

ПОЛОЖЕНИЕ

**по организации и проведению работ по обеспечению
безопасности персональных данных при их обработке
в казенном учреждении Воронежской области
«Нижедевицкий социально – реабилитационный
центр для несовершеннолетних»**

Содержание

Термины и определения	3
1. Общие положения	4
2. Область применения	5
3. Процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере ПД.....	5
4. Порядок обработки персональных данных в Учреждении	6
4.1. Определение способов обработки персональных данных в Учреждении.....	6
4.2. Обработка персональных данных в автоматизированном режиме.....	6
4.3. Обработка ПД, осуществляемая без использования средств автоматизации.....	6
4.4. Цели обработки персональных данных	8
4.5. Состав персональных данных	8
4.6. Условия и порядок обработки персональных данных.....	8
4.7. Правила рассмотрения запросов субъектов персональных данных или их представителей	10
4.8. Сроки обработки и хранения персональных данных	10
4.9. Лицо, ответственное за организацию обработки персональных данных в Учреждении	11
5. Общая характеристика информационных систем персональных данных	11
6. Правила работы с обезличенными персональными данными.....	12
7. Обеспечение безопасности персональных данных	12
8. Структура организационной системы обеспечения безопасности персональных данных.....	13
9. Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных	14
10. Организация доступа к персональным данным	15
11. Организационные меры обеспечения безопасности персональных данных, связанные с персоналом	16
12. Обязанности лиц, допущенных к обработке персональных данных в информационных системах	16
13. Учет лиц, допущенных к персональным данным, обрабатываемым в информационных системах	17
14. Организация парольной защиты	17
15. Использование ресурсов сети Интернет	18
16. Антивирусная защита.....	19
17. Организация антивирусной защиты в Учреждении	19
18. Учет носителей информации	20
19. Порядок хранения электронных носителей персональных данных	20
20. Резервирование информации	21
21. Порядок уничтожения персональных данных по достижении цели обработки	21
22. Контроль состояния обеспечения безопасности персональных данных в Учреждении	21
23. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных	22
24. Реагирование на инциденты нарушения информационной безопасности и сбои	23
24.1. Информирование об инцидентах нарушения информационной безопасности	23
24.2. Информирование о проблемах безопасности	23
24.3. Информирование о сбоях программного обеспечения	24
24.4. Реагирование на факты разглашения персональных данных	24
25. Ответственность за разглашение персональных данных	24
Приложение 1	25
Приложение 2	26
Приложение 3	27
Приложение 4	28
Приложение 5	29
Приложение 6.	30
Приложение 7.	35
Приложение 8.	36
Приложение 9.....	37

Термины и определения

В рамках настоящего Положения используются следующие термины, определения и понятия:

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

документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным субъектов, требование не допускать их распространения без согласия субъекта или иного законного основания;

обезличивание персональных данных – действия, в результате которых невозможно 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;

обработка персональных данных без использования средств автоматизации (неавтоматизированная) – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;

общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами РФ не распространяется требование соблюдения конфиденциальности;

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

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

субъект персональных данных – физическое лицо, чьи персональные данные подлежат обработке;

уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1. Общие положения

1.1. Положение по организации и проведению работ по обеспечению безопасности персональных данных (далее – Положение) при их обработке в казенном учреждении Воронежской области «Нижедевицкий социально-реабилитационный центр для несовершеннолетних» (далее – Учреждение) разработано в целях организации обработки персональных данных сотрудников и иных субъектов, персональные данные которых подлежат обработке в Учреждении, определения порядка получения, обработки, передачи персональных данных, установления прав, обязанностей и ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и общий порядок организации работ по обеспечению безопасности персональных данных.

1.2. Настоящее Положение разработано на основе «Концепции информационной безопасности при обработке персональных данных в органах социальной защиты населения Воронежской области», утверждаемой приказом Департамента, Политики информационной безопасности и в соответствии с требованиями Конституции Российской Федерации, Трудового кодекса Российской Федерации, Кодекса Российской Федерации об административных правонарушениях, Гражданского кодекса Российской Федерации, Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 21 марта 2012 года № 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 или муниципальными органами», от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказов Федеральной службы по техническому и экспортному контролю Российской Федерации от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и других нормативных правовых актов.

1.3. Целью организации обработки персональных данных и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах Учреждения является обеспечение конституционных прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.4. Обработка персональных данных должна осуществляться на основе следующих принципов:

- обработка персональных данных должна осуществляться на законном основании;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;
- обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- Учреждение должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

- обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- соблюдения принципов и правил обработки персональных данных при поручении такой обработки другому лицу;
- соблюдение конфиденциальности персональных данных;
- соблюдение обязанностей, возлагаемых на Учреждение персональными данными, действующим законодательством и иными нормативными актами по персональным данным;
- принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в области персональных данных;
- недопустимость ограничения прав и свобод человека и гражданина по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных;
- недопустимость использования оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных;
- личной ответственности должностных лиц, осуществляющих обработку персональных данных;
- документального оформления всех принятых решений по обработке персональных данных.

1.5. Требования настоящего Положения должны пересматриваться при появлении новых угроз безопасности персональных данных, при изменении организационной структуры системы защиты персональных данных Учреждения, в других случаях при необходимости внесения изменений в организацию и порядок проведения работ по защите информации.

2. Область применения

Требования настоящего Положения носят обязательный характер для всех сотрудников Учреждения, в целях выполнения должностных обязанностей имеющих доступ к персональным данным, а также для сотрудников Учреждения, на которых возложено решение задач обеспечения безопасности персональных данных. Работники Учреждения, участвующие в обработке персональных данных, должны быть ознакомлены с настоящим Положением под роспись.

3. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

Обработка персональных данных в информационных системах Учреждения должна осуществляться на законной и справедливой основе.

Учреждение устанавливает следующие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных:

- издание нормативных правовых актов Департамента по вопросам обработки и защиты персональных данных;
- назначение ответственных за организацию обработки и обеспечение безопасности персональных данных;
- определение сотрудников, допущенных к обработке (получение, хранение, передача и т.д.) (далее - обработка) персональных данных в Учреждении и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных;
- ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, под роспись до начала работы с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, обеспечение обучения указанных работников;

- получение персональных данных лично у субъекта персональных данных, в случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных, в случае возникновения необходимости получения персональных данных у третьей стороны Учреждение извещает об этом субъекта персональных данных заранее, получает его письменное согласие и сообщает ему о целях, предполагаемых источниках и способах получения персональных данных;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- опубликование на официальном сайте Учреждения в информационно-телекоммуникационной сети Интернет документов, определяющих политику Учреждения в отношении обработки персональных данных;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, политике Учреждения в отношении обработки персональных данных, локальным актам Учреждения.

4. Порядок обработки персональных данных в Учреждении

4.1. Определение способов обработки персональных данных в Учреждении.

Обработка персональных данных подразделяется на:

- обработка персональных данных, осуществляемая в автоматизированном режиме (в информационных системах (ИС));
- обработка персональных данных, осуществляемая без использования средств автоматизации.

4.2. Обработка персональных данных в автоматизированном режиме

4.2.1. Обработка персональных данных в ИС с использованием средств автоматизации осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

4.2.2. Не допускается обработка персональных данных в ИС с использованием средств автоматизации, если применяемые меры и средства обеспечения безопасности не соответствуют требованиям, утвержденным Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.2.3. Обработка персональных данных с использованием средств автоматизации осуществляется в рамках ИС Учреждения и внешних информационных систем, предоставляемых сторонними организациями.

4.3. Обработка ПДн, осуществляемая без использования средств автоматизации

4.3.1 Правила обработки персональных данных без использования средств автоматизации. Сотрудники Учреждения, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Учреждением без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Учреждения.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации; имени (наименовании) и адресе Учреждения; фамилию, имя, отчество и адрес субъекта персональных данных; источник получения персональных данных; сроки обработки персональных данных; перечень действий с персональными данными, которые будут совершаться в процессе их обработки; общее описание используемых Учреждением способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

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), в специальных разделах или на полях форм (бланков).

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.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

4.3.2. Порядок обработки персональных данных без использования средств автоматизации. Обработка персональных данных без использования средств автоматизации осуществляется в рамках осуществления кадровой и бухгалтерской работы с персоналом Учреждения, в том числе присвоения квалификационных категорий, подготовки и переподготовки, проведения конкурсов, конференций, обучающих семинаров, а также в рамках повышения качества оказываемых услуг (прием жалоб граждан на качество оказываемых услуг).

Обработка персональных данных без использования средств автоматизации, осуществляемая в рамках ведения кадровой деятельности Учреждения, осуществляется при заключении трудового договора с работником, заполнении им личной карточки формы Т-2, автобиографии и другой необходимой при приеме на работу документации:

- паспорт или иной документ, удостоверяющий личность;

- трудовая книжка, за исключением случаев, когда работник принимается на работу впервые или на условиях совместительства;

- страховое свидетельство государственного пенсионного страхования;

- документы воинского учета – для военнообязанных и лиц, подлежащих призыву на военную службу (военный билет);

- документы об образовании, о квалификации или наличии специальных знаний (диплом, свидетельство об аттестации и присвоении категории, документ об усовершенствовании или специализации);

- личная медицинская книжка;

- документы о присвоении ученой степени, ученого звания;

- документы, подтверждающие те или иные факты, касающиеся жизни сотрудника (например, свидетельство о заключении брака и расторжении брака, свидетельство о рождении ребенка);

- документы, подтверждающие наличие наград, присвоения званий и т.д.;

- свидетельство о постановке на учет в налоговом органе (при наличии);

- необходимые справки (например, справка о доходах по форме НДФЛ-2 с прежнего места работы, справка об отсутствии судимости по соответствующим статьям УК РФ и др.).

4. 4. Цели обработки персональных данных

Обработка персональных данных в Учреждении осуществляется в целях:

- выполнения полномочий по реализации на территории области государственной политики по социальной поддержке и социальному обслуживанию населения;
- организации кадрового и бухгалтерского учета сотрудников Учреждения.

