Приложение №1 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

ПОЛИТИКА

Государственного бюджетного учреждения социального обслуживания Ярославской области Гаврилов – Ямского дома – интерната для престарелых и инвалидов в отношении обработки персональных данных

1.Общие положения

Полное наименование: Государственное бюджетное учреждение социального обслуживания Ярославской области Гаврилов – Ямского дома – интерната для престарелых и инвалидов.

Юридический адрес: Ярославская область, г. Гаврилов-Ям, ул. Кирова, д. 6.

Почтовый адрес: 152240, Ярославская область, г. Гаврилов-Ям, ул. Кирова, д. 6.

Регистрационный номер записи в реестре операторов, осуществляющих обработку персональных данных: 11-0188213 от 31.03.2011

Государственное бюджетное учреждение социального обслуживания Ярославской области Гаврилов – Ямского дома – интерната для престарелых и инвалидов (далее – Оператор) в терминах Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (в редакции) является **оператором персональных данных** – юридическим лицом, осуществляющим обработку персональных данных и определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия, совершаемые с персональными данными.

Обработка персональных данных осуществляется Оператором в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», ст.ст 86-90 Трудового кодекса Российской Федерации, Федерального закона № 261-ФЗ от 25.07.2011г., Постановлением Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и принятых иных нормативных правовых актов, регулирующих вопросы обработки и защиты персональных данных. При обработке персональных данных Оператор придерживается принципов, установленных законодательством Российской Федерации в области персональных данных.

2. Термины и принятые сокращения

Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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;

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

3. Цели и условия обработки персональных данных

Оператор осуществляет обработку персональных данных на законной и справедливой основе с согласия субъекта на их обработку, в следующих **целях**:

– ведение бухгалтерского учета деятельности ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов,

– составление первичных учетных документов;

– расчет заработной платы и иных выплат работникам ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов и зачисление денежных средств на карт-счета;

– формирование бюджетной, налоговой и иной отчетности о деятельности ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов;

– создание и использование полнотекстовой базы данных локальных актов (приказов)по основной деятельности ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов;

– составление и печать характеристик на сотрудников ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов;

– учет прохождения сотрудниками ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов ежегодных медицинских осмотров;

– подготовка сведений для назначения дополнительных выплат сотрудникам ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов

– подготовка сведений о получателях социальных услуг

– ведение и актуализации справочной информации;

– исполнение гражданско-правовых договоров, судебных актов (исполнительных производств), контрактов (обеспечение оплаты денежных обязательств перед контрагентами), исполнение кассового обслуживания;

– предоставление отчетности об уплате налогов и сборов с доходов работников и контрагентов (физических лиц), страховых взносов в рамках обязательного пенсионного, медицинского и социального страхования в территориальные органы ПФР, ФНС России, ФСС России;

– для обработки биометрических персональных данных;

– осуществление кадровой работы,

– проведение закупок, заключение и исполнение договоров (контрактов);

– подготовка материалов для передачи в судебные и иные инстанции;

– рассмотрение обращений граждан, в том числе запросов в архив;

– для защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

– учета входящей и исходящей корреспонденции и внутренних документов ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов.

Для достижения перечисленных целей Оператор прибегает к обработке персональных данных следующих субъектов:

- работники ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов

- бывшие работники ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов

- потребители социальных услуг *(социальные клиенты)* ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов

- контрагенты ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов

Оператор осуществляет обработку персональных данных как **с использованием средств вычислительной техники** (в том числе, в информационных системах), так и **без использования технических средств**.

В целях предотвращения нарушений законодательства Российской Федерации в сфере персональных данных Оператором обеспечивается надлежащее **документальное сопровождение** процессов обработки персональных данных:

– анализ правовых оснований обработки персональных данных, в т.ч. оценка вреда субъекту персональных данных в случае нарушения действующего законодательства;

– документальное закрепление целей обработки;

– установление сроков обработки персональных данных;

– регламентация процессов обработки персональных данных (в том числе процесса допуска к персональным данным, процесса прекращения обработки персональных данных);

– определение круга лиц, осуществляющих обработку персональных данных и (или) имеющих доступ к персональным данным;

– нераспространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено ФЗ №152;

– выявление и классификация информационных систем персональных данных

– распределение и закрепление обязанностей и ответственности работников Оператора в сфере обработки и обеспечения безопасности персональных данных.

Предоставление права доступа к персональным данным (допуск к обработке персональных данных), обрабатываемым Оператором, осуществляется в соответствии с установленным порядком.

Обеспечение безопасности персональных данных, обрабатываемых Оператором, достигается скоординированным применением различных по своему характеру мер как организационного, так и технического характера (средства защиты информации, учёт машинных носителей персональных данных, установление правил доступа к персональным данным и пр.).

Оператором реализованы меры физической защиты помещений, где размещены технические средства, обрабатывающие персональные данные, и хранятся материальные носители персональных данных, от несанкционированного проникновения.

Все сотрудники Оператора, допущенные к обработке персональных данных, ознакомлены под роспись с положениями законодательства РФ о персональных данных, в т.ч. с требованиями к защите персональных данных, локальными актами Оператора по вопросам обработки и защиты персональных данных в части, их касающейся.

4.Права субъектов персональных данных и способ их реализации

В соответствии с положениями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» субъект персональных данных имеет следующие **права** в отношении **своих** персональных данных:

1) право на получение сведений, касающихся обработки персональных данных Оператором[1]:

– подтверждение факта обработки персональных данных Оператором;

– правовые основания и цели обработки персональных данных;

– применяемые Оператором способы обработки персональных данных;

– наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

2) право на ознакомление с персональными данными, принадлежащими субъекту персональных данных, обрабатываемыми Оператором;

3) право требования от Оператора уточнения его персональных данных, их блокирования или уничтожения, в случае, если персональные данные являются неполными, устаревшими (неактуальными), неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

4) право на отзыв согласия на обработку персональных данных (если такое согласие было дано Оператору), в т.ч. на отзыв согласия на обработку персональных данных для распространения (Оператор обязан обеспечить возможность определения перечня персональных данных субъекта для распространения) ;

5) право на обработку специальных категорий персональных данных (расовая, национальная принадлежность, политические взгляды, состояние здоровья, интимная жизнь и др.) только с письменного согласия субъекта на обработку персональных данных;

Субъект персональных данных может реализовать свои права на получение сведений, касающихся обработки его персональных данных Оператором, и на ознакомление с персональными данными, принадлежащими субъекту, обрабатываемыми Оператором, путем **обращения** (лично или через представителя) по адресу: Ярославская область, г. Гаврилов-Ям, ул. Кирова, д. 6, контактный телефон – (48534)2 05 68, кабинет специалиста по кадрам, время приема – с 8:00 до 12:00, с 12:30 до 16:30 , либо путем направления письменного **запроса** по адресу: 152240, Ярославская область, г. Гаврилов-Ям, ул. Кирова, д. 6, в адрес Руководителя или специалиста по кадрам. Запрос может быть направлен в форме электронного документа,

[1] За исключением случаев, описанных в части 8 статьи 14 Федерального закона

подписанного электронной подписью в соответствии с законодательством Российской Федерации, по адресу: gavrilstar@yandex.ru .

