



Департамент социальной политики и занятости населения Брянской области
Государственное бюджетное стационарное учреждение социального
обслуживания населения Брянской области
«Дятьковский дом-интернат для престарелых и инвалидов»»

ПРИКАЗ

08.02.2024 г. № 17

п. Бытошь

*Об утверждении правил обработки
персональных данных в ГБСУСОН
«Дятьковский дом-интернат для
престарелых и инвалидов»*

В целях выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 №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»

ПРИКАЗЫВАЮ:

1. Утвердить «Правила обработки персональных данных в государственном бюджетном стационарном учреждении социального обслуживания населения «Дятьковский дом-интернат для престарелых и инвалидов» (Приложение 1 к приказу).
2. Контроль исполнения настоящего приказа оставляю за собой.

Директор:

С.И.Киселев

Правила обработки персональных данных в ГБУСОН «Дятьковский дом-интернат для престарелых и инвалидов»

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Учреждение	ГБУСОН «Дятьковский дом-интернат для престарелых и инвалидов»
Персональные данные (ПДн)	Любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники
Блокирование персональных данных	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
Информационная система персональных данных (ИСПДн)	Информационная система, включающая в себя 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 работниками Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов ПДн, либо иным образом, затрагивающих их права и свободы или права и свободы 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
Материальный носитель	Бумажный или машиночитаемый носители информации (в том числе магнитный и электронный), на которых осуществляются запись и хранение сведений
Неправомерные действия с ПДн	Нарушение установленного данными правилами порядка обработки ПДн
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

Передача 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
Распространение персональных данных	Действия, направленные на раскрытие персональных данных неопределенному кругу лиц
Сбор персональных данных	Накопление информации на материальных носителях и (или) в автоматизированных информационных системах
Трансграничная передача персональных данных	Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу
Третьи лица	Любые лица (как физические, так и юридические), не являющиеся стороной индивидуального трудового договора, договора гражданско-правового характера, заключенного с Учреждением
Хранение персональных данных	Комплекс мероприятий, направленных на обеспечение сохранности полноты и целостности сформированных массивов персональных данных с последующим их накоплением или без такового, создание и поддержание надлежащих условий для их использования
Уничтожение персональных данных	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных
Уничтожение персональных данных в ИСПДн и на электронных носителях информации	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных или на носителях информации
Уничтожение материальных носителей (бумажных)	Гарантированное уничтожение бумажных носителей ПДн путем shredding (измельчения) либо через термическую обработку (сжиганием)
Уничтожение материальных носителей (электронных)	Гарантированное уничтожение носителей путем воздействия на рабочие слои электронных носителей, в результате которого разрушается физическая, магнитная или химическая структура рабочего слоя, после которого съём данных становится невозможным
Уточнение персональных данных	Процесс поддержания персональных данных в актуальном состоянии
Уполномоченный орган по защите прав субъектов ПДн	Федеральный орган исполнительной власти, осуществляющий самостоятельно функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Правила обработки персональных данных устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее - Правила), и единый порядок организации процесса обработки персональных данных в Учреждении.

2.2. Документ разработан в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

2.3. Правила обязательны для исполнения всеми работниками Учреждения, допущенными к обработке персональных данных.

2.4. Все работники Учреждения, на которых распространяются положения данных Правил о порядке обработки персональных данных, должны быть ознакомлены с ними под роспись.

3. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

3.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, не совместимая с целями сбора персональных данных.

3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой.

3.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.5. 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.

3.6. 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. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

3.7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных 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 законодательством Российской Федерации.

4. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В УЧРЕЖДЕНИИ

Цели обработки персональных данных в Учреждении определяются документом «Политика в отношении обработки персональных данных» утверждаемом нормативным актом Учреждения.

5. КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ В УЧРЕЖДЕНИИ

Категории субъектов, персональные данные которых обрабатываются в Учреждении, определяются в документе «Политика в отношении обработки персональных данных», утвержденным нормативным актом Учреждения.

6. КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В УЧРЕЖДЕНИИ

Категории обрабатываемых персональных данных утверждаются нормативным актом Учреждения.

7. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Лица, получающие доступ к персональным данным работников, обязаны обеспечить конфиденциальность персональных данных. Перечень лиц, осуществляющих обработку персональных данных утверждается нормативным актом Учреждения.

Обработка персональных данных в Учреждении может осуществляться как с использованием средств автоматизации, так и без использования таких средств.

Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных, осуществляется путем:

А) непосредственного получения оригиналов необходимых документов от гражданина (субъекта);

Б) копирования оригиналов документов;

В) внесения сведений в учетные формы (на бумажных и электронных носителях);

Г) внесения персональных данных и обработки их в автоматизированной информационной системе.

При сборе персональных данных непосредственно от гражданина (субъекта) работник Учреждения (или подведомственного органа), осуществляющий сбор (получение) персональных данных обязан разъяснить ему юридические последствия отказа предоставить свои персональные данные.