4.5. Состав персональных данных

4.5.1. Состав (объем и содержание) персональных данных определяется нормативными правовыми актами, устанавливающими порядок предоставления мер социальной поддержки, социального обслуживания, кадрового, бухгалтерского учета, иными документами, регламентирующими порядок осуществления полномочий Учреждения. Состав персональных данных не должен превышать перечень информации, необходимой для реализации конкретных полномочий.

4.5.2. Субъектами персональных данных, сведения о которых обрабатываются в информационных системах Учреждения, являются:

- работники – сотрудники Учреждения по трудовым договорам, физические лица, с которыми заключены договоры на оказание услуг, бывшие сотрудники, уволившиеся из Учреждения;
- соискатели – кандидаты для приема на работу в Учреждение;
- граждане, обратившиеся и направленные в Учреждение за получением социальных услуг.

Для перечисленных субъектов персональных данных Учреждение выполняет функции оператора.

4.5.3 Оператор получает сведения о персональных данных субъекта из следующих источников:

- информация, представляемая гражданином при обращении за социальной поддержкой, социальным обслуживанием: паспорт или иной документ, удостоверяющий личность, удостоверение о праве на льготы (при необходимости), документы МСЭ (при необходимости), страховое свидетельство обязательного пенсионного страхования, справка о составе семьи, справка о доходах, другие документы, установленные порядком предоставления социальной поддержки, социального обслуживания;
- информация, представляемая работником при поступлении на работу в Учреждение: паспорт или иной документ, удостоверяющий личность, трудовая книжка, страховое свидетельство обязательного пенсионного страхования, документы воинского учета, документ об образовании, о квалификации или наличии специальных знаний, свидетельство о присвоении ИНН;
- анкетные сведения, заполняемые субъектом персональных данных при обращении или при приеме на работу;
- иные документы и сведения, предоставляемые субъектом персональных данных;
- сведения, полученные в рамках межведомственного информационного взаимодействия, в том числе через систему межведомственного электронного взаимодействия.

4.6. Условия и порядок обработки персональных данных

4.6.1. 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.

4.6.2. Обработка персональных данных осуществляется оператором с согласия субъектов персональных данных, за исключением случаев, предусмотренных федеральными законами.

Субъект персональных данных является собственником своих персональных данных и самостоятельно по своей воле принимает решение о передаче оператору своих персональных данных и дает согласие на их обработку, за исключением случаев, предусмотренных федеральным законодательством. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

Типовая форма согласия субъекта на обработку его персональных данных в связи с поступлением на работу в Учреждение приведена в приложении 1 к настоящему Положению.

В случае отказа предоставить ПДн оператор обязан разъяснить субъекту ПДн или его законному представителю юридические последствия отказа предоставления ПДн. Форма разъяснения представлена в Приложении 5.

4.6.3. Получение, хранение, передача или любое другое использование персональных данных субъекта персональных данных осуществляется исключительно в целях реализации основных полномочий Учреждения, обеспечения соблюдения законов и иных нормативных правовых актов.

4.6.4. Получение персональных данных может осуществляться как путем представления их самим субъектом, так и путем получения их из иных источников.

4.6.5. Если планируется получение персональных данных у третьей стороны, то субъект уведомляется об этом заранее и от него должно быть получено письменное согласие. Оператор сообщает субъекту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

4.6.6. Обработку персональных данных в Учреждении осуществляют должностные лица, допущенные к данной обработке.

Состав должностных лиц, имеющих доступ к обработке персональных лиц, определяется на основе заявок руководителей структурных подразделений Учреждения на предоставление прав (полномочий) доступа пользователя к персональным данным.

Внутри учреждения к разряду потребителей персональных данных, помимо руководителя и его заместителей, относятся сотрудники структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- сотрудники структурного подразделения «Административно-управленческий персонал» (директор, заместитель директора по воспитательной и реабилитационной работе, главный бухгалтер, бухгалтер, юрисконсульт, инспектор по кадрам, техник-программист, заведующий складом);
- сотрудники структурного подразделения «Медицинское обслуживание» (заведующий медицинским кабинетом, врач-педиатр, медицинская сестра, медицинская сестра диетическая);
- сотрудники структурного подразделения «Организация питания» (повар);
- сотрудники структурного подразделения «Хозяйственно-обслуживающий персонал» (машинист по стирке и ремонту спецодежды);
- сотрудники структурного подразделения «Социально-трудовая реабилитация и культурно-воспитательное обслуживание» (заведующий отделением, специалист по социальной работе, социальный педагог, воспитатель, педагог-психолог, инструктор по труду, младший воспитатель).

4.6.7. Учреждение на основании договора может поручать обработку персональных данных третьим лицам. Передача документов (иных материальных носителей), содержащих персональные данные, третьим лицам осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг или соглашения об информационном взаимодействии;
- соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных граждан;
- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные гражданина, ее перечень, цель использования, фамилию, имя, отчество и должность лица, которому поручается получить данную информацию.

4.6.8. Передача персональных данных третьим лицам осуществляется с составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные субъектов.

4.6.9. Не допускается получение и обработка персональных данных субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

4.6.10. Положение по организации обработки персональных данных лиц, непосредственно получающих социальные услуги в Учреждении, а также формы согласий на обработку персональных данных приведены в приложениях 6,7,8,9 к настоящему Положению.

4.6.11. Процедура оформления доступа к персональным данным субъекта предусматривает ознакомление с настоящим Положением, лиц, допущенных к обработке персональных данных, под роспись, а также истребование с лиц, допущенных к обработке персональных данных, письменного обязательства о соблюдении конфиденциальности персональных данных субъекта и соблюдении правил их обработки, подготовленного по форме, приведенной в приложении 3.

4.7. Правила рассмотрения запросов субъектов персональных данных или их представителей.

4.7.1. Субъект персональных данных (его законный представитель) имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к гражданину, а также на ознакомление с такими персональными данными. Гражданин вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Обращения субъектов персональных данных о соблюдении их законных прав регистрируются учреждением – оператором в специальном журнале. Форма журнала приведена в приложении 2 к настоящему Положению.

4.7.2. Сведения о наличии персональных данных при обращении субъекта персональных данных предоставляются субъекту персональных данных оператором в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос содержит номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4.7.3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
- способы обработки персональных данных, применяемые оператором;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

4.8. Сроки обработки и хранения персональных данных

4.8.1. Персональные данные, связанные с реализацией трудовых отношений, обрабатываются и хранятся в течение срока действия служебного контракта (трудового договора) и в течение 75 (семидесяти пяти) лет после его прекращения.

4.8.2. Персональные данные, связанные с предоставлением мер социальной поддержки, социального обслуживания, обрабатываются и хранятся до достижения цели их обработки, в соответствии с правилами бухгалтерского учета и в соответствии с «Перечнем типовых управленческих документов, образующихся в деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», утвержденным приказом Министерства культуры РФ от 25.08.2010 №558.

4.9. Лицо, ответственное за организацию обработки персональных данных в Учреждении

4.9.1. Приказом Учреждения назначается лицо, ответственное за организацию обработки персональных данных в Учреждении (далее - Ответственное лицо).

4.9.2. Ответственное лицо получает указания непосредственно от директора Учреждения и подотчетно ему.

4.9.3. Ответственное лицо обязано:

- осуществлять внутренний контроль за соблюдением в учреждении законодательства Российской Федерации о персональных данных, в том числе за соблюдением правил обработки персональных данных;
- доводить до сведения сотрудников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований 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.

5. Общая характеристика информационных систем персональных данных

5.1. Обработка персональных данных граждан осуществляется в следующих информационных системах Учреждения:

5.1.2. В целях бухгалтерского учета, взаимодействия и обмена информацией с ПФР, налоговой службой, ФСС используется программный продукт «СБИС++ Электронная отчетность»), включающий следующие сведения:

фамилия, имя, отчество, дата рождения субъекта персональных данных;

данные документа, удостоверяющего личность субъекта персональных данных;

адрес места жительства субъекта персональных данных;

должность субъекта персональных данных;

ИНН субъекта персональных данных;

номер страхового свидетельства обязательного пенсионного страхования субъекта персональных данных;

сведения о доходах.

5.1.3. В целях учета несовершеннолетних – получателей социальных услуг – и их родителей (законных представителей) используется программный продукт «АРМ Реабилитация», включающий следующие сведения:

фамилия, имя, отчество субъекта персональных данных;

число, месяц, год и место рождения;

пол;

образование;

состояние здоровья;

домашний адрес (адрес регистрации, фактического проживания);

социальный статус;

сведения о семье и о родителях;

6. Правила работы с обезличенными персональными данными

6.1. Обезличивание персональных данных в Учреждении может проводиться с целью снижения ущерба от разглашения персональных данных, снижения класса защищенности информационных систем персональных данных и по достижении целей обработки персональных данных или утраты необходимости в достижении этих целей.

Способы обезличивания персональных данных:

- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений;
- деление сведений на части и обработка в разных информационных системах.

6.2. Решение о необходимости обезличивания персональных данных принимает директор Учреждения.

6.3. Кадровая служба Учреждения готовит предложения по обезличиванию персональных данных, обоснование такой необходимости и способы обезличивания.

6.4. Список лиц, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, утверждается приказом Учреждения.

6.5. Контроль за соблюдением проводимых мероприятий по обезличиванию персональных данных осуществляется в рамках внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных.

7. Обеспечение безопасности персональных данных

7.1. Мероприятия по обеспечению безопасности персональных данных являются составной частью управленческой и производственной деятельности Учреждения и осуществляются во взаимосвязи с другими мерами по обеспечению защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

7.2. Информационная безопасность – механизм защиты, обеспечивающий:

- конфиденциальность: доступ к информации только авторизованных пользователей;
- целостность: достоверность и полноту информации и методов ее обработки;
- доступность: доступ к информации авторизованных пользователей по мере необходимости.