В соответствии с частью 3 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» **запрос** субъекта персональных данных (или его представителя) **должен содержать**:

– номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

– сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;

– подпись субъекта персональных данных или его представителя (в случае недееспособности субъекта персональных данных).

Рекомендуемые формы запросов субъектов персональных данных или их представителей приведены в приложении к данному документу.

Оператор обязуется безвозмездно предоставить запрашиваемые сведения субъекту персональных данных или его представителю в доступной форме **в течение тридцати дней** с даты обращения или даты получения запроса субъекта персональных данных или его представителя либо дать в письменной форме мотивированный ответ, содержащий ссылку на положения федерального закона (законов), являющиеся основанием для отказа в предоставлении информации.

В случае если необходимые сведения были предоставлены субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться **повторно** к Оператору или направить ему повторный запрос в целях получения данных сведений **не ранее чем через тридцать дней** после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

В срок, не превышающий **семи рабочих дней** со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные, обрабатываемые Оператором, являются неполными, неточными или неактуальными, Оператор обязуется **внести** в них **необходимые изменения**.

В срок, не превышающий **семи рабочих дней** со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные, обрабатываемые Оператором, являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязуется **уничтожить** такие персональные данные.

Оператор обязан **уведомить** субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

Субъект персональных данных имеет право на отзыв согласия на обработку персональных данных (в случае, если такое согласие было дано Оператору). Рекомендуемая форма заявления об отзыве согласия на обработку персональных данных приведена в приложении к настоящему документу.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки, и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение в срок, не превышающий **тридцати дней** с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных, либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

В случае невозможности уничтожения персональных данных в течение указанного срока, Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование и уничтожение в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

5. Модель угроз и нарушителя безопасности персональных данных при их обработке в информационных системах персональных данных

5.1. Под угрозами безопасности персональных данных при их обработке в информационных системах понимается совокупность условий и факторов, создающих потенциальную опасность, связанную с утечкой информации и (или) с несанкционированными и (или) непреднамеренными воздействиями на нее.

5.2. Угрозы безопасности персональных данных при их обработке в информационных системах могут быть связаны как с преднамеренными действиями сотрудников учреждения, так и со специально осуществляемыми неправомерными действиями отдельных организаций, также иными источниками угроз.

5.3. В целях формирования перечня угроз безопасности персональных данных при их обработке в информационных системах выделяются следующие виды угроз:

5.3.1. Угрозы связанные с преднамеренными или непреднамеренными действиями операторов по обработке персональных данных имеющих доступ к тем или иным информационным системам.

5.3.2. Угрозы связанные с преднамеренными или непреднамеренными действиями операторов по обработке персональных данных не имеющих доступ к тем или иным информационным системам.

5.3.3. Угрозы, связанные со стихийными природными явлениями.

5.3.4. Угрозы, связанные с внедрением вредоносных программ.

5.3.5. Угрозы, связанные с закладочным устройством - элементом средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в оборудование, предметы интерьера, а также в технические средства и системы обработки информации).

5.3.6. Угрозы, связанные с нарушением правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации.

5.3.7. Угрозы, связанные с несообщением фактов утраты, компрометации ключей, парольной защиты в информационных системах.

5.4. Контролируемой зоной информационных систем персональных данных являются помещения учреждения. В пределах контролируемой зоны находятся рабочие места операторов по обработке персональных данных в информационных системах, сетевое и телекоммуникационное оборудование.

5.5. В соответствии с наличием права постоянного или разового доступа в контролируемую зону объектов размещения информационных систем персональных данных все физические лица могут быть отнесены к следующим категориям:

- категория 1 - лица, имеющие право доступа в контролируемую зону информационных систем обработки персональных данных;
- категория 2 - лица, не имеющие право доступа в контролируемую зону информационных систем обработки персональных данных.

5.6. Все потенциальные нарушители безопасности персональных данных подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны.

5.7. В качестве внешнего нарушителя, кроме лиц категории 1 должны рассматриваться лица категории 2, находящиеся за пределами контролируемой зоны.

5.8. В отношении информационных систем персональных данных в качестве внешнего нарушителя из числа лиц категории 1 могут выступать:
- бывшие сотрудники учреждения;
- посторонние лица, пытающиеся получить доступ к персональным данным;
- представители преступных организаций.

6. Правила организации парольной защиты в информационных системах персональных данных

6.1. С целью ограничения доступа к информационным системам обработки персональных данных в учреждении утверждается единая система установки паролей на базе общего и прикладного программного обеспечения средств защиты информации.

6.2. На всех компьютерах, на которых имеется доступ к информационным системам обработки персональных данных, должен быть установлен пароль.

6.3. Личные пароли должны выбираться пользователями самостоятельно, с учетом следующих требований:
- длина пароля должна быть не менее 8 буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, и т. д.), а также общепринятые сокращения;
- в пароле должны присутствовать символы трех категорий - прописные, строчные, десятичные цифры;
- запрещается выбирать пароли, которые использовались ранее.

6.4. Правила хранения паролей:

6.4.1. Запрещается записывать пароли на бумаге, в файл, электронную записную книжку и друге носители информации, в том числе на предметах;

6.4.2. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6.4.3. Пароли всех операторов персональных данных хранятся у администратора безопасности персональных данных в недоступном месте.

6.4.4. Личные пароли сотрудников, допущенных к информационным системам персональных данных, разглашению не подлежат.

6.5. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

6.6. Нарушение пользователями целостности установленного программного обеспечения, а также самовольное установление программ, не предназначенных для выполнения должностных обязанностей, категорически запрещается.

6.7. Порядок плановой и внеплановой смены личного пароля.

6.7.1. Плановая смена паролей должна проводиться регулярно, но не реже одного раза в квартал.

6.7.2. Проведение плановой смены личных паролей контролирует администратор безопасности персональных данных.

6.7.3. Внеплановая смена любого пароля пользователя информационных систем персональных данных производится:
- по желанию самого пользователя;
- при компрометации существующего пароля;
- по требованию администратора безопасности персональных данных.

