УТВЕРЖДАЮ

И.о. директора ГУ ТО «Социально-реабилитационный центр для несовершеннолетних №3»

_____ (А.А. Федина)

«02» августа 2021 г.

Положение об обработке и защите персональных данных работников и получателей социальных услуг в ГУ ТО «Социально-реабилитационный центр для несовершеннолетних № 3»

1. Общие положения

1.1. Настоящее Положение ГУ ТО «Социально-реабилитационный центр для несовершеннолетних № 3» (далее – Учреждение) разработано в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и защите информации", Трудовым кодексом Российской Федерации, другими действующими нормативными правовыми актами Российской Федерации (далее - Положение).

1.2. Цель настоящего Положения - защита персональных данных работников и получателей социальных услуг Учреждения от несанкционированного доступа и разглашения. Персональные данные работников всегда являются конфиденциальной, строго охраняемой информацией, в соответствии с действующим законодательством Российской Федерации.

1.3. Положение устанавливает порядок получения, учета, обработки, накопления, хранения и распространения информации, содержащей сведения, отнесенные к персональным данным работников Учреждения, получателей социальных услуг и их законных представителей. Под работниками и получателями социальных услуг подразумеваются лица, заключившие договор с Учреждением.

1.4. Положение и изменения к нему утверждаются руководителем Учреждения и вводятся его приказом. Все работники Учреждения, имеющие доступ к персональным данным, должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

2. Понятие и состав персональных данных

2.1. Персональными данными является любая информация, прямо или косвенно относящаяся к субъекту персональных данных - определенному или определяемому физическому лицу. Под информацией о сотрудниках и получателях социальных услуг понимаются сведения о фактах, событиях и обстоятельствах жизни сотрудника и получателя социальных услуг, позволяющие идентифицировать его личность.

2.2. Персональные данные сотрудников, получателей социальных услуг и их законных представителей используются учреждением, в частности, в целях выполнения требований:

- трудового законодательства при приеме на работу и заключении трудового договора, в процессе трудовых отношений, при предоставлении гарантий и компенсаций и др.;

- налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц;

- пенсионного законодательства при формировании и предоставлении персонифицированных данных о каждом получателе доходов, учитываемых при

начислении страховых взносов на обязательное пенсионное страхование и обеспечение;

- заполнение первичной статистической документации в соответствии с постановлением Госкомстата РФ от 05.01.2004 г. №1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;

- для реализации и исполнения Федерального закона от 21.05.1999 г. № 120 «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних», Федерального закона от 28 декабря 2013 г. №442 "Об основах социального обслуживания граждан в Российской Федерации", Гражданского Кодекса РФ и других действующих нормативно правовых актов РФ.

2.3. Персональные данные являются строго конфиденциальными, любые лица, получившие к ним доступ, обязаны хранить эти данные в тайне (Приложение 1). Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

2.4. В состав персональных данных сотрудников учреждения входят:

- 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;
- свидетельство о присвоении ИНН;
- страховое пенсионное свидетельство СНИЛС;
- адрес места жительства;
- номер контактного телефона или сведения о других способах связи;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, трудовые книжки и сведения о трудовой деятельности работников;
- 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 работодатель вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора.

2.5. В состав персональных данных получателей социальных услуг входят:
- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- число, месяц, год рождения;
- место рождения;
- информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- сведения о составе семьи;
- семейное положение, наличие детей, родственные связи;
- адрес места жительства;
- номер контактного телефона или сведения о других способах связи;
- место учебы;
- сведения о родителях, попечителях, опекунах;
- принадлежность лица к конкретной нации, этнической группе, расе;
- привычки и увлечения, в том числе вредные (алкоголь, наркотики и др.);
- медицинские сведения;
- свидетельство о присвоении ИНН;
- страховое пенсионное свидетельство СНИЛС;
- сведения о наличии судимостей;
- прочие сведения, которые могут идентифицировать человека.