7.3. Организация и проведение работ по обеспечению безопасности персональных данных в Учреждении осуществляются в соответствии со следующими принципами:

- законности осуществляемых в Учреждении целей, способов обработки персональных данных и мероприятий по обеспечению безопасности персональных данных;
- обеспечения баланса интересов государства, Учреждения, работников и иных субъектов, персональные данные которых подлежат обработке в Учреждении;
- обеспечения соответствия осуществляемых в Учреждении мероприятий по обеспечению безопасности персональных данных требованиям правовых, нормативных и методических документов федеральных органов исполнительной власти, уполномоченных в области защиты персональных данных;
- обеспечения соответствия осуществляемых в Учреждении мероприятий по обеспечению безопасности персональных данных составу и уровню опасности угроз безопасности персональных данных;
- комплексности проводимых мероприятий по обеспечению безопасности персональных данных;
- непрерывности и преемственности мероприятий по обеспечению безопасности персональных данных;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных (достаточности персональных данных для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных).

7.4. Под организацией обеспечения безопасности персональных данных при их обработке в информационных системах понимается формирование и всестороннее обеспечение реализации совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредованного ущерба от возможной реализации угроз безопасности персональных данных в информационных системах, и осуществляемых на всех стадиях жизненного цикла информационных систем персональных данных в целях:

- предотвращения возможных (потенциальных) угроз безопасности;
- нейтрализации и/или парирования реализуемых угроз безопасности;
- ликвидации последствий реализации угроз безопасности и восстановления нормального функционирования информационных систем персональных данных.

7.5. Система защиты персональных данных, в общем случае, представляет собой совокупность организационных мер и технических средств защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемых в информационных системах персональных данных информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности персональных данных. Структура, состав и основные функции системы защиты персональных данных определяются в соответствии с частными моделями угроз безопасности персональных данных и классами информационных систем персональных данных.

Основные меры обеспечения безопасности персональных данных определены в Политике информационной безопасности.

8. Структура организационной системы обеспечения безопасности персональных данных

8.1. Управление и координация деятельности Учреждения по обеспечению безопасности персональных данных осуществляются комиссией Учреждения по обеспечению безопасности персональных данных (далее – комиссия Учреждения).

8.2. Организация работ по обеспечению безопасности персональных данных и поддержанию достигнутого уровня защиты персональных данных на этапах эксплуатации информационных систем персональных данных в Учреждении возложены на заместителя директора по воспитательной и реабилитационной работе и техника-программиста.

8.3. В целях обеспечения безопасности персональных данных заместитель директора по воспитательной и реабилитационной работе и техник-программист взаимодействуют со всеми структурными подразделениями Учреждения, сотрудники которых имеют доступ к информационным системам персональных данных.

8.4. В зависимости от задач и целей создания информационных систем персональных данных, а также обрабатываемых в них персональных данных ответственными за обеспечение безопасности персональных данных при их обработке в информационных системах назначаются сотрудники Учреждения.

8.5. Ответственность за организацию и выполнение правил обеспечения безопасности персональных данных в структурных подразделениях Учреждения возложена на руководителей структурных подразделений Учреждения.

8.6. Комиссия учреждения:

8.6.1. Осуществляет руководство деятельностью по разработке и актуализации документов Учреждения по обеспечению безопасности персональных данных, в том числе:

- приказов учреждения по вопросам безопасности персональных данных;
- перечня сведений конфиденциального характера;
- положений, руководств, регламентов и инструкций по вопросам организации и контроля обеспечения информационной безопасности.

8.6.2. Осуществляет контроль выполнения требований документов, регламентирующих деятельность по обеспечению информационной безопасности работниками Учреждения.

8.7. Заместитель директора по воспитательной и реабилитационной работе и техник-программист:

8.7.1. Отвечают за ведение и актуализацию документов Учреждения по обеспечению безопасности персональных данных, в том числе:

- списков сотрудников, допущенных к обработке персональных данных (по подразделениям Учреждения, по информационным системам);
- актов классификации информационных систем персональных данных;
- моделей (частных моделей) угроз безопасности информационных систем персональных данных.

8.7.2. Руководят и контролируют работу лиц, ответственных за обеспечение безопасности персональных данных при их обработке в информационных системах, в части реализации правил (политик) безопасности (разрешительная система доступа), настроек средств защиты информации, состава пользователей информационных систем.

8.7.3. Отвечают за ведение и актуализацию эксплуатационной документации Учреждения по обеспечению безопасности персональных данных, в том числе:

- журналов учета выданных паролей;
- журналов учета внешних носителей персональных данных;
- документации на средства защиты информации, включая лицензии, сертификаты.

8.8. Руководители структурных подразделений Учреждения, ответственные за вопросы обеспечения информационной безопасности в своих подразделениях:

- организуют контроль выполнения мероприятий по защите персональных данных в подразделениях;
- отвечают за ведение и актуализацию списка сотрудников, допущенных к обработке персональных данных (по информационным системам);
- отвечают за своевременную подачу заявок на допуск сотрудников к обработке персональных данных в информационных системах Учреждения;
- отвечают за своевременное предоставление информации об исключении из списка лиц, допущенных к обработке персональных данных в информационных системах, сотрудников отделов (в связи с увольнением, изменением должностных обязанностей, переводом на другую работу (должность, отдел) и т.д.).

8.9. Лица, ответственные за обеспечение безопасности персональных данных при их обработке в информационных системах:

- осуществляют контроль за администрированием информационных систем в части вопросов обеспечения информационной безопасности;
- взаимодействуют с администраторами информационных систем.

8.10. Администраторы информационных систем осуществляют администрирование информационных систем персональных данных Учреждения.

8.11. Пользователи информационных систем персональных данных:

- осуществляют обработку персональных данных в информационных системах персональных данных Учреждения согласно установленным для них правам доступа и полномочиям;
- отвечают за выполнение правил обработки персональных данных и правил доступа к информационным ресурсам информационных систем персональных данных, установленными положениями, регламентами и инструкциями Учреждения;
- отвечают за целостность и сохранность установленных на их автоматизированных рабочих местах средств защиты информации;
- отвечают за правильное использование внешних носителей персональных данных, их своевременный учет в журналах учета внешних носителей персональных данных.

9. Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных

Помещения, в которых размещается оборудование, предназначенное для обработки персональных данных в информационных системах, хранятся машиночитаемые носители и документы, содержащие конфиденциальную информацию, расположены рабочие места специалистов, осуществляющих обработку персональных данных, должны исключать возможность бесконтрольного проникновения в них посторонних лиц, обеспечивать сохранность оборудования, машиночитаемых носителей информации и документов, защиту конфиденциальной информации от несанкционированного доступа.

Для этого входные двери этих помещений оборудуются прочными, оборудованными надежными замками. Окна помещений, расположенных на первых этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, защищаются металлическими решетками (при необходимости).

9.2. В помещениях, где размещены технические средства, участвующие в обработке персональных данных, а также хранятся носители персональных данных (далее - Помещения), право самостоятельного доступа имеют только сотрудники Учреждения, рабочие места которых размещены в соответствующем Помещении.

9.3. Нахождение посторонних лиц и лиц, не имеющих права доступа к персональным данным, в этих помещениях допускается только в присутствии работников, ответственных за расположенные в них рабочие места. При этом исключается возможность доступа посторонних лиц к обрабатываемым персональным данным через выводимую на экран монитора и принтер информацию, а также к носителям персональных данных.

9.4. Средства вычислительной техники, с помощью которых осуществляется обработка персональных данных и другой конфиденциальной информации, располагаются таким образом, чтобы был исключен несанкционированный просмотр информации, выводимой на экраны мониторов и на другие средства отображения информации.

9.5. В рабочее время, в случае ухода всех сотрудников, имеющих право самостоятельного доступа, из Помещения, а также в нерабочее время дверь в Помещение закрывается на ключ.

9.6. Уборка Помещения проводится только в присутствии сотрудника, имеющего право самостоятельного доступа в Помещение.

Техническое обслуживание средств вычислительной техники, коммуникационного оборудования, входящих в состав объекта информатизации, осуществляется только персоналом, допущенным к техническому обслуживанию под наблюдением сотрудника, ответственного за автоматизированное рабочее место. При проведении данных работ обработка конфиденциальной информации запрещена.

На время проведения ремонта Помещения все технические средства, участвующие в обработке персональных данных, а также носители персональных данных переносятся в другое Помещение, используемое для обработки персональных данных.

Для проведения регламентных (наладочных), ремонтных и других работ во время обработки конфиденциальной информации посторонние лица допускаются в эти помещения только в экстренных случаях по согласованию с должностным лицом, ответственным за обеспечение информационной безопасности, и в присутствии лиц, ответственных за обработку персональных данных, при условии исключения несанкционированного доступа к персональным данным и иной конфиденциальной информации и контроля за порядком осуществления проводимых работ.

Ремонт (вне помещений Учреждения), списание, утилизация (выбытие), реализация и другие действия с оборудованием, на котором обрабатывались или хранились информационные системы персональных данных, осуществляется только при условии, если информация, находящаяся на носителях информации этого оборудования, надежно удалена (стерта) без возможности ее восстановления и последующего прочтения, о чем составляется соответствующий акт.

Контроль за соблюдением порядка доступа сотрудников в Помещения осуществляют руководители структурных подразделений Учреждения.

10. Организация доступа к персональным данным

10.1. Организация доступа к персональным данным реализуется оператором с соблюдением принципов конфиденциальности, доступности и целостности таких данных.

10.2. Обеспечение конфиденциальности персональных данных не требуется:

- в отношении общедоступных персональных данных;
- в случае обезличивания персональных данных.

10.3. Доступ к персональным данным субъекта имеют сотрудники Учреждения в соответствии с занимаемой должностью, правами и полномочиями, которым эти данные необходимы для выполнения должностных обязанностей.

Сотрудники Учреждения, которым персональные данные необходимы для выполнения должностных обязанностей, подписывают обязательство о неразглашении персональных данных субъектов. Форма обязательства приведена в приложении 3 к настоящему Положению.