6.7.4. Внеплановая смена всех паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности персональных данных.

6.8. Операторы должны своевременно сообщать администратору информационной безопасности об изменении, утере, компрометации паролей.

6.9. Любая смена паролей отражается в Журнале смены паролей пользователей.

7. Порядок обработки персональных данных без использования средств автоматизации

7.1. Обработка персональных данных без использования средств автоматизации в учреждении осуществляется в виде формирования личных дел сотрудников, анкет претендентов на замещение вакантных должностей и личных дел получателей социальных услуг.

7.2. 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).

7.3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых, заведомо не совместимы.

7.4. Типовая форма документа, предполагающая или допускающая включение в нее персональных данных, должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

7.5. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем изготовления нового материального носителя с уточненными персональными данными.

7.6. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

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

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

8. Порядок работы с обезличенными данными в случае обезличивания персональных данных

8.1. Обезличенные персональные данные конфиденциальны и не подлежат разглашению.

8.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

8.3. В учреждении могут применяться следующие методы обезличивания персональных данных:
- метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);
- метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);
- метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);
- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

8.4. Непосредственное обезличивание персональных данных выбранным способом производят операторы, осуществляющие обработку таких данных.

9. Безопасность и защита персональных данных

9.1. С целью обеспечения безопасности персональных данных при их обработке и предотвращению угроз учреждение принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

9.2. Все реализуемые учреждением мероприятия по организационной и технической защите персональных данных осуществляются на законных основаниях, в том числе в соответствии с

требованиями законодательства Российской Федерации в сфере обработки персональных данных.

9.3. Учреждение применяет необходимые и достаточные правовые, организационные и технические меры по обеспечению безопасности персональных данных, включающие в себя использование средств защиты информации, обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по его недопущению, восстановление персональных данных, ограничение доступа к персональным данным, регистрацию и учёт действий с персональными данными, а также контроль и оценку эффективности применяемых мер по обеспечению безопасности персональных данных.

10. Осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

10.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных проводятся периодические проверки условий обработки персональных данных.

10.2. Проверки осуществляются постоянно действующей комиссией по информационной безопасности, функционирующей на основании положения. (Приложение к Политике)

10.3. Внутренние проверки проводятся по необходимости в соответствии с поручением директора учреждения.

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

10.5. Для каждой проверки составляется акт проведения внутренней проверки.

10.6. При выявлении в ходе проверки нарушений постоянно действующей комиссией по информационной безопасности в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

10.7. В ходе осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных производится проверка осуществления обработки персональных данных.

10.7.1. С использованием средств автоматизации:

- соответствие полномочий пользователя порядку доступа к персональным данным;
- соблюдение пользователями информационных систем персональных данных требований к хранению паролей;
- соблюдение пользователями информационных систем персональных данных антивирусной защиты;
-наличие программного обеспечения не связанного с исполнением служебных обязанностей;
- соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;
- соблюдение раздельного хранения персональных данных, обработка которых осуществляется в различных целях;

10.7.2. Без использования средств автоматизации:

- условия хранения бумажных носителей с персональными данными;
- соблюдение раздельного хранения персональных данных, обработка которых осуществляется в различных целях;
- соблюдение порядка доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

11. Заключительные положения

11.1. Учреждение в ходе своей деятельности может предоставлять и (или) поручать обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. При этом обязательным условием предоставления и (или) поручения обработки персональных данных другому лицу является обязанность сторон по соблюдению конфиденциальности и обеспечению безопасности персональных данных при их обработке.

11.2. Учреждение не размещает персональные данные субъекта персональных данных в общедоступных источниках без его предварительного согласия.

11.3. Учреждение в ходе своей основной деятельности при обработке персональных данных не осуществляет трансграничной передачи персональных данных на территорию иностранных государств.

11.4. В случае возникновения необходимости осуществления трансграничной передачи персональных данных на территорию иностранных государств органам власти иностранного государства, иностранным физическим или юридическим лицам учреждение обязано обеспечить адекватную защиту прав субъектов персональных данных и обеспечения при трансграничной передаче безопасности их персональных данных в соответствии с законодательством Российской Федерации в сфере обработки персональных данных, в том числе при условии наличия письменного согласия субъекта персональных данных на трансграничную передачу.

11.5. В учреждении назначаются должностные лица, ответственные за организацию обработки и обеспечение безопасности персональных данных.

11.6. Каждый вновь принятый на работу работник учреждения, непосредственно осуществляющий обработку персональных данных, подлежит ознакомлению с требованиями законодательства Российской Федерации по обработке и обеспечению безопасности персональных данных, с настоящей Политикой и другими организационно-распорядительными документами по вопросам обработки и обеспечения безопасности персональных данных и обязуется их соблюдать.

11.7. Ответственность должностных лиц учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними организационно-распорядительными документами учреждения.

Приложение к Политике ГБУ СО ЯО
Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
в отношении обработки персональных данных

**Запрос на предоставление сведений,
касающихся обработки персональных данных
субъекта персональных данных**

Директору ГБУ СО ЯО
Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
Ф.И.О. директора

От: _____
(фамилия, имя, отчество субъекта персональных данных)

паспорт: _____, выданный _____
(серия, номер) (дата выдачи)

_____
(наименование органа, выдавшего паспорт)

Сведения, подтверждающие участие субъекта в отношениях с Оператором:

_____
(№ и дата заключения договора, иные сведения)

В соответствии со ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» прошу предоставить следующие сведения (отметить необходимое):

☐ подтверждение факта обработки моих персональных данных;

☐ правовые основания и цели обработки моих персональных данных;

☐ способы обработки моих персональных данных;

☐ наименование и место нахождения Оператора, сведения о лицах, которые имеют доступ к моим персональным данным или которым могут быть раскрыты мои персональные данные;

☐ обрабатываемые персональные данные, относящиеся ко мне, и источник их получения;

☐ сроки обработки моих персональных данных, в том числе сроки их хранения;

☐ порядок осуществления мною прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

☐ сведения об осуществленной или предполагаемой трансграничной передаче моих персональных данных;

☐ наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку моих персональных данных по поручению Оператора;

☐ иные сведения: _____.