3. Носители персональных данных

3.1. Бумажные носители персональных данных:
- трудовая книжка;
- автобиография;
- приказы директора;
- листки нетрудоспособности;
- материалы по учету рабочего времени;
- личная карточка Т-2;
- входящая и исходящая корреспонденция военкомата, страховой компании, правоохранительных органов;
- договора;
- личные дела сотрудников и получателей социальных услуг.

3.2. Электронные носители персональных данных - база 1С-бухгалтерия, СБИС, информационная система «Адресная социальная помощь», Региональная система электронного правительства Тульской области.

3.3. Персональные данные на бумажных носителях хранятся в сейфе (закрытом на ключ шкафу).

3.4. Персональные данные на электронных носителях защищены паролем доступа, доступ к специализированной программе осуществляется только через личный доступ и пароль, право на использование персональных данных имеют только сотрудники, ответственные за обработку персональных данных.

4. Обязанности работодателя

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

4.2. 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.

4.3. 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.

4.4. 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, работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

4.5. 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.

4.6. 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.

4.7. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

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

5. Права и обязанности сотрудников, получателей социальных услуг и их законных представителей в области защиты их персональных данных

5.1. В целях защиты персональных данных, хранящихся в учреждении, сотрудники, получатели социальных услуг и их законные представители имеют право:

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

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

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

законодательством. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения.

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

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

5.1.6. Определять своих представителей для защиты своих персональных данных.

5.1.7. На сохранение и защиту своей личной и семейной тайны.

5.2. Работник обязан:

5.2.1. Передавать работодателю или его представителю комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом Российской Федерации. Работодатель проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами. Представление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

5.2.2. Своевременно в разумный срок, не превышающий 5 дней, сообщать работодателю об изменении своих персональных данных. Сотрудники ставят учреждение в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

5.2.3. В целях защиты частной жизни, личной и семейной тайны сотрудники, получатели социальных услуг и их законные представители не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

6. Сбор, обработка и хранение персональных данных

6.1. Под обработкой 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.

6.2. Обработка персональных данных 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.

6.3. При определении объема и содержания обрабатываемых персональных данных сотрудников Учреждения и получателей социальных услуг оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом, Федеральным законом №120 «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних», Федеральным законом от 28 декабря 2013 г. №442 "Об основах социального обслуживания граждан в Российской Федерации", и иными действующими нормативно правовыми актами РФ.

6.4. Получение персональных данных получателей социальных услуг может осуществляться как путем представления их самими получателями социальных услуг, их родителями, опекунами, так и путем получения их из иных источников. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Оператор должен сообщить сотруднику 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;

6.5. В случаях, непосредственно связанных с вопросами трудовых и социально реабилитационных отношений, данные о частной жизни сотрудника и получателя социальных услуг (информации о жизнедеятельности в сфере семейных бытовых, личных отношений, взаимодействие членов семьи) могут быть получены и обработаны оператором только с его письменного согласия;

6.6. Обработка персональных данных осуществляется с согласия сотрудника, получателя социальных услуг или его законного представителя на обработку его персональных данных (Приложения 2, 3).

6.7. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

6.8. Письменное согласие работника на обработку своих персональных данных должно включать:

- фамилию, имя, отчество, адрес субъекта персональных данных, паспортные данные;
- наименование и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

6.9. Согласие работника не требуется, если:

- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона;
-обработка персональных данных осуществляется в целях исполнения трудового договора;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
-персональные данные являются общедоступными;
-персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;
-персональные данные обрабатываются по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом;

6.10. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

6.11. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

6.12. При принятии решений, затрагивающих интересы сотрудника получателя социальных услуг, оператор не имеет права основываться на их персональных

данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

7. Передача и распространение персональных данных

Передача ПД может осуществляться путем их распространения, предоставления или открытием доступа к ним.

7.1. При передаче персональных данных физического лица Учреждение должно соблюдать следующие требования:

- не сообщать персональные данные физического лица третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы его жизни и здоровью, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные физического лица в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные физического лица, 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. Лица, получающие персональные данные, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен персональными данными физического лица в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников и получателей социальных услуг только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные физического лица их представителям в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.
- не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

7.2. Распространение персональных данных — это один из видов передачи данных, при котором персональные данные раскрываются неопределенному кругу лиц.