10.4. Правила и порядок оформления доступа сотрудников Учреждения к персональным данным, а также порядок разграничения доступа к ним определяются положением о разрешительной системе доступа Учреждения.

10.5. Доступ сторонних организаций к персональным данным осуществляется в соответствии с действующим законодательством, а также в рамках реализации договорных отношений или по письменным запросам, по решению руководителя Учреждения.

10.6. Доступ сотрудников Учреждения к персональным данным может быть приостановлен по решению должностных лиц, ответственных за обеспечение безопасности персональных данных, в следующих случаях:

- увольнение работника;
- выявление нарушений работником правил обработки и защиты персональных данных, установленных федеральным законодательством, локальными нормативными правовыми актами Учреждения, настоящим Положением;
- изменение должностных обязанностей, перевода на другую работу.

11. Организационные меры обеспечения безопасности персональных данных, связанные с персоналом

11.1. Все сотрудники, имеющие доступ к персональным данным, обязаны четко знать и строго выполнять установленные правила и обязанности по доступу к персональным данным и соблюдению режима безопасности персональных данных.

11.2. Лица, осуществляющие обработку персональных данных, информируются о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти Воронежской области, настоящим документом.

11.3. Обязанности по соблюдению требований безопасности включаются в трудовые договоры.

11.4. Все сотрудники, осуществляющие обработку персональных данных, подписывают обязательство о неразглашении персональных данных граждан.

11.5. При вступлении в должность нового сотрудника руководитель структурного подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, настоящим документом, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования персональных данных.

12. Обязанности лиц, допущенных к обработке персональных данных в информационных системах

12.1. Лица, допущенные к обработке персональных данных, другой конфиденциальной информации, обязаны:

- не сообщать конфиденциальную информацию лицам, не имеющим права доступа к ней;
- обеспечивать сохранность материальных носителей с конфиденциальной информацией;
- не делать неучтенных копий на бумажных и электронных носителях;
- не оставлять включенными персональные компьютеры с предоставленными правами доступа в информационные системы персональных данных, не оставлять материалы с конфиденциальной информацией на рабочих столах. После окончания работы (в перерывах) покидая рабочее место, сотрудник обязан убрать документы и электронные носители с конфиденциальной информацией в закрываемые на замок сейфы, шкафы, столы, и т.п.;
- не оставлять незапертыми помещения, в которых расположены рабочие места работников, имеющих доступ к персональным данным, на время отсутствия работников на рабочих местах;
- не вносить изменения в настройку средств защиты информации, не изменять и не тиражировать программное обеспечение;
- не осуществлять самостоятельно дополнительную установку каких-либо программных и/или аппаратных средств на персональные компьютеры;
- использовать аппаратные и программные средства только в служебных целях;

- при работе с документами, содержащими конфиденциальную информацию, исключать возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними;
- не выносить документы и иные материальные носители с конфиденциальной информацией, а также их копии из служебных помещений, предназначенных для работы с ними;
- немедленно сообщать непосредственному руководителю о недостатке, утрате, утечке или искажении конфиденциальной информации, об обнаружении неучтенных материалов с указанной информацией;
- не допускать действий, способных повлечь утечку конфиденциальной информации.

13. Учет лиц, допущенных к персональным данным, обрабатываемым в информационных системах

13.1. Допуск к персональным данным, обрабатываемым в информационной системе, лицам, доступ которых к защищаемой информации необходим для выполнения служебных (трудовых) обязанностей, должен производиться в соответствии с порядком, установленным разрешительной системой доступа.

13.2. Разрешительная система доступа составляется на каждую информационную систему персональных данных и содержит перечень лиц, допущенных к обработке персональных данных в информационной системе, с указанием уровня прав доступа.

13.3. Ведение разрешительной системы доступа возложено на кадровую службу Учреждения.

13.4. Основанием для обеспечения доступа к персональным данным, обрабатываемым в информационных системах, и включения должностных лиц в разрешительную систему доступа являются сведения, подаваемые руководителями структурных подразделений оператора.

14. Организация парольной защиты

14.1. В целях обеспечения защиты от несанкционированного доступа к персональным данным и регистрации действий пользователей с персональными данными в информационных системах персональных данных организуется система парольной защиты.

14.2. Для обеспечения доступа к информационным системам персональных данных всем пользователям устанавливаются личные пароли. Личные пароли доступа к средствам информационных систем персональных данных выдаются пользователям лицом, ответственным за обеспечение безопасности персональных данных.

14.3. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть.
- пароль должен состоять не менее чем из 6 символов.
- в пароле должны присутствовать символы трех категорий:
прописные буквы русского, английского алфавита;
строчные буквы русского, английского алфавита;
цифры (от 0 до 9).

Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).

Запрещается выбирать пароли, которые уже использовались ранее.

14.4. Обязательным требованием организации парольной защиты является полная плановая смена паролей в информационных системах персональных данных не реже одного раза в 3 месяца. Ответственным за проведение плановой смены паролей является лицо, ответственное за обеспечение безопасности персональных данных.

14.5. Правила ввода пароля:

- ввод пароля осуществляется с учетом регистра, в котором пароль был задан;
- во время ввода паролей исключается возможность его подсматривания посторонними лицами или техническими средствами.

14.6. Правила хранения пароля:

запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

14.7. Лица, допущенные к обработке персональных данных в информационных системах Учреждения, обязаны:

- четко знать и строго выполнять требования организации парольной защиты;
- своевременно сообщать должностному лицу, ответственному за обеспечение безопасности персональных данных, об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

Запрещается:

- вести разговоры с посторонними лицами о процедурах доступа к информационным системам и информации;
- набирать на клавиатуре при посторонних лицах персональный пароль и записывать его;
- сообщать устно или письменно свой персональный пароль.

15. Использование ресурсов сети Интернет

15.1. Подключение информационных систем персональных данных к сетям общего доступа и (или) международного обмена (сети Интернет и других), не допускается.

15.2. При необходимости подключения средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных и другой конфиденциальной информации, к сетям общего доступа и (или) международного обмена (сети Интернет и других) такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

15.3. Решение об организации доступа к сети Интернет на конкретных компьютерах принимается руководителем Учреждения на основании сведений, представленных руководителем структурного подразделения.

15.4. Почтовый обмен с сетью Интернет организуется через ограниченное количество точек, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям организации) почтовых серверов с безопасной системой репликации почтовых сообщений между ними.

15.5. Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных к сетям общего доступа и (или) международного обмена (сети Интернет и других), не допускается.

15.6. При работе в сетях общего доступа и (или) международного обмена соблюдаются следующие правила:

15.6.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) на элементах информационной системы проводится при служебной необходимости.

При работе в сети Интернет запрещается:

- осуществлять работу при отключенных средствах защиты;
- передавать по сети Интернет защищаемую информацию без использования средств шифрования;
- скачивать из сети Интернет программное обеспечение и другие файлы;
- посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО, сайты с подозрительным контентом и другие);
- нецелевое использование подключения к сети Интернет.

16. Антивирусная защита

16.1. Антивирусная защита направлена на предотвращение угроз, связанных с воздействием вредоносного программного кода.

16.2. Основные принципы антивирусной защиты:

- антивирусное программное обеспечение устанавливается, настраивается и активируется на всех серверах, рабочих станциях и локальных персональных компьютерах, используемых специалистами Учреждения.

- эксплуатация средств антивирусной защиты осуществляется только на основании лицензионных соглашений с их правообладателями.

- все возможные каналы поступления вредоносных программ в информационно-технологическую инфраструктуру Учреждения анализируются и защищаются средствами антивирусной защиты.

- контролю на предмет обнаружения вредоносных программ подвергается вся информация, создаваемая и обрабатываемая техническими средствами, а также принимаемая (передаваемая) посредством сменных носителей информации и средств телекоммуникаций.

- с целью эффективной борьбы с новыми видами вредоносных программ выполняется регулярное обновление всех средств антивирусной защиты.

Любые средства вычислительной техники, используемые в Учреждении, в ходе эксплуатации подвергаются непрерывному антивирусному мониторингу и сканированию.

17. Организация антивирусной защиты в Учреждении

17.1. Администрирование средств антивирусной защиты информационных систем персональных данных, конфигурирование и определение политик работы клиентских модулей, системный мониторинг возлагаются на техника-программиста Учреждения.

17.2. Действия пользователей по обеспечению антивирусной защиты при повседневной деятельности:

- обязательной антивирусной проверке подвергается любая информация, получаемая пользователем из сети Интернет посредством электронной почты, путем загрузки с веб-сайтов либо иным доступным способом.

- антивирусной проверке подвергаются все съемные носители информации (дискета, флеш-память, компакт-диск и пр.) перед подключением к персональному компьютеру.

- запрещается посещать сайты с потенциально опасным программным обеспечением (сайты с подозрительным контентом).

- запрещается открывать файлы, полученные по электронной почте от неизвестного отправителя или вызывающие подозрения.

- запрещается установка и запуск на рабочей станции программ и файлов, полученных из источников, не предусмотренных технологией обработки информации или не предназначенных для выполнения пользователем своих функциональных обязанностей.

- пользователям запрещается влиять на работоспособность средства антивирусной защиты (отключать антивирусную защиту, изменять параметры антивирусной защиты, изменять настройки межсетевых экранов и пр.).

О любых ошибках в работе средств антивирусной защиты следует немедленно сообщать технику – программисту Учреждения или в отдел развития информационных ресурсов департамента социальной защиты Воронежской области.

При получении от отдела развития информационных ресурсов Департамента сообщения о распространении вирусной эпидемии и инструкции по предотвращению, необходимо принять меры по выполнению требований инструкции, по недопущению заражения рабочей станции, проникновения вирусов в информационно-технологическую инфраструктуру Учреждения.