Указанные сведения прошу предоставить:

☐ в письменном виде по адресу: _____

☐ по адресу электронной почты: _____

_____ _____
(дата) (подпись)

**Запрос на предоставление сведений,
касающихся обработки персональных данных субъекта,
от представителя субъекта персональных данных**

Директору ГБУ СО ЯО
Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
Ф.И.О. директора

От: _____
(фамилия, имя, отчество представителя субъекта персональных данных)

паспорт: _____, выданный _____
(серия, номер) (дата выдачи)

_____
(наименование органа, выдавшего паспорт)

В соответствии со ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», действуя на основании

_____,
(реквизиты документа, подтверждающего полномочия представителя субъекта персональных данных)

прошу предоставить следующие сведения (отметить необходимое):

☐ подтверждение факта обработки персональных данных субъекта;

☐ правовые основания и цели обработки персональных данных субъекта;

☐ способы обработки персональных данных субъекта;

☐ наименование и место нахождения Оператора, сведения о лицах, которые имеют доступ к персональным данным субъекта или которым могут быть раскрыты персональные данные субъекта;

☐ обрабатываемые персональные данные, относящиеся к субъекту, и источник их получения;

☐ сроки обработки персональных данных субъекта, в том числе сроки их хранения;

☐ порядок осуществления субъектом прав, предусмотренным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

☐ сведения об осуществленной или предполагаемой трансграничной передаче;

☐ наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных субъекта по поручению Оператора;

☐ иные сведения: _____

в отношении _____
(фамилия, имя, отчество субъекта персональных данных)

документ, удостоверяющий личность: _____, выданный _____
(серия, номер) (дата выдачи)

_____
(наименование органа, выдавшего документ)

Сведения, подтверждающие участие субъекта в отношениях с Оператором:

_____
(№ и дата заключения договора, иные сведения)

Указанные сведения прошу предоставить:

☐ в письменном виде по адресу: _____

☐ по адресу электронной почты: _____

Приложение №2 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

ПРАВИЛА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
в ГБУ СО ЯО Гаврилов-Ямском доме-интернате для престарелых и инвалидов

I.Общие положения

1. Настоящие Правила обработки персональных данных (далее — Правила) в ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов (далее – Учреждение) разработаны в соответствии с законодательством Российской Федерации и устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2. Настоящие Правила регламентируют процессы обработки персональных данных в Учреждении, в т.ч. устанавливают меры по обеспечению их обработки, как Оператора, осуществляющего обработку персональных данных.

3. Обработка персональных данных в Учреждении осуществляется в целях рассмотрения обращений граждан, предоставления социальных услуг и в связи с реализацией трудовых отношений.

II. Условия и цели обработки персональных данных

2.1. Настоящими Правилами определяется следующие условия обработки персональных данных, относительно субъектов персональных данных.

2.1.1. Персональные данные работников ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов , граждан, претендующих на замещение должностей в ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов, обрабатываются в целях обеспечения кадровой работы, в оформлении трудовых отношений, начислении заработной платы, в том числе в целях содействия работникам ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов в обучении, прохождения медицинского осмотра, учета результатов исполнения работниками должностных обязанностей, обеспечения работникам установленных законодательством Российской Федерации условий труда, гарантий и компенсаций.

2.1.2. Персональные данные физических лиц, обратившихся в Учреждение в письменной форме или в форме электронного документа, а также с устным обращением, обрабатываются в целях их рассмотрения и последующего уведомления о результатах рассмотрения.

2.1.3. Персональные данные лиц, обратившихся за оказанием социальных услуг, обрабатываются в целях предоставления социальных услуг.

2.2. Согласие на обработку персональных данных субъекта персональных данных, чьи данные обрабатываются в целях, указанных в пункте 2.1.1 настоящих Правил, не требуется при обработке персональных данных в соответствии с пунктом 2 части 1 статьи 6 Федерального закона «О персональных данных», кроме случаев, предусмотренных пунктом 2.3 настоящих Правил.

2.3. Необходимо получить согласие субъекта персональных данных на обработку его персональных данных:

при передаче персональных данных третьей стороне (за исключением случаев, предусмотренных федеральными законами);

при распространении персональных данных;

при принятии решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных.

2.4. Согласие на обработку персональных данных субъекта необходимо получать непосредственно у субъекта персональных данных в любой форме, позволяющей подтвердить факт его получения, если иное не установлено федеральными законами.

2.5. Согласие на обработку персональных данных, разрешённых субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешённых субъектом персональных данных для распространения.

2.6. Организация сбора и хранения письменных согласий на обработку персональных данных субъектов персональных данных возлагается на специалистов ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов, непосредственно осуществляющие обработку персональных данных.

2.7. Цели обработки персональных данных в Учреждении закрепляются в Перечне целей и сроков обработки персональных данных.

2.8. Обработка персональных данных в Учреждении строго ограничивается достижением целей, указанных в Перечне целей и сроков обработки персональных данных. Обработка персональных данных в иных целях не допускается.

2.9. Добавление в Перечень новой цели обработки персональных данных может осуществляться как по решению директора Учреждения, так и по инициативе работников Учреждения, которые должны уведомить лицо, ответственное за организацию обработки персональных данных, о необходимости введения новой цели обработки персональных данных. Работникам Учреждения запрещается осуществлять обработку персональных данных до включения новой цели в Перечень целей и сроков обработки персональных данных и обеспечения должного документального сопровождения процесса обработки персональных данных в соответствии с данной целью (определение необходимости взимания согласия субъекта на обработку его персональных данных и разработка формы согласия; актуализация внутренних документов).

2.10. Содержание (перечень категорий) обрабатываемых персональных данных и круг субъектов, персональные данные которых обрабатываются в Учреждения, определяются целями обработки персональных данных и закрепляются в Перечне целей и сроков обработки персональных данных. Обработка персональных данных, избыточных по отношению к установленным целям обработки, не допускается.

III. Действия (операции), совершаемые с персональными данными

3.1. Учреждение осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных и иные действия, указанные в Федеральном законе № 152-ФЗ от 27.07.2006 «О персональных данных».

3.2. Обработка персональных данных, обрабатываемых в случаях, предусмотренных пунктом 2 настоящих Правил, осуществляется путем:

копирования оригиналов документов;

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

получения оригиналов необходимых документов (трудовая книжка, автобиография, иные документы, предоставляемые специалисту по кадрам) Учреждения;

получения оригиналов необходимых документов от получателя социальных услуг (паспорт, иные документы, биометрические данные, предоставляемые уполномоченным лицам Учреждения);

создания персональных данных в ходе кадровой работы;

получения письменных обращений в установленной форме;

регистрации персональных данных на бумажных и электронных носителях информации;

получения объяснений, информации, справок от физических лиц, организаций и органов, находящихся на территории Российской Федерации, а также на территориях иностранных государств, в порядке, установленном международным договором Российской Федерации;

получения персональных данных из общедоступных источников;

фиксации (регистрации) в соответствующих журналах, книгах.

