. Передавать работодателю или его представителю комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом Российской Федерации при приеме на работу.

4.2. Своевременно в разумный срок, не превышающий 5 дней, сообщать работодателю об изменении своих персональных данных.

4.3. Строго соблюдать требования инструкций руководства учреждения по защите персональных данных.

5. ПРАВА РАБОТНИКА

Работник имеет право:

5.1. На полную информацию о своих персональных данных и обработке этих данных.

5.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством Российской Федерации.

5.3. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных трудовым законодательством.

Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.4. Требовать извещения работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.5. Обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите его персональных данных.

5.6. Определять своих представителей для защиты своих персональных данных.

6. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

6.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители).

6.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации.

6.4. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

6.5. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

6.6. Работники Учреждения обеспечивают раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

6.7. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

6.8. Материальные носители с персональными данными должны храниться в запирающихся на ключ помещениях, металлических шкафах, сейфах, иных шкафах, имеющих запираемые блок-секции.

6.9. Должностным лицам, работающим с персональными данными, запрещается разглашать информацию, содержащую персональные данные, устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью и не запрещено законодательством РФ.

6.10. Не допускается без согласования с оператором формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные.

6.11. Передача персональных данных не допускается с использованием средств телекоммуникационных каналов связи (телефон, телефакс, электронная почта и т.п.) без письменного согласия субъекта персональных данных (**Приложение № 1,2,3**), за исключением случаев, установленных законодательством Российской Федерации.

Форма письменного согласия субъекта персональных данных может отличаться от установленной, но должна соответствовать законодательству РФ, регулирующие данные правоотношения.

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

6.13. Особенности обеспечения безопасности информации и конфиденциальности персональных данных, обрабатываемые без использования средств автоматизации, определяются внутренними документами Учреждения, регламентирующими данный порядок (**Приложение № 7**).

7. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

7.1. Безопасность персональных данных при их обработке в автоматизированных информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

7.2. Допуск должностных лиц к обработке персональных данных в автоматизированной информационной системе осуществляется на основании соответствующих разрешительных документов (приказов) и ключей доступа (паролей).

7.3. Размещение автоматизированных информационных систем, специальное оборудование и организация с их использованием работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в соответствующих помещениях посторонних лиц.

7.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа или под чужими, а равно общими (одинаковыми) паролями, не допускается.

7.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, не допускается (за исключением случаев: с письменного согласия субъекта персональных данных (**Приложение № 1,2,3**), установленных законодательством Российской Федерации).

7.6. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

7.7. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

7.8. При обработке персональных данных в автоматизированной информационной системе разработчиками, администраторами систем и иными уполномоченными лицами должны обеспечиваться:

- обучение лиц, использующих средства защиты информации, применяемые в автоматизированных информационных системах, правилами работы с ними;

- учет лиц, допущенных к работе с персональными данными в автоматизированной информационной системе, прав и паролей доступа;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- описание системы защиты персональных данных;

- иные требования по защите персональных данных, установленных инструкциями по их использованию и эксплуатации.

7.9. Особенности обеспечения безопасности информации и конфиденциальности персональных данных, связанные с использованием конкретных автоматизированных информационных систем, определяются внутренними документами Учреждения, регламентирующими порядок использования указанных информационных систем, а также эксплуатационной и инструктивной документацией, касающейся технических средств обработки персональных данных в рамках конкретной автоматизированной информационной системы (Приложение № 8).

8. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИХ ТВЕРДЫМИ КОПИЯМИ), А ТАКЖЕ ИХ УТИЛИЗАЦИИ

8.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

8.2. Ответственность за сохранность информации на съемных носителях персональных данных несут работники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Работники учреждения получают учтенный съемный носитель персональных данных от уполномоченного лица для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета съемных носителей. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному должностному лицу, о чем делается соответствующая запись в журнале учета.

8.3. Не допускается:

- хранение съемных носителей с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам;

- вынос съемных носителей с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

8.4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Вынос

съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с разрешения руководителя Учреждения.

8.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся на них сведений немедленно ставится в известность руководитель Учреждения.

На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

8.6. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению путем сжигания.

8.7. Перед уничтожением съемного носителя, отслужившим установленный срок, находящаяся на нем информация подлежит копированию на новый съемный носитель.

8.8. Уничтожение съемных носителей, отслуживших установленный срок, с конфиденциальной информацией и копирование указанной информации на новый съемный носитель осуществляется соответствующей комиссией, состав которой утверждается приказом руководителя Учреждения. По результатам уничтожения носителей составляется акт.

9. ПОРЯДОК ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. При передаче персональных данных работника оператор должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных законодательством РФ;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.

9.2. Обязанность оператора предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено считается исполненной с момента направления третьей стороне письменного уведомления по форме указанной в **Приложении № 4**

9.3. Согласие на передачу персональных данных третьим лицам составляется субъектом персональных данных по форме указанной в **Приложении № 3**

9.4. В случае если лицо, обратившееся с запросом, не уполномочено на получение персональных данных, либо отсутствует письменное согласие работника, оператор обязан отказать в предоставлении персональных данных.

Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении таких данных.

10. ПОРЯДОК ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

10.1. Право полного доступа к персональным данным работников имеют:

- главный врач;
- заместители главного врача;
- начальник отдела кадров.

Другие категории работников (специалисты и др.) имеют право ограниченного доступа к персональным данным, в объеме необходимом для исполнения своих служебных обязанностей.

При необходимости реализации отдельных полномочий руководства учреждения работник с ограниченным правом доступа к персональным данным может быть временно допущен к исполнению обязанностей или поручений, которые требуют полного допуска к таким данным.

Решение о полном допуске к персональным данным принимает лицо, имеющее право полного доступа к персональным данным, который несет ответственность за принятое решение в соответствии с действующим законодательством наравне с лицом, получившим такой допуск. Решение о полном допуске к персональным данным оформляется письменно.

10.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

10.3. Персональные данные предоставляются субъекту персональных данных или его представителю оператором при обращении, либо при получении запроса субъекта персональных данных или его представителя.

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

10.5. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с

оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.

Форма запроса указана в **Приложении № 5**

11. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

11.2. Лица, нарушившие требования настоящего Положения, несут дисциплинарную ответственность в соответствии с локальными нормативными актами Учреждения в порядке, предусмотренным трудовым законодательством РФ.

11.3 Лица, состоящие в трудовых и/или гражданско правовых с Учреждением, подписывает обязательство о неразглашении персональных данных, согласно форме указанной в **Приложении № 6**