17.3. Действия пользователей при обнаружении вируса:

К основным признакам проявления вирусов относятся:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;

- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Вирус может быть обнаружен как при проверке полученного по электронной почте или иным способом подозрительного файла либо съемного машинного носителя информации на вирусы, так и при сканировании системы антивирусной программой в «прозрачном» для пользователя режиме. Предупреждения об обнаружении вируса отображаются в виде всплывающего окна.

При обнаружении или наличии подозрения на присутствие вирусного программного обеспечения на автоматизированном рабочем месте (персональном компьютере пользователя) пользователь обязан немедленно сообщить об этом технику-программисту Учреждения или в отдел развития информационных ресурсов департамента социальной защиты Воронежской области и прекратить работу на персональном компьютере.

Запрещается самостоятельное «лечение» зараженных файлов, персональных компьютеров, съемных носителей. Все необходимые антивирусные процедуры проводятся техником-программистом Учреждения или специалистами отдела развития информационных ресурсов департамента социальной защиты Воронежской области.

Запрещается перенос информации с помощью внешних носителей на другие компьютеры.

Запрещается запускать программы или открывать файлы, в которых был обнаружен вирус.

18. Учет носителей информации

18.1. В Учреждении организуется учет внешних носителей персональных данных (далее – защищаемые носители). Учет защищаемых носителей осуществляется специально уполномоченными из числа сотрудников лицами.

18.2. Учет всех защищаемых носителей информации производится с помощью их маркировки и занесения учетных данных в журнал учета внешних носителей персональных данных с отметкой об их движении (выдаче и возврате). С этой целью на защищаемых носителях персональных данных проставляются следующие реквизиты:

- регистрационный номер;
- дата и роспись уполномоченного лица.

Выдача защищаемых носителей персональных данных сотруднику производится под его личную роспись.

Листы журналов нумеруются, прошиваются и печатаются.

19. Порядок хранения электронных носителей персональных данных

19.1. Хранение документов и информационных ресурсов, содержащих персональные данные и иную конфиденциальную информацию, в электронном виде осуществляется только на предварительно учтенных машиночитаемых (электронных) носителях.

19.2. Носители информации с персональными данными хранятся в служебных помещениях, в надежно запираемых и опечатываемых шкафах (сейфах). При этом создаются надлежащие условия, обеспечивающие их физическую сохранность.

19.3. Запрещается выносить носители с персональными данными из служебных помещений без согласования с уполномоченным лицом.

19.4. Проверка наличия учитываемых носителей персональных данных проводится один раз в год лицами, ответственными за обеспечение безопасности персональных данных. В ходе ревизии может быть определен перечень носителей персональных данных, которые (или информация на которых) подлежат уничтожению.

19.5. Уничтожение носителей персональных данных (или информации на них), утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных журналах об этом делается отметка со ссылкой на соответствующий акт.

20. Резервирование информации

20.1. В целях обеспечения возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним, проводится резервирование (резервное копирование) персональных данных.

20.2. Резервирование должно осуществляться на различные защищаемые носители информации с соответствующим уровнем надежности и долговечности.

20.3. Хранение резервных копий осуществляется в надежных сейфах (металлических шкафах) и в серверных помещениях.

20.4. Доступ к резервным копиям строго регламентируется.

20.5. Правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных устанавливают должностные лица Учреждения, ответственные за обеспечение безопасности персональных данных при обработке в информационных системах.

20.6. Контроль над процессом осуществления резервного копирования объектов защиты возлагается на должностных лиц, ответственных за обеспечение безопасности персональных данных при обработке в информационных системах.

21. Порядок уничтожения персональных данных по достижении цели обработки

21.1. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено служебным контрактом, договором или соглашением, стороной которого является субъект персональных данных, либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

21.2. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено служебным контрактом, договором или соглашением, стороной которого является субъект персональных данных, либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

21.3. Уничтожение носителей персональных данных, утративших свое практическое значение и не подлежащих архивному хранению, производится на основании акта уничтожения, утверждаемого руководителем Учреждения.

21.4. Решение об удалении (стирании) записей, содержащих персональные данные, в электронных базах данных принимается сотрудниками, допущенными к обработке персональных данных самостоятельно в срок, не превышающий тридцати дней по достижении целей обработки или с момента утраты необходимости в достижении этих целей.

21.5. Сведения, содержащие персональные данные, и относимые к архивным документам, образующимся в процессе деятельности Учреждения, включаются в состав электронных архивов и хранятся согласно установленным законодательством срокам отдельно от баз данных информационных систем Учреждения.

22. Контроль состояния обеспечения безопасности персональных данных в Учреждении

22.1. Основными целями контроля состояния обеспечения безопасности персональных данных являются:

- установление степени соответствия принятых мер по обеспечению безопасности персональных данных требованиям законодательных и иных нормативных актов, норм, правил и инструкций по обеспечению безопасности персональных данных;
- выявление потенциальных каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на нее, выработка рекомендаций по их закрытию.

22.2. Основными задачами контроля являются:

- оценка эффективности проводимых мер по обеспечению безопасности персональных данных;
- анализ причин выявленных нарушений и недостатков в организации и обеспечении безопасности персональных данных, выработка рекомендаций по их устранению;
- оценка и анализ возможностей злоумышленника по добыванию персональных данных, выявление каналов утечки информации, каналов несанкционированного доступа к информации и специальных воздействий на нее, выработка рекомендаций по закрытию этих каналов.

22.3. Контроль заключается в проверке выполнения законодательства Российской Федерации по вопросам защиты персональных данных, а также в оценке обоснованности и эффективности принятых мер защиты.

22.4. Организационный контроль состояния обеспечения безопасности персональных данных в Учреждении проводится в форме внутренних проверок обеспечения безопасности персональных данных. Организационный контроль проводится совместно с сотрудниками структурных подразделений, ответственными за вопросы обеспечения безопасности информации своих подразделений.

22.5. Технический контроль состояния обеспечения безопасности персональных данных проводится в целях контроля функционирования системы защиты персональных данных, контроля установленных правил (политик) безопасности, конфигурационных настроек средств защиты информации, входящих в состав системы защиты персональных данных. Организация и проведение технического контроля состояния обеспечения безопасности персональных данных возлагается на лиц, ответственных за обеспечение безопасности персональных данных.

22.6. К техническому контролю состояния обеспечения безопасности персональных данных могут привлекаться специализированные организации, имеющие оформленные в установленном порядке лицензии на осуществление деятельности по технической защите конфиденциальной информации, оказывающие услуги по контролю (аудиту) состояния обеспечения безопасности персональных данных.

22.7. Непосредственный контроль за выполнением требований законодательства РФ по защите персональных данных при обработке персональных данных осуществляют лица, ответственные за обеспечение безопасности персональных данных.

23. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в Учреждении проводятся периодические проверки условий обработки персональных данных. Проверки осуществляются лицами, ответственными за обеспечение безопасности персональных данных, комиссией Учреждения.

Проверки осуществляются на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

Контролируемые вопросы в ходе проведения проверок:

- наличие у сотрудников допуска к обработке персональных данных;
- наличие согласий субъектов на обработку их персональных данных;
- соблюдение целей, состава и сроков обработки персональных данных;
- соблюдение правил по обезличиванию персональных данных;
- соблюдение правил доступа в помещения, в которых ведется обработка персональных данных;
- соответствие полномочий сотрудников разрешительной системе доступа к информационным ресурсам, программным и техническим средствам информационной системы персональных данных;
- соблюдение сотрудниками парольной политики;
- соблюдение сотрудниками антивирусной политики;
- соблюдение сотрудниками правил работы со съемными носителями персональных данных;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- соблюдение порядка работы со средствами защиты информации.

По итогам каждой проверки составляется протокол, который утверждается руководителем Учреждения и хранится у ответственного секретаря комиссии Учреждения в течение трех лет. Форма протокола приведена в приложении 4 к настоящему Положению.

При выявлении в ходе проверки нарушений в протоколе указываются мероприятия по устранению нарушений и сроки исполнения. Информация о результатах проверки и мерах, необходимых для устранения выявленных нарушений, докладывается руководителю Учреждения.

24. Реагирование на инциденты нарушения информационной безопасности и сбои

Реагирование на инциденты нарушения информационной безопасности и сбои направлено на сведение к минимуму ущерба от инцидентов, а также осуществление мониторинга случаев инцидентов.

Инцидент – любое непредвиденное или нежелательное событие, которое может нарушать деятельность или информационную безопасность.

К инцидентам информационной безопасности относятся:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политик или рекомендаций;
- нарушение физических защитных мер;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Реагирование на инциденты нарушения информационной безопасности включает в себя:

- разбирательство и составление заключений по фактам несоблюдения условий хранения 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.

Все сотрудники немедленно сообщают о любых наблюдаемых или предполагаемых инцидентах нарушения информационной безопасности своему непосредственному руководителю и должностному лицу, ответственному за информационную безопасность.

24.1. Информирование об инцидентах нарушения информационной безопасности

Все сотрудники незамедлительно информируют руководителя структурного подразделения и должностное лицо, ответственное за информационную безопасность, об инцидентах нарушения информационной безопасности.

В случае выявления фактов распространения персональных данных или утраты материальных носителей персональных данных руководитель Учреждения принимает решение о проведении служебной проверки.

Комиссия Учреждения осуществляет мониторинг и анализ инцидентов в целях выявления существенных инцидентов нарушения информационной безопасности, новых уязвимостей, проверки эффективности политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушения информационной безопасности.

24.2. Информирование о проблемах безопасности

Все сотрудники, осуществляющие обработку персональных данных, должны обращать внимание и сообщать руководителю структурного подразделения и должностному лицу, ответственному за информационную безопасность, о любых замеченных или предполагаемых недостатках и угрозах в области безопасности персональных данных, в том числе в информационных системах персональных данных. При этом не допускается самостоятельный поиск сотрудниками подтверждения подозреваемого недостатка в системе безопасности. Это требование предъявляется в интересах самих сотрудников, поскольку тестирование слабых мест защиты может быть интерпретировано как неправомерное использование системы.