3.3. При сборе персональных данных специалист ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов, осуществляющий получение персональных данных непосредственно от субъекта персональных данных, обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3.4. Обработка персональных данных в связи с реализацией Учреждением трудовых отношений осуществляется с письменного согласия субъектов персональных данных, которое действует со дня их поступления на работу и на время ее прохождения, как с использованием средств автоматизации, так и без использования таких средств. Обеспечение защиты персональных данных, содержащихся в личных делах субъектов персональных данных, от неправомерного их использования или утраты осуществляется специалистом по кадрам. Персональные данные и иные сведения, содержащиеся в личных делах субъектов персональных данных, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации), а в случаях, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации, - к сведениям, составляющим государственную тайну.

3.5. При обработке Учреждением персональных данных в целях предоставления социальных услуг и в связи с реализацией трудовых отношений лица, уполномоченные на обработку персональных данных (далее – уполномоченные 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 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. Осуществлять передачу персональных данных сотрудников в пределах Компании в соответствии с настоящими Правилами. Предупреждать лиц, получивших персональные данные сотрудника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные сотрудника, обязаны соблюдать режим секретности (конфиденциальности). 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, Учреждение 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, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

д) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта 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 актом.

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

3.6. 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 от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

в) требовать внесения необходимых изменений, уничтожения или блокирования 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.

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

4.1. Источником информации о нарушениях законодательства Российской Федерации в сфере персональных данных могут служить:

- сообщения работников Учреждения;
- сообщения субъектов персональных данных;
- уведомления/сообщения органов, осуществляющих контроль или надзор за деятельностью Учреждения.

4.2. При получении сообщения о нарушениях законодательства Российской Федерации в сфере персональных данных по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например, путем совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных, указанных в подписи сообщения или названных при звонке).

4.3. Работник Учреждения, получивший информацию о нарушениях законодательства Российской Федерации в сфере персональных данных, сообщает об этом сотруднику Учреждения, ответственному за организацию обработки персональных данных, и своему непосредственному руководителю.

4.4. Сотрудник Учреждения, ответственный за организацию обработки персональных данных, в письменной форме сообщает о факте нарушения директору Учреждения, сотруднику, возглавляющему комиссию по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

4.5. Комиссия собирает и анализирует все данные об обстоятельствах нарушения законодательства Российской Федерации в сфере персональных данных (электронные письма, работа информационных систем, показания сотрудников и др.), устанавливает, имела ли место утечка сведений и обстоятельства, ей сопутствующие, определяет перечень лиц, виновных в нарушении предписанных законодательством мероприятий по защите персональных данных, устанавливает причины и условия, способствовавшие нарушению.

4.6. По итогам работы комиссии директору Учреждения предоставляется отчет, в котором указываются причина нарушения законодательства Российской Федерации в сфере персональных данных, последствия данного факта, лица, виновные в возникновении нарушения законодательства Российской Федерации в сфере персональных данных, предложения о наказании виновных лиц и мерах по недопущению подобных инцидентов в будущем.

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

5.1. По окончании сроков хранения персональных данных, они физически уничтожаются с целью невозможности восстановления и дальнейшего использования.

Уничтожение персональных данных, размещённых на бумажных носителях, осуществляется способами, не допускающими дальнейшую возможность ознакомления с данными документами.

Уничтожение персональных данных, размещённых на жестких дисках компьютеров, а также съемных носителях производится специальными программными средствами, осуществляющими удаление информации без возможности ее восстановления.

Уничтожение персональных данных, размещённых на неперезаписываемых оптических дисках формата CD-R, DVD-R, осуществляется путем физического уничтожения носителя.

5.2. Уничтожение персональных данных осуществляется комиссией по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

5.3. По результатам работы комиссии составляется акт уничтожения персональных данных.

VI. Правила допуска и доступа к персональным данным

Уполномоченные должностные лица допускаются к информации, содержащей персональные данные, в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими служебных обязанностей.

Иные лица допускаются к персональным данным с разрешения директора Учреждения с соблюдением требований настоящих Правил.

В соответствии с ч. 3 ст. 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» Учреждение вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе муниципального контракта, либо на основании локального акта Учреждения. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных.

В поручении Учреждения (договоре, контракте или локальном акте) должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Допуск к персональным данным, в том числе содержащимся в информационных системах персональных данных сторонних организаций, деятельность которых не связана с исполнением функций Учреждения, регламентируется законодательством и нормативными правовыми Российской Федерации, а также контрактами (договорами, соглашениями) Учреждения с операторами соответствующих информационных систем персональных данных.

Доступ к техническим (программно-техническим) средствам информационных систем персональных данных Учреждения предоставляется сторонним организациям, выполняющим работы на договорной основе.

Порядок допуска указанных организаций определяется в контракте на выполнение работ (оказание услуг). Решением о допуске является подписанный в установленном порядке контракт на выполнение работ (оказание услуг).

Доступ к персональным данным сторонних организаций осуществляется на основании письменных запросов или письменных соглашений (договоров) сторон об обмене информацией.

В письменном запросе (соглашении, договоре) должны быть указаны следующие сведения:

- цель получения информации;
- конкретное наименование информации (состав персональных данных);
- способ доступа (предоставления), а также сведения о регистрации в уполномоченных органах по защите прав субъектов персональных данных, осуществляющих функции по контролю и надзору в сфере информационных технологий и связи.

При наличии соглашения со сторонней организацией о допуске к персональным данным (предоставлении информации) доступ к персональным данным осуществляется в порядке, указанном в подписанном соглашении (договоре).

Доступ к персональным данным, в том числе содержащимся в информационных системах персональных данных сторонних организаций, выполняющих работы на договорной основе, осуществляется на основании подписанного договора на оказание услуг, а также настоящих Правил.

Запрещается передача электронных копий баз (банков) данных, содержащих персональные данные, любым сторонним организациям, за исключением случаев, предусмотренных законодательством Российской Федерации.

VII. Ответственность за нарушение установленных требований по обращению с персональными данными и обеспечению их безопасности

7.1. Ответственность за своевременность и качество выполнения требований законодательства Российской Федерации в сфере персональных данных несет директор Учреждения.

7.2. Лицо, ответственное за организацию обработки персональных данных, несет ответственность за:

– соответствие процессов обработки персональных данных в Учреждении заявленным целям их обработки;

– соблюдение сроков обработки персональных данных и их соответствие заявленным целям их обработки;

– правомерность передачи персональных данных третьим лицам или их опубликования;

– актуальность уведомления уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных.

