Приложение № 2
к приказу № 50 от 19.09.2018г

ПОЛОЖЕНИЕ
об обработке персональных данных в ГБУСО «Социальный приют для детей и подростков Погарского района « Надежда»», осуществляемых с использованием средств автоматизации

1. Основные понятия

1.1. Положение об обработке персональных данных в ГБУСО «Социальный приют для детей и подростков Погарского района « Надежда»» с использованием средств автоматизации разработано в соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 27 июля 2004 года №79-ФЗ «О государственной гражданской службе Российской Федерации», Постановлением Правительства РФ от 17 ноября 2007 года №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Положение определяет порядок и условия обработки персональных данных в Приюте с использованием средств автоматизации.

1.3. Обработка персональных данных в приюте осуществляется в целях исполнения государственных функций по предоставлению гражданам государственных услуг в сфере социальной защиты населения в пределах своей компетенции, ведения кадрового и бухгалтерского учёта, обучения и должностного роста, обеспечения личной безопасности сотрудников и членов его семьи, учета результатов исполнения им должностных обязанностей, в целях обеспечения сохранности имущества приюта

1.4. Настоящее Положение утверждается директором приюта и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным субъектов персональных данных.

II. Порядок обработки персональных данных сотрудников приюта и иных лиц

2.1. Основные термины, используемые в настоящем положении.

Персональные данные (ПДн) — 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.

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

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.

Использование персональных данных — действия (операции) с персональными данными, совершаемые работодателем в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работника или других лиц, либо иным образом затрагивающих права и свободы работника или других лиц.

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

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.

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

Информационная система персональных данных (ИСПДн) — 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.

Конфиденциальность персональных данных — обязательное для соблюдения работодателем или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия работника или наличия иного законного основания.

Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на кото-

рые в соответствии с федеральными законами РФ не распространяется требование соблюдения конфиденциальности.

2.2. Обработка персональных данных сотрудников приюта или иных лиц (под иными лицами подразумеваются кандидаты на замещение вакантных должностей в приюте и граждане, обратившиеся за получением государственных услуг) в приют осуществляется с их письменного согласия.

2.3. Представитель нанимателя в лице руководителя (и.о руководителя) приюта, осуществляющего полномочия нанимателя от имени учредителя (далее - представитель нанимателя), а также ответственный за организацию обработки персональных данных - обеспечивают защиту персональных данных сотрудников, содержащихся в личных делах, от неправомерного их использования или утраты.

2.4. При обработке персональных данных сотрудников в целях реализации возложенных на приют полномочий уполномоченные должностные лица обязаны соблюдать следующие требования:

а) объем и характер обрабатываемых персональных данных, способы обработки персональных данных должны соответствовать целям обработки персональных данных;

б) защита персональных данных сотрудника от неправомерного их использования или уничтожения обеспечивается в порядке, установленном нормативными правовыми актами Российской Федерации;

в) передача персональных данных не допускается без письменного согласия субъекта персональных данных, за исключением случаев, установленных федеральными законами. В случае, если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение персональных данных, либо отсутствует письменное согласие субъекта персональных данных на передачу его персональных данных, приют вправе отказать в предоставлении персональных данных. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации;

г) обеспечение конфиденциальности персональных данных сотрудников, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

д) хранение персональных данных должно осуществляться в форме, позволяющей определить сотрудника и иное лицо, являющееся субъектом персональных данных, не дольше, чем этого требуют цели их обработки. Указанные сведения подлежат уничтожению по достижении цели обработки или в случае утраты необходимости в их достижении, если иное не установлено законодательством Российской Федерации. Факт уничтожения персональных данных оформляется соответствующим актом;

е) опубликование и распространение персональных данных допускается в случаях, установленных законодательством Российской Федерации.

2.5. Обработка биометрических и специальных категорий персональных данных, осуществляется с их письменного согласия, за исключением случаев, предусмотренных законодательством Российской Федерации в области персональных данных. Использование и хранение биометрических и специальных категорий персональных данных вне информационных систем персональных данных может осу-

ществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

2.6. В целях обеспечения защиты персональных данных субъекты персональных данных вправе:

а) получать полную информацию о своих персональных данных и способе обработки этих данных (в том числе автоматизированной);

б) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, за исключением случаев, предусмотренных Федеральным законом "О персональных данных";

в) требовать внесения необходимых изменений, уничтожения или блокирования соответствующих персональных данных, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

г) обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействие) уполномоченных должностных лиц.