24.3. Информирование о сбоях программного обеспечения

Сотрудники, осуществляющие обработку персональных данных с использованием средств вычислительной техники, обязаны соблюдать следующий порядок действий в случаях сбоев используемого программного обеспечения:

- симптомы проблемы (сбоя) и любые сообщения, появляющиеся на экране, фиксируются (распечатываются, переписываются, сохраняются в электронном виде);
- компьютер изолируется (отключается от локальной вычислительной сети учреждения при наличии), работа на нем прекращается;
- не допускается перенос информации с помощью внешних носителей на другие компьютеры;
- о проблеме немедленно извещается руководитель структурного подразделения и должностное лицо, ответственное за информационную безопасность.

Пользователям запрещается пытаться самостоятельно удалить подозрительное программное обеспечение. Ликвидация последствий сбоев осуществляется техником-программистом или специалистами отдела развития информационных ресурсов департамента.

24.4. Реагирование на факты разглашения персональных данных

По каждому факту разглашения персональных данных или утраты материальных носителей персональных данных руководитель Учреждения принимает решение о проведении служебной проверки.

По факту утечки сведений из информационных систем персональных данных в состав комиссии, проводящей служебную проверку, обязательно включается представитель отдела развития информационных ресурсов департамента социальной защиты Воронежской области.

25. Ответственность за разглашение персональных данных

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

Ответственность за обеспечение требований по защите персональных данных и иной конфиденциальной информации возлагается на руководителя Учреждения.

Персональная ответственность – одно из главных требований по организации и проведению работ по обеспечению безопасности персональных данных и обязательное условие обеспечения эффективности этих работ.

Ответственность за утрату документов или машиночитаемых носителей с конфиденциальной информацией или разглашение сведений, содержащихся в них, персонально несет работник, допустивший утрату, разглашение.

Ответственность за несанкционированный доступ к персональным данным и иной конфиденциальной информации, совершение нерегламентированных действий с персональными данными, повлекшими их уничтожение, распространение, изменение, несет персонально лицо, совершившее эти действия.

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

**Согласие
субъекта на обработку его персональных данных в связи с поступлением на работу в казенное учреждение Воронежской области «Нижедевицкий социально-реабилитационный центр для несовершеннолетних»**

Я, _____
(фамилия, имя, отчество)

(адрес)

(паспорт: серия, номер, дата выдачи, кем выдан)

в соответствии со статьями 86, 88 Трудового кодекса Российской Федерации, статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие казенному учреждению Воронежской области «Нижедевицкий социально – реабилитационный центр для несовершеннолетних» (далее - оператор), находящемуся по адресу: 396870, Воронежская область, Нижедевицкий район, село Нижедевицк, ул. Юбилейная, д.21б, на обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (УФНС, ПФР, ФСС и т.д.), обезличивание, блокирование, уничтожение) моих персональных данных, в составе: фамилия, имя, отчество; число, месяц, год рождения; место рождения; гражданство; образование; владение иностранными языками; судимость; допуск к государственной тайне; выполняемая работа с начала трудовой деятельности; награды и знаки отличия; близкие родственники (степень родства, ФИО, год, число, месяц и место рождения, место работы, домашний адрес); пребывание за границей; отношение к воинской обязанности, воинское звание; домашний адрес (адрес регистрации, фактического проживания); номер телефона; документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан); наличие заграничного паспорта (серия, номер, кем и когда выдан) номер страхового свидетельства обязательного пенсионного страхования; ИНН.

Обработка моих персональных данных может осуществляться с использованием средств автоматизации и без использования таковых исключительно в целях реализации трудовых отношений.

Согласие вступает в силу с момента его подписания.

Оператор может осуществлять обработку моих персональных данных в течение срока действия трудового договора и в течение 75 (семидесяти пяти) лет после его прекращения.

Я вправе отозвать свое согласие на обработку персональных данных посредством письменного заявления.

Дата начала обработки персональных данных: _____
(число, месяц, год)

(подпись)

(расшифровка подписи)

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных граждан

Я, _____,
(ФИО сотрудника)
исполняющий (ая) должностные обязанности _____,

(наименование должности и подразделения)

обязуюсь:

1. Не разглашать, не раскрывать публично, а также соблюдать установленный порядок передачи третьим лицам сведений, составляющих персональные данные граждан, которые мне будут доверены или станут известны в связи с исполнением своих должностных обязанностей.
2. Выполнять относящиеся ко мне требования положения по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, приказов, распоряжений, инструкций и других нормативных актов по обеспечению безопасности персональных данных.
3. В случае моего увольнения, все носители, содержащие персональные данные граждан, которые находились в моем распоряжении в связи с исполнением мною должностных обязанностей, передать непосредственному начальнику или сотруднику, определенному непосредственным начальником.
4. Немедленно сообщать непосредственному начальнику об утрате или недостатке документов или иных носителей, содержащих персональные данные граждан, и о других фактах, которые могут привести к разглашению персональных данных граждан, а также о причинах и условиях возможной утечки персональных данных.
5. После прекращения права на допуск к конфиденциальным сведениям, в том числе расторжения служебного контракта, прекратить обработку персональных данных, не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Об ответственности за разглашение персональных данных граждан предупрежден(а).

(подпись)

(расшифровка подписи)

« ___ » _____ 20__ г.

Протокол
проведения проверки условий обработки персональных данных в КУ ВО «Нижедевицкий
социально – реабилитационный центр для несовершеннолетних»

Настоящий Протокол составлен в том, что «___» _____ 20__ года комиссией КУ ВО «Нижеде-
вицкий СРЦДН» по обеспечению безопасности персональных данных проведена проверка _____

(тема проверки)

Проверка осуществлялась в соответствии с требованиями _____

(название документа)

Проверено: _____

Выявленные нарушения: _____

Меры по устранению нарушений: _____

Срок устранения нарушений: _____

Председатель комиссии:

(должность)

(подпись)

(Ф.И.О.)

Члены комиссии:

(должность)

(подпись)

(Ф.И.О.)

(должность)

(подпись)

(Ф.И.О.)

(должность)

(подпись)

(Ф.И.О.)

(должность)

(подпись)

(Ф.И.О.)

(должность)

(подпись)

(Ф.И.О.)

(должность)

(подпись)

(Ф.И.О.)

**Разъяснение
субъекту персональных данных юридических последствий отказа предоставить
свои персональные данные**

Уважаемый (ая) _____!
Ф.И.О субъекта персональных данных

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152 «О персональных данных» (в ред. Федерального закона от 25.07.2011), а именно со ст.6, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну оператору КУ ВО «Нижедевицкий социально – реабилитационный центр для несовершеннолетних» (юридический адрес: 396870, Воронежская область, Нижедевицкий район, село Нижедевицк, ул. Юбилейная, д.21б) необходимо получить согласие на обработку Ваших персональных данных.

Форма согласия устанавливается в п.4 ст.9 Федерального закона от 27 июля 2006 года № 152 «О персональных данных» и включает в себя:

- 1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- 2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- 3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- 4) цель обработки персональных данных;
- 5) перечень персональных данных, на обработку которых даётся согласие субъекта персональных данных;
- 6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- 7) перечень действий с персональными данными, на совершение которых даётся согласие, общее описание используемых оператором способов обработки персональных данных;
- 8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- 9) подпись субъекта персональных данных.

Ваши персональные данные используются оператором с целью обработки (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу, обезличивание, блокирование, уничтожение) во исполнение действующего законодательства в сфере защиты прав и законных интересов субъектов персональных данных.

Ваши персональные данные используются и передаются в организации, сотрудничающие с КУ ВО «Нижедевицкий СРЦДН» в рамках исполнения действующего законодательства в сфере защиты прав и законных интересов субъектов персональных данных.

Лист согласия заполняется собственноручно субъектом персональных данных.

В случае Вашего отказа оператор не сможет совершать любые действия, связанные с обработкой Ваших персональных данных, в связи с чем Вам может быть отказано в услугах, требующих такой обработки.

Разрешение будет храниться в КУ ВО «Нижедевицкий социально – реабилитационный центр для несовершеннолетних» (юридический адрес: 396870, Воронежская область, Нижедевицкий район, село Нижедевицк, ул. Юбилейная, д.21б), его содержание будет недоступно другим, поэтому распространяться оно будет только на деятельность по обработке персональных данных, осуществляемую КУ ВО «Нижедевицкий СРЦДН». Любой другой оператор персональных данных должен будет независимо получать от Вас разрешение на обработку ваших персональных данных.

Принимая решение, не забывайте, что в любой момент на основании того же закона Вы можете изменить своё решение.

Директор КУ ВО «Нижедевицкий СРЦДН»

Р.М. Манаенкова

« ___ » _____ 20__ года

ПОЛОЖЕНИЕ

об организации учета, обработки, использования, хранения и защиты персональных данных несовершеннолетних, проходящих курс социальной реабилитации и (или) находящихся на патронатном сопровождении в КУ ВО «Нижедевицкий социально-реабилитационный центр для несовершеннолетних», и их родителей (законных представителей)

1. Общие положения.

1.1. Положение об организации учета, обработки, использования, хранения и защиты персональных данных (далее – Положение) несовершеннолетних, проходящих курс социальной реабилитации и (или) находящихся на патронатном сопровождении, и их родителей (законных представителей) (далее – субъектов) в КУ ВО «Нижедевицкий социально-реабилитационный центр для несовершеннолетних» (далее - Учреждение) разработано в соответствии со статьей 24 Конституции Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», ст. 87 Трудового Кодекса Российской Федерации, Уставом Учреждения.

1.2. Настоящее Положение определяет понятия, общие требования, порядок и организацию учета, обработки, использования, хранения и защиты персональных данных субъектов.

1.3. Целью учета и использования персональных данных является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2. Основные понятия и процедуры, общие требования к организации учета, обработки, хранения и защиты персональных данных

2.1. В настоящем Положении используются следующие основные понятия:

2.1.1. Персональные данные – любая информация, относящаяся к субъекту персональных данных (физическому лицу), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Персональные данные несовершеннолетнего (ребенка), его родителей (законных представителей) – информация, необходимая Учреждению в связи с отношениями, возникающими между ребенком, его родителями (законными представителями) и Учреждением.