7.3. Лицо, ответственное за обеспечение безопасности персональных данных, несет ответственность за соблюдение установленных законодательством Российской Федерации и внутренними документами Учреждения требований по обеспечению безопасности персональных данных при их обработке.

7.4. Работник, получающий доступ к документам, файлам, базам данных или их частям, содержащим персональные данные, несет персональную ответственность за любые действия, совершаемые с информацией или ее носителями им или от его имени.

7.5. Лица, виновные в нарушении законодательно установленных норм, регулирующих порядок обработки персональных данных, а также требований по обеспечению их безопасности, в том числе осуществившие несанкционированный доступ к персональным данным или несанкционированную передачу (сообщение) персональных данных третьим лицам, несут административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

7.6. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного внутренними документами порядка обращения с персональными данными работодатель вправе применять предусмотренные Трудовым Кодексом Российской Федерации дисциплинарные взыскания.

Приложение к Правилам обработки
персональных данных

Утверждаю

_____
(должность, фамилия и инициалы)
«___» _____ 20__ г.

АКТ
уничтожения персональных данных
Учреждения

Председатель комиссии: _____
(Должность, Ф.И.О)

Члены комиссии:
(Должность, Ф.И.О)
(Должность, Ф.И.О)
(Должность, Ф.И.О)
(Должность, Ф.И.О.)

составили настоящий акт в том, что «__» _____ 20__ г. произведено уничтожение персональных данных, _____
(наименование персональных данных)

находящихся на _____
(наименование носителя информации)

Персональные данные были уничтожены путем _____
_____
(способ уничтожения информации)

Председатель комиссии:
_____ _____ «__» _____ 20__ г.
(Фамилия, инициалы) (подпись)

Члены комиссии:
_____ _____ «__» _____ 20__ г.
(Фамилия, инициалы) (подпись)
_____ _____ «__» _____ 20__ г.
(Фамилия, инициалы) (подпись)
_____ _____ «__» _____ 20__ г.
(Фамилия, инициалы) (подпись)
_____ _____ «__» _____ 20__ г.
(Фамилия, инициалы) (подпись)

Приложение №3 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

ПЕРЕЧЕНЬ
целей и сроков обработки персональных данных, обрабатываемых
в ГБУ СО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов в связи с реализацией трудовых отношений, а также в связи с предоставлением социальных услуг

№ п/п	Цели обработки ПДн	Категории субъектов ПДн, перечень обрабатываемых ПДн	Правовые основания обработки ПДн	Сроки обработки ПДн	Действия с ПДн по окончании обработки
1	Ведение бухгалтерского учета деятельности Учреждения; составление первичных учетных документов, а также их проектов; расчет заработной платы и иных выплат работникам Учреждения; формирование бюджетной, налоговой и иной отчетности о деятельности Учреждения; Предоставление отчетности об уплате налогов и сборов с доходов работников и контрагентов (физических лиц) Учреждения, а также страховых взносов в рамках обязательного пенсионного, медицинского и социального страхования в территориальные органы ПФР, ФНС России, ФСС России	ПДн работников Учреждения: - фамилия, имя, отчество; - пол; - дата и место рождения; - сведения о гражданстве; - реквизиты документа, удостоверяющего личность (серия, номер, дата выдачи и наименование органа, выдавшего документ); - СНИЛС; - ИНН; - сведения о приеме на работу, переводах на другую должность, увольнении; - сведения о присвоении класса вредности, разрядов; - сведения об отпусках, командировках, периодах временной нетрудоспособности; - сведения о заработной плате;	Налоговый кодекс РФ. Часть вторая от 5 августа 2000 г. № 117-ФЗ (п. 2 ст. 230); Федеральный закон от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (п. 1, п. 2 ст. 8; ст. 9); Федеральный закон от 03.07.2016г. №250-ФЗ(в редакции от 30.04.2021г); Инструкция о порядке ведения индивидуального (персонифицированного) учета сведений о	Обработка ПДн осуществляется в течение срока действия трудового договора, а также после увольнения работника в течение сроков предоставления необходимой отчетности и в течение срока действия согласия на хранение ПДн. Обработка ПДн осуществляется в течение срока действия согласия на обработку персональных данных, в течение срока действия договора с Учреждением	По истечении сроков обработки ПДн подлежат удалению или, при необходимости, переводу в установленном порядке на архивное хранение

№ п/п	Цели обработки ПДн	Категории субъектов ПДн, перечень обрабатываемых ПДн	Правовые основания обработки ПДн	Сроки обработки ПДн	Действия с ПДн по окончании обработки
		- номер карт-счета; - информация о страховых взносах; - сведения об исчислении страхового стажа; сведения об исчисленных налогах и налоговых вычетах. - дата заключения договора, дата расторжения (исполнения) договора (только для контрагентов); - сведения об отпусках, периодах временной нетрудоспособности (только для работников); - сведения о доходах за отчетный период;	застрахованных лицах, утвержденная приказом МинТРуда от 21.12.2016г. № 766н; Порядок представления в налоговые органы сведений о доходах физических лиц и сообщений о невозможности удержания налога и сумме налога на доходы физических лиц, утвержденный приказом ФНС России от 15.10.2020 г. № ЕД-7-11/753@; Постановление Правления ПФР от 3 июля 2006 г. № 192п «О формах документов индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования и инструкции по их заполнению»; постановление Правления ПФР от 16 января 2014 г. № 2п «Об утверждении формы расчета по начисленным и уплаченным страховым		

№ п/п	Цели обработки ПДн	Категории субъектов ПДн, перечень обрабатываемых ПДн	Правовые основания обработки ПДн	Сроки обработки ПДн	Действия с ПДн по окончании обработки
			взносам на обязательное пенсионное страхование в Пенсионный фонд Российской Федерации и на обязательное медицинское страхование в Федеральный фонд обязательного медицинского страхования плательщиками страховых взносов, производящими выплаты и иные вознаграждения физическим лицам, и Порядка ее заполнения» (вместе с «Порядком заполнения формы расчета по начисленным и уплаченным страховым взносам на обязательное пенсионное страхование в Пенсионный фонд Российской Федерации и на обязательное медицинское страхование в Федеральный фонд обязательного медицинского страхования плательщиками страховых взносов, производящими выплаты		