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

3.1. Обработка персональных данных сотрудников приюта – смешанная,

3.1.1. Состав персональных данных ЦОД №1 :

- фамилия, имя, отчество;
- дата рождения;
- месяц рождения,
- год рождения;
- место рождения,
- адрес места жительства;
- образование;
- профессия;
- семейное положение;
- состояние здоровья;
-ИНН;
-СНИЛС;
- стаж работы,
-данные, удостоверяющие личность;
-документ, подтверждающий отсутствие (наличие) судимости;
-сведения о воинской обязанности и военной службе;
- гражданство;
-документ, дающий право на меры социальной поддержки
- сведения о месте учебы;
- данные водительского удостверения;

3.1.2. Состав персональных данных, содержащихся в 1-С « Бухгалтерия»:

Фамилия, имя, отчество, дата рождения, должность, паспортные данные, сумма заработка, сумма отчислений с заработной платы, ИНН, СНИЛС, количество иждивенцев

3.1.3 Состав персональных данных граждан, обратившихся за получением государственных услуг (ЦОД №3):

- фамилия, имя, отчество;
- дата рождения;
- месяц рождения,
- год рождения;
- место рождения,
- адрес места жительства;
- семейное положение;
- социальное положение;
- имущественное положение;
-образование;
-доходы;
-национальная принадлежность;
-состояние здоровья;
-СНИЛС;
-состав семьи;
-данные документа, удостоверяющего личность;
- гражданство;
-сведения о жилом помещении;
-сведения о номере лицевого счета кредитном учреждении;
-документ, дающий право на меры социальной поддержки;
- сведения о месте учебы;
- данные полиса ОМС;

3.2. Классификация вышеуказанных информационных систем персональных данных осуществляется в порядке, установленном законодательством Российской Федерации.

IV. Доступ к персональным данным

4.1. Общие положения

4.1.1. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

4.1.2. Уполномоченными должностными лицами при обработке персональных данных в информационных системах персональных данных должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

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

4.1.4. Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации, в том числе к информационно-телекоммуникационной сети Интернет, не допускается.

4.1.5. Доступ пользователей к персональным данным в информационных системах персональных данных в приюте должен требовать обязательного прохождения процедуры идентификации и аутентификации.

4.1.6. Структурными подразделениями (должностными лицами) приюта г. Сельцо, ответственными за обеспечение безопасности персональных данных при их обработке в информационных системах, должно быть обеспечено:

а) своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководства приюта;

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

в) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) постоянный контроль над обеспечением уровня защищенности персональных данных;

д) функционирование системы резервного копирования информационных систем;

е) знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

ж) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

з) при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;

и) 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.

4.1.7. В случае выявления нарушений порядка обработки персональных данных в информационных системах приюта г. Сельцо уполномоченными должност-

ными лицами принимаются меры по установлению причин нарушений и их устранению.

4.2. Внутренний доступ.

4.2.1.Перечень специалистов приюта, имеющих доступ к персональным данным субъектов персональных данных, определяется приказом директора приюта

Коды доступа и пароли на вход в информационную систему должны быть уникальны, являться конфиденциальной информацией и не подлежать разглашению.

4.2.2. Все персональные компьютеры (ПК), на которых производится обработка персональных данных, должны иметь систему парольной защиты от несанкционированного доступа, антивирусную защиту и быть оборудованы сертифицированными техническими средствами защиты персональных данных.

4.2.3 Подключения ПК, на которых производится обработка персональных данных, к сети Интернет утверждается директором приюта

4.2.4. Отключение ПК специалистов, на которых выполняется обработка персональных данных, от сети Интернет, производится приказом директора приюта

4.2.5. Персональные данные могут быть представлены для ознакомления:

а) сотрудникам, допущенным к обработке персональных данных с использованием средств автоматизации в части, касающейся исполнения их должностных обязанностей (в соответствии с Перечнем лиц, допущенных к обработке персональных данных, утвержденным приказом начальника управления);

б) уполномоченным работникам федеральных органов исполнительной власти в порядке, установленном законодательством Российской Федерации.

4.2.6. Лица, осуществляющие обработку персональных данных, несут персональную ответственность за неразглашение информации, полученной в процессе работы, за достоверность, полноту и целостность данных в информационных системах.

4.2.7. Перечень помещений в приюте, в которых обрабатываются персональные данные, определен приказом начальника управления. Указанные помещения в рабочее время при отсутствии в них ответственных сотрудников должны быть закрыты. Проведение уборки в этих помещениях должно производиться в присутствии соответствующих сотрудников.