2.1.2. Оператор – лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

2.1.3. 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.

2.1.4. Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц или на ознакомление с персональными данными ограниченного круга лиц.

2.1.5. Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных либо иным образом затрагивающих права и свободы субъекта персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с действующим законодательством не распространяется требование соблюдения конфиденциальности.

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

2.1.7. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2.1.8. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

2.1.9. Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных работников, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

2.1.10. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

2.2. В целях обеспечения прав и свобод человека и гражданина при получении и обработке персональных данных субъекта в Учреждении должны соблюдаться следующие требования:

2.2.1. Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки.

2.2.2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

2.2.3. Учет и обработка персональных данных должны осуществляться оператором с письменного согласия субъекта персональных данных в соответствии со статьей 24 Конституции Российской Федерации: для детей в возрасте до 14 лет согласие дают родители (законные представители), с 14 лет – личное согласие дают сами несовершеннолетние. Кроме того, родители (законные представители) дают согласие на обработку личных персональных данных.

2.2.4. Согласие субъекта персональных данных на учет и обработку персональных данных не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании действующего законодательства; в целях исполнения договора, одной из сторон которого является субъект персональных данных; для защиты жизни, здоровья и иных жизненно важных интересов субъекта персональных данных.

2.2.5. Оператором или иным лицом, получающим доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

2.2.6. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных, в отношении общедоступных персональных данных (фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии).

2.2.7. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе.

2.2.8. Субъект персональных данных в обязательном порядке предоставляет свои персональные данные, предусмотренных действующим законодательством, в целях защиты основ нравственности, здоровья, прав и законных интересов других лиц, обеспечения безопасности:

- фамилию, имя, отчество, адрес, данные основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилия, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- перечень персональных данных и действий с ними, на обработку которых дает согласие субъект персональных данных.

2.2.9. Субъекты персональных не должны отказываться от своих прав на сохранение и защиту тайны своих персональных данных.

2.2.10. Защита персональных данных субъекта от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет собственных средств в порядке, установленном действующим законодательством.

3. Основные условия проведения обработки персональных данных.

3.1. Учреждение определяет объем, содержание обрабатываемых персональных данных детей, их родителей (законных представителей), руководствуясь действующим законодательством.

3.2. К персональным данным детей, их родителей (законных представителей), получаемым Учреждением и подлежащим хранению в Учреждении в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения:

- 3.2.1. фамилия, имя, отчество;
- 3.2.2. образование родителей (законных представителей);
- 3.2.3. место регистрации и место фактического проживания;
- 3.2.4. номер домашнего и мобильного телефонов родителей (законных представителей);
- 3.2.5. место работы, занимаемая должность родителей (законных представителей);
- 3.2.6. номер служебного телефона родителей (законных представителей);
- 3.2.7. данные паспорта родителей (законных представителей);
- 3.2.8. реквизиты лицевого банковского счета родителей (законных представителей);
- 3.2.9. сведения о близких родственниках;
- 3.2.10. данные свидетельства о рождении ребенка;
- 3.2.11. номер полиса обязательного медицинского страхования ребенка;
- 3.2.12. сведения о состоянии здоровья ребенка;
- 3.2.13. биометрические данные (фотографическая карточка);
- 3.2.14. документы, подтверждающие права на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным действующим законодательством;
- 3.2.15. дополнительные данные, сообщаемые в заявлении о приеме ребенка.

Все персональные данные ребенка предоставляются его родителями (законными представителями).

3.3. Обработка персональных данных детей, их родителей (законных представителей) осуществляется в целях обеспечения соблюдения законодательных и нормативных актов, содействия в успешной социальной реабилитации детей, обеспечения их личной безопасности, контроля качества оказания социальных услуг и обеспечения сохранности имущества.

3.4. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных действующим законодательством.

3.5. Субъекты персональных данных и их представители должны быть ознакомлены под расписку с документами Учреждения, устанавливающими порядок обработки персональных данных субъекта, а также об их правах и обязанностях в этой области.

4. Хранение и использование персональных данных.

4.1. Персональные данные субъектов хранятся на бумажных и электронных носителях в специально предназначенных для этого помещениях Учреждения.

4.2. В процессе хранения персональных данных субъектов должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;
- сохранность имеющихся персональных данных, ограничение доступа к ним в соответствии с действующим законодательством и настоящим Положением;
- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

4.3. Доступ к персональным данным детей, их родителей (законных представителей) имеют:

- директор учреждения;
- заместитель директора по воспитательной и реабилитационной работе;
- заведующий отделением;
- социальный педагог;
- специалист по социальной работе;
- воспитатели;
- педагог-психолог;
- медицинский персонал.

4.4. Доступ к персональным данным субъектов могут иметь иные работники, определяемые приказом руководителя Учреждением, в пределах своей компетенции.

4.6. Помимо лиц, указанных в пунктах 4.3, 4.4 настоящего Положения, право доступа к персональным данным субъектов имеют только лица, уполномоченные действующим законодательством.

4.7. Лица, имеющие доступ к персональным данным, обязаны использовать персональные данные субъектов лишь в целях, для которых они предоставлены.

4.8. Ответственными за организацию и осуществление хранения персональных данных субъектов являются работники, определенные приказом руководителя Учреждением.

4.9. Персональные данные ребенка отражаются в его личном деле, медицинской карте и др. документах, формирующихся в процессе социальной реабилитации и патронатного сопровождения ребенка. Личные дела детей хранятся в кабинете специалистов в специально оборудованных шкафах по алфавиту. Медицинские карты детей хранятся в специально оборудованных шкафах в медицинском кабинете по алфавиту.

4.10. Персональные данные родителей (законных представителей) отражаются в заявлении о приеме ребенка в Учреждение и (или) договоре с Учреждением. Указанные документы (заявления и (или) договоры) хранятся в специально оборудованных шкафах в кабинете специалистов.

5. Передача персональных данных.

5.1. При передаче персональных данных субъектов другим юридическим и физическим лицам Учреждение должно соблюдать следующие требования:

5.1.1. Персональные данные субъекта не могут быть сообщены третьей стороне без письменного согласия родителей (законных представителей) ребенка, за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью ребенка, а также в случаях, установленных действующим законодательством.

5.1.2. Лица, получающие персональные данные субъектов должны предупреждаться о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Учреждение вправе требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъектов, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными субъектов в порядке, установленном действующим законодательством.

5.1.3. Передача персональных данных субъекта его представителям может быть осуществлена в установленном действующим законодательством порядке только в том объеме, который необходим для выполнения указанными представителями их функций.

6. Обязанности и права субъектов персональных данных.

6.1. В целях обеспечения достоверности персональных данных родители (законные представители) обязаны:

6.1.1. При приеме детей в Учреждение представлять уполномоченным работникам достоверные сведения о себе, своих детях.

6.1.2. В случае изменения сведений, составляющих персональные данные ребенка или своих, обязаны в течение 10 дней сообщить об этом руководителю Учреждения.

6.2. Родители (законные представители) ребенка имеют следующие права:

6.2.1. Получать полную информацию о своих персональных данных и их обработке.

6.2.2. Получать сведения об операторе, месте его нахождения, о наличии у оператора персональных данных, знакомиться с этими персональными данными, за исключением случаев, предусмотренных частью 5 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

6.2.3. Требовать от оператора уточнения своих данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными или не являются необходимыми для заявленной цели обработки. Указанное требование должно быть оформлено письменным заявлением родителя (законного представителя) на имя директора Учреждения.

6.2.4. Защищать свои права и законные интересы, обжаловать в суде любые неправомерные действия или бездействия Учреждения при обработке и защите его персональных данных.

6.3. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

6.3.1. Обработка персональных данных осуществляется в целях безопасности.

6.3.2. Предоставление персональных данных нарушает конституционные права и свободы других лиц.

7. Обязанности и права оператора.

7.1. Оператор при сборе персональных данных обязан:

7.1.1. Предоставить субъекту персональных данных следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора;

- цель обработки персональных данных и ее правовое основание;

- предполагаемые пользователи персональных данных;

- установленные действующим законодательством права субъекта персональных данных.

7.1.2. Разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

7.1.3. Предоставить субъекту персональных данных по его просьбе информацию о персональных данных в соответствии с частью 4 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», а также внести в них необходимые изменения, уничтожить или заблокировать соответствующие персональные данные в случае, если эти данные являются неполными, устаревшими, недостоверными или не являются необходимыми для заявленной цели обработки.

7.1.4. Принимать необходимые организационные и технические меры, в том числе использовать шифровальные средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

7.1.5. Предупредить лиц, получающих персональные данные субъекта, 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 будет соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим секретности (конфиденциальности).

7.1.6. Разрешить доступ к персональным данным субъекта только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций.

7.2. Оператор имеет право:

7.2.1. Осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных в следующих случаях:

- оператора и субъекта персональных данных связывают трудовые отношения;

- оператора и субъекта персональных данных связывает заключение договора для достижения целей, предусмотренных Уставом Учреждения;

- персональные данные являются общедоступными;

- персональные данные включают в себя только фамилии, имена и отчества субъектов персональных данных;

- персональные данные, обрабатываемые без использования средств автоматизации в соответствии с федеральными законами, нормативными актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

7.3. Оператор не имеет права:

7.3.1. Сообщать персональные данные работника третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных действующим законодательством.

7.3.2. Сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

7.3.4. Запрашивать письменную информацию о состоянии здоровья субъекта персональных данных, за исключением тех сведений, которые относятся к вопросу о возможности выполнения субъектом трудовой функции.

8. Ответственность субъектов персональных данных.

8.1. Субъект персональных данных несет ответственность за:

8.1.1. Предоставление недостоверных и (или) неполных персональных данных (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, другая информация).

8.1.2. Несвоевременность предоставления своих персональных данных.