№ п/п	Цели обработки ПДн	Категории субъектов ПДн, перечень обрабатываемых ПДн	Правовые основания обработки ПДн	Сроки обработки ПДн	Действия с ПДн по окончании обработки
			и иные вознаграждения физическим лицам (форма РСВ-1 ПФР)»; приказ Фонда социального страхования РФ от 26 сентября 2016 г. № 382		
2	Своевременное оповещение при возникновении чрезвычайных ситуаций, организация и ведение гражданской обороны, организация работы по противопожарной безопасности и антитеррористической защищенности	ПДн работников Учреждения, руководителей территориальных органов, руководителей Учреждения: – фамилия, имя, отчество; – номер телефона (рабочего, домашнего, мобильного); – адрес места жительства	Федеральный закон от 12 февраля 1998 г. № 28-ФЗ «О гражданской обороне» (ч. 2 ст. 8, ст. 13); Федеральный закон от 31 декабря 2004 г. № 35-ФЗ «О противодействии терроризму» (ч. 3, ч. 4 ст. 5); Приказ МЧС РФ от 14 ноября 2008 г. № 687 «Об утверждении Положения об организации и ведении гражданской обороны в муниципальных образованиях и организациях»	Обработка ПДн осуществляется с момента поступления сведений от субъекта ПДн до потери актуальности ПДн	По истечении сроков обработки ПДн подлежат удалению или, при необходимости, переводу в установленном порядке на архивное хранение
3	Предоставление социальных услуг	ПДн потребителей социальных услуг и членов их семей: - фамилия, имя, отчество; - дата рождения; - адрес регистрации, адрес фактического проживания; - данные контактного телефона	Федеральный закон № 210-ФЗ от 27.07.2010 «Об организации предоставления государственных и муниципальных услуг», Федеральный закон “Об	Обработка ПДн осуществляется с момента поступления сведений о субъекте ПДн до момента достижения целей обработки ПДн	По истечении сроков обработки ПДн подлежат уничтожению

Цели обработки ПДн	Категории субъектов ПДн, перечень обрабатываемых ПДн	Правовые основания обработки ПДн	Сроки обработки ПДн	Действия с ПДн по окончании обработки
	родственников. - паспортные данные; - сведения о семейном положении; - сведения о трудовой деятельности, - сведения о доходах; -данные пенсионного удостоверения, удостоверения Ветерана Вов, Ветерана труда; -сведения об инвалидности; -сведения об индивидуальной программы реабилитации инвалида; Медицинский полис; - иные персональные данные, необходимые для предоставления социальных услуг	основах социального обслуживания граждан в Российской Федерации" от 28.12.2013 N 442-ФЗ от 28.12.2013; Приказ Министерства труда и социальной защиты населения РФ от 30.07.2014 № 500 н «Об утверждении рекомендаций по определению индивидуальной в социальных услугах получателей социальных услуг»; Закона Ярославской области от 19 декабря 2008 года N 65-з «Социальный кодекс Ярославской области»; Постановление Правительства ЯО от 18.12.2014 № 1335-п «О порядке предоставления социальных услуг поставщиками социальных услуг и признании утратившим силу постановления Администрации области от 04.04.2005 № 46-А»; Приказ департамента		

№ п/п	Цели обработки ПДн	Категории субъектов ПДн, перечень обрабатываемых ПДн	Правовые основания обработки ПДн	Сроки обработки ПДн	Действия с ПДн по окончании обработки
			труда и социальной поддержки населения Ярославской области от 26.05.2015 № 27-15 «Об утверждении административного регламента »		
4	***Ведение реестра потребителей социальных услуг Учреждения***	ПДн потребителей социальных услуг Учреждения: - регистрационный номер; - фамилия, имя, отчество; - дата рождения; - сведения о гражданстве; - сведения об образовании и квалификации по диплому; - паспортные данные; - СНИЛС; - Пенсионное удостоверение; - Данные удостоверения Ветерана Вов; - Данные удостоверения Ветерана труда; - Сведения о трудовой деятельности; - Семейное положение; - Сведения об инвалидности; - Сведения об индивидуальной программе реабилитации инвалида; - Сведения о телефонах родственников; - Сведения о данных	Федеральный закон "Об основах социального обслуживания граждан в Российской Федерации" от 28.12.2013 N 442-ФЗ от 28.12.2013 Приказ Министерства труда и социальной защиты населения РФ от 30.07.2014 № 500 н «Об утверждении рекомендаций по определению индивидуальной в социальных услугах получателей социальных услуг» Закона Ярославской области от 19 декабря 2008 года N 65-з «Социальный кодекс Ярославской области»; Постановление Правительства ЯО от	Обработка ПДн осуществляется в течение срока нахождения потребителя социальных услуг в ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов	По истечении сроков обработки ПДн подлежат удалению или, при необходимости, переводу на архивное хранение

№ п/п	Цели обработки ПДн	Категории субъектов ПДн, перечень обрабатываемых ПДн	Правовые основания обработки ПДн	Сроки обработки ПДн	Действия с ПДн по окончании обработки
		медицинского полиса; - Сведения о данных военного билета; - Справка о размере пенсии	18.12.2014 № 1335-п «О порядке предоставления социальных услуг поставщиками социальных услуг и признании утратившим силу постановления Администрации области от 04.04.2005 № 46-А»; Приказ департамента труда и социальной поддержки населения Ярославской области от 26.05.2015 № 27-15 «Об утверждении административного регламента»		
5	Учет входящей и исходящей корреспонденции и внутренних документов Учреждения	ПД лиц, обратившихся с заявлением в Учреждение: - фамилия, имя, отчество; - адрес места жительства; - контактный телефон; - сведения о документе (реквизиты, наименование)	Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации» от 2 февраля 2006 г. № 59−ФЗ (ч. 2 ст. 8)	Обработка ПД осуществляется в течение периода регистрации документа	По истечении сроков обработки ПДн подлежат удалению или, при необходимости, переводу в установленном порядке на архивное хранение
6	Рассмотрение обращений граждан	ПДн лиц, направивших обращение в Учреждение: - даты получения и регистрации обращения; - фамилия, имя, отчество; - почтовый адрес, если ответ должен быть направлен в письменной форме;	Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (ст. 7; ст. 8; ст. 10); Правила организации хранения,	Обработка ПД осуществляется в течение срока рассмотрения обращения, а также в течение сроков формирования необходимой	По истечении сроков обработки ПД подлежат переводу в установленном порядке на архивное хранение