7.3. Согласие на обработку персональных данных, разрешенных работником, получателем социальных услуг и их представителями для распространения, оформляется отдельно от иных согласий на обработку их персональных данных (Приложение 4). Данное согласие должно содержать перечень сведений, разрешенных физическим лицом к распространению среди неограниченного круга лиц. Оператор обязан обеспечить физическому лицу возможность самостоятельно определить содержание данного перечня персональных данных.

7.4. Физическое лицо вправе установить запрет на передачу (кроме предоставления доступа) своих общедоступных данных неограниченному кругу лиц. Право на установление такого запрета является безусловным. Отказ оператора в установлении данного запрета не допускается. При установлении запрета на дальнейшую обработку и распространение своих общедоступных сведений, оператор, первоначально получивший согласие, обязан будет публично уведомить о таком запрете всех третьих лиц и в течение трех рабочих дней изъять эти сведения из общего доступа.

7.5. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в лю-

бое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

7.6. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

7.7. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения

8. Доступ к персональным данным

8.1. Внутренний доступ (доступ внутри Учреждения).

8.1.1. Право доступа к персональным данным сотрудников, получателей социальных услуг и их законных представителей, необходимых для выполнения конкретных функций в пределах компетенции имеют:

- директор учреждения;
- специалист по кадрам;
- заместители директора;
- главный бухгалтер;
- бухгалтеры;
- юрисконсульт;
- системный администратор;
- заведующие отделениями;
- специалисты по социальной работе;
- педагог-психолог;
- педагог-организатор;
- логопед;
- дефектолог;
- медицинская сестра;
- врач-педиатр;
- работники Учреждения, получатели социальных услуг и их законные представители - носители данных.

8.1.2. Перечень лиц, допущенных к обработке персональных сотрудников, получателей социальных услуг и их законных представителей утверждается приказом директора.

8.1.3. Другие сотрудники Учреждения имеют доступ к персональным данным только с письменного согласия самого работника, получателя социальных услуг и его законного представителя, носителя данных.

8.2. Внешний доступ.

8.2.1. К числу массовых потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры. Не требуется согласие работника на передачу персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника;
- в Фонд социального страхования Российской Федерации, Пенсионный фонд Российской Федерации в объеме предусмотренном действующим законодательством Российской Федерации;
- в налоговые органы;
- в военные комиссариаты;
- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства работодателем;
- по мотивированному запросу органов прокуратуры;
- по мотивированному требованию правоохранительных органов и органов безопасности;
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- по запросу суда;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом;
- в случаях, связанных с исполнением работником должностных обязанностей;
- в кредитную организацию, обслуживающую платежные карты работников
- министерство труда и социальной защиты Тульской области;

8.2.2 Надзорно - контрольные органы имеют доступ к информации только в сфере своей компетенции.

8.2.3 Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным сотрудника только в случае его письменного разрешения.

8.2.4. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии заверенного заявления работника.

8.2.5. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника. В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

9. Порядок обработки персональных данных субъектов персональных данных в информационных системах

Обработка персональных данных в учреждении осуществляется в информационной системе 1С бухгалтерия, информационная система «Адресная социальная помощь», Региональная система электронного правительства Тульской области. в целях обеспечения соблюдения трудового и финансового законодательства.

Информационная система содержит персональные данные, указанные в пунктах 2.4. и 2.5 настоящего Положения.

Специалистам, имеющим право осуществлять обработку персональных данных в информационных системах учреждении, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе

9.1. Обеспечение безопасности персональных данных, обрабатываемых в ин-

формационных системах персональных данных, достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

9.2. Должностное лицо, ответственное за обеспечение информационной безопасности, организует и контролирует ведение учета материальных носителей персональных данных.