Места обработки и хранения персональных данных определяются нормативным актом Учреждения.

Перечень помещений, в которых обрабатываются и хранятся персональные данные, порядок доступа в них определяются нормативным актом Учреждения.

Персональные данные могут храниться на машинных и/или бумажных носителях. Хранение носителей осуществляется в оборудованных для этих целей прочных, запираемых на замки и опечатываемых шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

Хранение персональных данных осуществляется в форме, позволяющей определить персональные данные конкретного гражданина (субъекта), не дольше, чем того требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении целей обработки.

Передача персональных данных гражданина (субъекта) третьим лицам не допускается без письменного его согласия, за исключением случаев, установленных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

При передаче персональных данных работника третьим лицам необходимо в соглашениях, определяющих необходимость передачи, указывать требования к защите переданных персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

8. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сроки обработки и хранения персональных данных утверждаются нормативным актом Учреждения.

9. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Для выявления нарушений в Учреждении должны быть предусмотрены процедуры по:

осуществлению внутреннего контроля соответствия обработки персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, требованиям к защите персональных данных, политике в отношении обработки персональных данных в Учреждении, нормативным актам Учреждения;

ознакомлению работников, непосредственно осуществляющих обработку персональных данных, с законодательством Российской Федерации о персональных данных, (включая требования к защите персональных данных), и настоящими Правилами, нормативными документами Учреждения в сфере защиты персональных данных;

недопущению объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой;

обеспечению при обработке персональных данных точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных;

обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер.

9.2. Для предотвращения нарушений должны быть предусмотрены процедуры по:

изданию нормативных актов Учреждения по вопросам обработки персональных данных;

организации обработки ПДн в ИСПДн, включающей действия по систематизации, накоплению, использованию, обезличиванию, хранению, передаче, а также уничтожению, блокированию в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

назначению ответственного за организацию обработки персональных данных в Учреждения и утверждению его инструкции;

назначению ответственного за обеспечение безопасности обрабатываемых персональных данных в Учреждении и утверждению его инструкции;

определению лиц, уполномоченных на обработку и (или) доступ к персональным данным и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных;

ознакомлению (под роспись) работников Учреждения, непосредственно осуществляющих обработку персональных данных, 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. Ознакомление работников организуется ответственным за организацию обработки персональных данных, а осуществляется ответственным за обеспечение безопасности обрабатываемых;

применению правовых, организационных и технических мер по обеспечению безопасности персональных данных, необходимых для выполнения требований к защите

персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных, в том числе:

- идентификация и аутентификация субъектов доступа и объектов доступа; управление доступом субъектов доступа к объектам доступа; ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных); регистрация событий безопасности; антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

применению мер, необходимых для обеспечения сохранности персональных данных и исключающих несанкционированный к ним доступ при хранении материальных носителей, включающих:

- организацию режима обеспечения безопасности помещений, в которых обрабатываются персональные данные и хранятся носители персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывания помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений;
- утверждения правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях;
- утверждения перечня лиц, имеющих право доступа в помещения; хранение съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками и приспособлениями для опечатывания замочных скважин или кодовыми замками;
- осуществление поэкземплярного учета машинных носителей персональных данных, путем ведения журнала учета носителей персональных данных;
- применению средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации;
- определению угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- опубликованию на официальном сайте Учреждения в информационно-телекоммуникационной сети «Интернет» документа, определяющего политику Учреждения в отношении обработки персональных данных.

9.3. Внутренний контроль соответствия обработки персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, требованиям к защите

персональных данных в Учреждении проводится комиссией, создаваемой нормативным актом Учреждения. В состав комиссии обязательно должен быть включен ответственный за обеспечение безопасности персональных данных. Внутренний контроль осуществляется в соответствии с годовым планом, утверждаемым нормативным актом Учреждения.

10. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ДОСТИЖЕНИИ ЦЕЛЕЙ ОБРАБОТКИ ИЛИ ПРИ НАСТУПЛЕНИИ ИНЫХ ЗАКОННЫХ ОСНОВАНИЙ

Порядок уничтожения персональных данных утверждается нормативным актом Учреждения.

11. РАССМОТРЕНИЕ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ

Порядок рассмотрения запросов субъектов персональных данных или их представителей утверждается нормативным актом Учреждения.

12. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ПРАВИЛ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Работники Учреждения несут персональную ответственность за соблюдение требований по обработке и обеспечению безопасности ПДн в соответствии с законодательством Российской Федерации.

12.2. При поступлении на работу в Учреждение работник, доступ которому к персональным данным необходим для исполнения должностных обязанностей, подписывает обязательство о соблюдении конфиденциальности информации.

12.3. Работник Учреждения может быть привлечен к ответственности в случаях:

- умышленного или неосторожного раскрытия ПДн;
- утраты материальных носителей ПДн;
- нарушения требований настоящих Правил и других нормативных документов Учреждения в части вопросов доступа и работы с ПДн.

12.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения субъектам персональных данных материального или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