4.2.8. Перечень мест хранения персональных данных (в том числе съёмных электронных носителей) определен приказом директора приюта. Места хранения должны быть доступны только кругу лиц, определенному Приказом о перечне лиц, допущенных к обработке персональных данных. Места хранения должны обеспечивать сохранность персональных данных.

4.3. Внешний доступ.

4.3.1 Приют в соответствии с действующим законодательством РФ имеет право передавать персональные данные сотрудников в следующие организации:

- Департамент семьи, социальной и демографической политики Брянской области
- территориальное отделение ФНС;
- Отделение Пенсионного Фонда России по Брянской области и (или) его подразделения;

- территориальное отделение Фонда обязательного медицинского страхования;
- Кредитные учреждения;
- Департамент финансов Брянской области

Персональные данные должны передаваться с соблюдением мер защиты персональных данных в соответствии с законодательством РФ, в минимально необходимых объемах для требуемых целей.

4.3.2. В случае необходимости передачи информации, содержащей персональные данные, в иные организации (учреждения) в целях предоставления государственных услуг и мер социальной поддержки граждан, Приют обязан заключить с организацией (учреждением) Договор (Соглашение) об информационном обмене, определяющий цель передачи персональных данных, их объем, условия, формат, способы, а также содержащий требования по соблюдению мер защиты персональных данных и сохранению её конфиденциальности.

Субъект персональных данных должен быть уведомлен о необходимости передачи его персональных данных. Для окончательного решения вопроса о передаче персональных данных управление должно получить у субъекта согласие на передачу его персональных данных.

V. Защита персональных данных

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

Защита персональных данных, обрабатываемых с использованием средств автоматизации, представляет собой комплекс организационно – технических мер, позволяющих предупреждать нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, а именно:

- Исполнение регламентов доступа специалистов к ИСПДн;
- Наличие системы регулярно изменяемых паролей доступа к ПК, на которых производится ИСПДн;
- Регулярное исполнение администраторами БД мероприятий по проверке целостности персональных данных в ИСПДн;
- Организация системы автоматического резервного копирования ИСПДн;
- Периодическое копирование ИСПДн на внешние носители;
- Использование блоков бесперебойного питания и(или) устройств резервного электроснабжения;
- Ограничение доступа лиц к серверному оборудованию, на котором находятся базы данных, содержащие персональные данные;

- Использование лицензионных операционных систем и лицензионного программного обеспечения;
- Использование системы разграничения доступа к ИС (в ИС);
- Антивирусная защита ПК;
- Использование средств криптошифрования и ЭЦП;
- Использование разделенных ЛВС для изоляции различных ИС;
- Использование системы межсетевого экранирования при работе с сетями общего доступа;
- Программно-аппаратные средства, позволяющие организацию, внедрение и использование защищённых каналов связи.

5.1.1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации.

5.1.2. Для защиты персональных данных необходимо соблюдать ряд мер:

- соблюдение порядка охраны территории, здания, помещений;
- соблюдение порядка приема, учета и контроля деятельности посетителей;
- ограничение состава сотрудников, связанных с обработкой персональных данных;
- регламентирование состава сотрудников, имеющих право доступа (входа) в помещения с ИСПДн;
- регламентирование состава сотрудников, имеющих право доступа к различным ИСПДн;
- соблюдение сотрудниками требований нормативно-методических документов по защите информации и сохранении конфиденциальности обрабатываемой информации;
- создание условий для работы с ИСПДн, необходимых и достаточных для соблюдения требований по защите персональных данных;
- соблюдение порядка сбора, хранения, передачи, блокирования, уничтожения персональных данных;
- предупреждение и своевременное выявление нарушений требований системы защиты ИСПДн;
- регулярное проведение мероприятий по контролю за соблюдением требований системы защиты ИСПДн.

5.2. Для защиты ИСПДн создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для посторонних лиц, пытающихся совершить несанкционированный доступ и овладение информацией.

5.3. Под посторонним лицом понимается любое лицо, не имеющее непосредственного доступа к ИСПДн.

VI. Ответственность за нарушение требований защиты при обработке персональных данных

6.1. Персональная ответственность специалистов - одно из главных требований к организации функционирования системы защиты персональных данных и обязательное условие обеспечения эффективности этой системы.

6.2. Ответственность за доступ сотрудника к ИСПДн несет лицо, принявшее решение о необходимости предоставления доступа сотруднику.

6.3. Сотрудник, работающий с ИСПДн, несет персональную ответственность за достоверность и сохранность обрабатываемой информации.

6.4. Лица, нарушившие требования системы защиты персональных данных, несут ответственность в соответствии с законодательством РФ сообразно тяжести наступивших последствий.