9.3. Должностное лицо за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных, должно обеспечить:

- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;
- разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

9.4. Должностное лицо, ответственное за обеспечение функционирования информационных систем персональных данных, принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

9.5. Обмен персональными данными при их обработке в информационных системах персональных данных осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

9.6. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

10.Защита персональных данных сотрудников, получателей социальных услуг и их законных представителей

10.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

10.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

10.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

10.4. Регламентация доступа сотрудников к конфиденциальным сведениям, документам и базе данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами учреждения.

10.5. Внутренняя защита.

Для защиты персональных данных сотрудников, воспитанников и их законных представителей необходимо соблюдать ряд мер:

- ограничение и регламентация состава специалистов, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудником требований нормативно - методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками учреждения;
- не допускается выдача личных дел сотрудников и воспитанников на рабочие места сотрудников, не имеющим право доступа к персональным дан-

ным сотрудников, воспитанников и их законных представителей.

10.6. Внешняя защита.

10.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

10.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, посетители, работники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров.

10.6.3. Для защиты персональных данных сотрудников, воспитанников и их законных представителей необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим;
- требования к защите информации при интервьюировании и собеседованиях.

10.6.4. Персональные компьютеры, в которых содержатся персональные данные субъектов защищаются паролями доступа. Пароли устанавливаются системным администратором оператора и сообщаются индивидуально сотруднику, допущенному к работе с персональными данными и осуществляющему обработку персональных данных субъектов.

10.6.5. В целях защиты оператор использует защищенный канал связи через ViPNet «деловая почта» для отправки персональных данных.

11. Сроки обработки и хранения персональных данных

11.1. Сроки обработки и хранения персональных данных определяются в соответствии с законодательством Российской Федерации. С учетом положений законодательства, устанавливаются следующие сроки обработки и хранения персональных данных сотрудников.

11.2. Персональные данные, содержащиеся в приказах по личному составу (о приеме, о переводе, об увольнении, об установлении надбавок и т.д.) хранятся в архиве в течение 75 лет.

11.3. Персональные данные, содержащиеся в личных делах, а также личных карточках, хранятся в архиве в течение 75 лет.

11.4. Персональные данные, содержащиеся в приказах о предоставлении отпусков, о краткосрочных командировках, подлежат хранению в кадровом подразделении в течение пяти лет с последующим уничтожением.

11.5. Персональные данные граждан, обратившихся в учреждение лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в течение пяти лет.

11.6. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

11.7. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют ответственные должностные лица, назначенные приказом директора учрежде-

ния.

11.8. Срок хранения персональных данных, внесенных в информационные системы персональных данных учреждения, должен соответствовать сроку хранения бумажных оригиналов.

12. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

12.1. Документы, содержащие персональные данные, с истекшими сроками хранения, подлежат уничтожению.

12.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании экспертной комиссии учреждения (далее - комиссия), состав которой утверждается приказом директора учреждения.

По итогам заседания составляются протокол и Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами комиссии и утверждается директором учреждения.

12.3. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

13. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

13.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

13.2. Директор учреждения, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

13.3. Каждый сотрудник учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

13.4. 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.

13.5.За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

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

13.7.В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

13.8.Уголовная ответственность за нарушение неприкосновенности частной жизни

(в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

13.9.Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

14.Заключительные положения

14.1. Настоящее Положение вступает в силу с момента его утверждения директором учреждения и действует бессрочно, до замены его новым Положением.

14.2. Все изменения в Положение вносятся приказом директора.

14.3. Все сотрудники учреждения должны быть ознакомлены с настоящим Положением под роспись.

14.4. Оператор во исполнение требований п.2, ст. 18.1. Федерального закона №152-ФЗ от 27 июля 2006 года «О персональных данных» для обеспечения неограниченного доступа к сведениям о реализуемых учреждением мероприятиях по защите персональных данных, и к документам, определяющим политику учреждения в отношении обработки персональных данных, размещает текст настоящего Положения на сайте учреждения.

Специалист по кадрам: _____ / А.С.Юркова

Юрисконсульт: _____ С.В. Митрофанова