8.1.3. Нарушение конфиденциальности и использование персональных данных в целях, не предусмотренных для их распространения другим лицам.

8.2. Субъект персональных данных, виновный в нарушении Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», несет гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную действующим законодательством ответственность.

9. Ответственность оператора.

9.1. Оператор несет ответственность за:

9.1.1. Учет, обработку, использование, хранение и защиту персональных данных, не соответствующих требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Устава и локальных актов Учреждения.

9.1.2. Недостоверность персональных данных, несвоевременность их обработки и передачи в соответствующие организации, учреждения для работы с ними.

9.1.3. Нарушение конфиденциальности и распространение персональных данных без согласия субъекта персональных данных или наличия иного законного основания.

9.1.4. Использование персональных данных в целях, не предусмотренных для их распространения другим лицам.

9.2. Оператор, виновный в нарушении Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», несет гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную действующим законодательством ответственность.

10. Заключительные положения.

10.1. Настоящее Положение вступает в действие с момента утверждения и издания приказа директора Учреждения.

10.2. Изменения и дополнения вносятся в настоящее Положение по мере необходимости и подлежат утверждению директором Учреждения.

СОГЛАСИЕ
несовершеннолетнего на обработку персональных данных
(при достижении возраста 14 лет)

Я _____,
зарегистрированный (ая) по адресу: _____,
фактически проживающий (ая) по адресу: _____,
паспорт: _____, выдан _____,
серия и номер _____ дата и наименование выдавшего органа _____

в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» даю своё согласие на обработку казенным учреждением Воронежской области «Нижедевицкий социально – реабилитационный центр для несовершеннолетних» (далее – Оператор) моих персональных данных, включающих: фамилию, имя, отчество, пол, дату рождения, адрес места жительства, контактный (е) телефон (ы), реквизиты полиса ОМС (ДМС), данные о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью (в медико - профилактических целях) в целях установления медицинского диагноза и оказания медицинских услуг, а также других персональных данных в целях оказания мне комплексной социальной помощи в виде государственных социальных услуг при условии, что их обработка осуществляется лицом, действующим в рамках соблюдения моих законных прав и интересов, в том числе профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

В процессе оказания Оператором мне комплексной социальной, в том числе медицинской, помощи в виде государственных социальных услуг я предоставляю право специалистам учреждения, в том числе медицинским работникам, передавать мои персональные данные, содержащие сведения, составляющие врачебную и иную тайну, другим должностным лицам Оператора, а также иным учреждениям в сфере защиты законных прав и интересов ребенка, в том числе учреждениям социального обслуживания населения, учреждениям здравоохранения в системе ОМС РФ и др., в рамках соблюдения моих законных прав и интересов, в том числе медицинского обследования и лечения.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными в соответствии с федеральным законодательством. Оператор вправе обрабатывать мои персональные данные как посредством автоматизации путем внесения их в электронную базу данных, включая в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов), так и без использования автоматизированных средств.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов (медицинской карты) и составляет *двадцать пять лет*.

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной «_____» _____ 20__ года, вступает в силу со дня его подписания и действует в течение всего срока обработки персональных данных до момента достижения цели обработки персональных данных или прекращения обязательств по заключённым договорам и соглашениям или исходя из документов Оператора, регламентирующих вопросы обработки персональных данных.

Я оставляю за собой право отозвать своё согласие посредством составления соответствующего письменного документа, который должен быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

С нормативно-правовой документацией КУ ВО «Нижедевицкий СРЦдН», определяющей политику Оператора в области персональных данных, в том числе с Положением об организации учета, обработки, использования, хранения и защиты персональных данных несовершеннолетних, проходящих курс социальной реабилитации и (или) находящихся на патронатном сопровождении в КУ ВО «Нижедевицкий социально-реабилитационный центр для несовершеннолетних», и их родителей (законных представителей) ознакомлен (а).

Контактный (е) телефон (ы): _____

Подпись субъекта персональных данных _____
подпись

расшифровка подписи

СОГЛАСИЕ
родителя (законного представителя) на обработку персональных данных несовершеннолетнего
(до достижения совершеннолетним возраста 14 лет)

Я _____,
зарегистрированный (ая) по адресу: _____,
фактически проживающий (ая) по адресу: _____,
паспорт: _____, выдан _____,
серия и номер _____ дата и наименование выдавшего органа _____

в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» даю своё согласие на обработку казенным учреждением Воронежской области «Нижедевицкий социально – реабилитационный центр для несовершеннолетних» (далее – Оператор) персональных данных моего ребенка _____,

включающих: фамилию, имя, отчество, пол, дату рождения, адрес места жительства, контактный (е) телефон (ы), реквизиты полиса ОМС (ДМС), данные о состоянии здоровья моего ребенка, заболеваниях, случаях обращения за медицинской помощью (в медико - профилактических целях) в целях установления медицинского диагноза и оказания медицинских услуг, а также других персональных данных в целях оказания моему ребенку комплексной социальной помощи в виде государственных социальных услуг при условии, что их обработка осуществляется лицом, действующим в рамках соблюдения законных прав и интересов моего ребенка, в том числе профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

В процессе оказания Оператором моему ребенку комплексной социальной, в том числе медицинской, помощи в виде государственных социальных услуг я предоставляю право специалистам учреждения, в том числе медицинским работникам, передавать персональные данные моего ребенка, содержащие сведения, составляющие врачебную и иную тайну, другим должностным лицам Оператора, а также иным учреждениям в сфере защиты законных прав и интересов ребенка, в том числе учреждениям социального обслуживания населения, учреждениям здравоохранения в системе ОМС РФ и др., в рамках соблюдения законных прав и интересов моего ребенка, в том числе медицинского обследования и лечения.

Настоящее согласие предоставляется на осуществление любых действий в отношении персональных данных моего ребенка, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение, трансграничную передачу персональных данных, а также осуществление любых иных действий с персональными данными моего ребенка в соответствии с федеральным законодательством. Оператор вправе обрабатывать персональные данные моего ребенка как посредством автоматизации путем внесения их в электронную базу данных, включая в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов), так и без использования автоматизированных средств. Срок хранения персональных данных моего ребенка соответствует сроку хранения первичных медицинских документов (медицинской карты) и составляет *двадцать пять лет*. Передача персональных данных моего ребенка иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной «_____» _____ 20__ года, вступает в силу со дня его подписания и действует в течение всего срока обработки персональных данных моего ребенка до момента достижения цели обработки персональных данных или прекращения обязательств по заключённым договорам и соглашениям или исходя из документов Оператора, регламентирующих вопросы обработки персональных данных.

Я оставляю за собой право отозвать своё согласие посредством составления соответствующего письменного документа, который должен быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

С нормативно-правовой документацией КУ ВО «Нижедевицкий СРЦдН», определяющей политику Оператора в области персональных данных, в том числе с Положением об организации учета, обработки, использования, хранения и защиты персональных данных несовершеннолетних, проходящих курс социальной реабилитации и (или) находящихся на патронажном сопровождении в КУ ВО «Нижедевицкий социально-реабилитационный центр для несовершеннолетних», и их родителей (законных представителей) ознакомлен (а).

Контактный (е) телефон (ы): _____

Подпись субъекта персональных данных _____
подпись

расшифровка подписи

СОГЛАСИЕ
родителя (законного представителя) на обработку
личных персональных данных

Я _____,
зарегистрированный (ая) по адресу: _____,
фактически проживающий (ая) по адресу: _____,
паспорт: _____, выдан _____,
серия и номер _____ дата и наименование выдавшего органа _____

в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» даю своё согласие на обработку казенным учреждением Воронежской области «Нижедевицкий социально – реабилитационный центр для несовершеннолетних» (далее – Оператор) моих персональных данных, включающих: фамилию, имя, отчество, пол, дату рождения, адрес места жительства, контактный (е) телефон (ы), реквизиты полиса ОМС (ДМС), данные о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью (в медико - профилактических целях) в целях установления медицинского диагноза и оказания медицинских услуг, а также других персональных данных в целях оказания мне комплексной социальной помощи в виде государственных социальных услуг при условии, что их обработка осуществляется лицом, действующим в рамках соблюдения моих законных прав и интересов, в том числе профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

В процессе оказания Оператором мне комплексной социальной, в том числе медицинской, помощи в виде государственных социальных услуг я предоставляю право специалистам учреждения, в том числе медицинским работникам, передавать мои персональные данные, содержащие сведения, составляющие врачебную и иную тайну, другим должностным лицам Оператора, а также иным учреждениям в сфере защиты законных прав и интересов ребенка, в том числе учреждениям социального обслуживания населения, учреждениям здравоохранения в системе ОМС РФ и др., в рамках соблюдения моих законных прав и интересов, в том числе медицинского обследования и лечения.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными в соответствии с федеральным законодательством. Оператор вправе обрабатывать мои персональные данные как посредством автоматизации путем внесения их в электронную базу данных, включая в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов), так и без использования автоматизированных средств.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов (медицинской карты) и составляет *двадцать пять лет*.

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной «___» _____ 20__ года, вступает в силу со дня его подписания и действует в течение всего срока обработки персональных данных до момента достижения цели обработки персональных данных или прекращения обязательств по заключённым договорам и соглашениям или исходя из документов Оператора, регламентирующих вопросы обработки персональных данных.

Я оставляю за собой право отозвать своё согласие посредством составления соответствующего письменного документа, который должен быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

С нормативно-правовой документацией КУ ВО «Нижедевицкий СРЦДН», определяющей политику Оператора в области персональных данных, в том числе с Положением об организации учета, обработки, использования, хранения и защиты персональных данных несовершеннолетних, проходящих курс социальной реабилитации и (или) находящихся на патронатном сопровождении в КУ ВО «Нижедевицкий социально-реабилитационный центр для несовершеннолетних», и их родителей (законных представителей) ознакомлен (а).

Контактный (е) телефон (ы): _____

Подпись субъекта персональных данных _____
подпись

_____ расшифровка подписи