№ п/п	Цели обработки ПДн	Категории субъектов ПДн, перечень обрабатываемых ПДн	Правовые основания обработки ПДн	Сроки обработки ПДн	Действия с ПДн по окончании обработки
		- адрес электронной почты, если ответ должен быть направлен в форме электронного документа; - текст ответа на обращение -	комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в государственных и муниципальных архивах, музеях и библиотеках, организациях Российской академии наук, утвержденные приказом Министерства культуры и массовых коммуникаций РФ от 03.03.2020г.№310.	отчетности	
7	Ведение кадровой работы	ПДн работников Учреждения: - фамилия, имя, отчество (в том числе прежние, если изменялись, с указанием причины изменения); - дата и место рождения; - сведения о гражданстве (в том числе прежнем, если изменялось); - сведения о владении иностранными языками; - сведения о приеме на работу, увольнении, переводе на другую должность; - реквизиты документа, удостоверяющего личность; - адрес места жительства (фактический и согласно регистрации);	Трудовой кодекс РФ от 30 декабря 2001 г. № 197-ФЗ (ст. 57; ст. 68; ст. 84.1); Правила ведения и хранения трудовых книжек, изготовления бланков трудовой книжки и обеспечения ими работодателей, утвержденные Постановлением Правительства РФ от 16 апреля 2003 г. № 225 (п. 12); Постановление Госкомстата РФ от	Обработка ПДн осуществляется в течение срока осуществления трудовой деятельности	По истечении сроков обработки ПДн подлежат переводу в установленном порядке на архивное хранение

	Цели обработки ПДн	Категории субъектов ПДн, перечень обрабатываемых ПДн	Правовые основания обработки ПДн	Сроки обработки ПДн	Действия с ПДн по окончании обработки
		- сведения о должностном окладе, надбавках, иных выплатах; - сведения о наложении дисциплинарных взысканий; - сведения об отпусках, командировках; - сведения о прохождении аттестации; - сведения о судимости; - сведения о допуске к государственной тайне; - сведения о стаже и предыдущих местах работы (время поступления, ухода, должность с указанием организации); - сведения о государственных наградах, иных знаках отличия; - сведения о семейном положении; - сведения о близких родственниках (степень родства, фамилия, имя, отчество, дата рождения, место учебы, место работы, должность, домашний адрес, - СНИЛС; - ИНН; - данные воинского учета; - сведения об образовании, в том числе о профессиональной переподготовке и повышении квалификации, стажировке;	5 января 2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплате»; приказ Минздрава РФ от 28.01.2021г № 29н «Об утверждении Порядка проведения обязательных предварительных осмотров работников.... И перечня медицинских противопоказаний к осуществлению работ с вредными и (или) опасными факторами, при выполнении которых проводятся предварительные и периодические медицинские осмотры (обследования)…		

№ п/п	Цели обработки ПДн	Категории субъектов ПДн, перечень обрабатываемых ПДн	Правовые основания обработки ПДн	Сроки обработки ПДн	Действия с ПДн по окончании обработки
		ПД работников Учреждения, пребывающих в запасе или подлежащих призыву на военную службу: - фамилия, имя, отчество; - наименование должности; - адрес места жительства; - воинское звание			
8	Исполнение гражданско-правовых договоров, контрактов, заключенных между ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов и ее контрагентами (физическими лицами, индивидуальными предпринимателями) (обеспечение оплаты денежных ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов перед контрагентами)	ПДн физических лиц и индивидуальных предпринимателей — контрагентов ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов и ее контрагентами: - фамилия, имя, отчество или фамилия, инициалы; - ИНН; - сведения о договоре (контракте); - реквизиты счета контрагента; - сведения о расчетах с контрагентом	Бюджетный кодекс РФ от 31 июля 1998 г. № 145-ФЗ (ст. 219; ст. 220.1); Положение Банка России «О правилах осуществления перевода денежных средств» от 29.06.2021 г. № 762п; Федеральный Закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров,работ,услуг для обеспечения государственных и муниципальных нужд» Федеральный Закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»	Обработка ПД осуществляется в течение срока действия договора (контракта) с контрагентом	По истечении сроков обработки ПД подлежат переводу в установленном порядке на архивное хранение

Приложение №4 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Перечень
информационных систем персональных данных
ГБУ СО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов

№ п/п	Наименование ИСПДн	Наличие подключения к сетям	Уровень защищенности ИСПДн
1.	АС « СМЕТА»	есть	1
2.	РКИС	есть	1
3.	СБИС++Электронная отчетность	есть	1
4.	Сбербанк-online	есть	1
5.	УРМ АС « Бюджет»	есть	1
6.	Программный комплекс ViPNet Client	есть	1

77940
5000
73984

Приложение №5 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Перечень должностей,
замещение которых предусматривает осуществление обработки
персональных данных либо осуществление доступа к персональным
данным в ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов

№ п/п	Должность
1	Директор
2	Заместитель директора
3	Главный бухгалтер, бухгалтеры
4	Заведующие отделением ОМ, АД, СМ, ст. медицинские сестры, средний медицинский персонал
5	юрисконсульт
6	Специалист по социальной работе
7	Специалист по кадрам
8	Делопроизводитель
9	Программист
10	Заведующий хозяйством
11	Библиотекарь
12	Специалист по трудотерапии

Приложение №6 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Порядок
доступа работников ГБУ СО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов в помещения, в которых ведется обработка персональных данных

1. Настоящий Порядок разработан в соответствии с законодательством Российской Федерации и определяет порядок доступа в помещения, в которых ведется обработка персональных данных в ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов (далее – Учреждение).

2. Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в Учреждении, определяется локальным актом ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов.

3. Ответственность за обеспечение надлежащего режима доступа в помещения, в которых ведется обработка персональных данных, и обеспечение безопасности персональных данных возлагается на руководителей соответствующих структурных подразделений Учреждения.

4. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Помещения в нерабочее время запираются на ключ. Вскрытие и закрытие помещений осуществляется уполномоченными лицами. По окончании работы уполномоченные лица обязаны убрать бумажные и электронные носители, содержащие персональные данные, в сейфы или закрытые шкафы, отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение; закрыть окна; закрыть двери помещения.

5. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Уполномоченным лицам запрещается передавать ключи от помещений третьим лицам.

6. Нахождение в помещениях Учреждения, в которых ведется обработка персональных данных, лиц, не уполномоченных на обработку персональных данных, возможно только в присутствии специалиста соответствующего структурного подразделения учреждения на время, ограниченное необходимостью решения вопросов, относящихся к компетенции соответствующего структурного подразделения Учреждения.

9. Работники Учреждения не должны покидать помещение, в котором ведется обработка персональных данных, оставляя в нем без присмотра посторонних лиц. После окончания рабочего дня дверь каждого помещения закрывается на ключ.

10. Уполномоченные должностные лица допускаются к информации, содержащей персональные данные, в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими служебных обязанностей. Иные лица допускаются к персональным данным с разрешения директора Учреждения, заместителя директора Учреждения, с соблюдением требований настоящего Порядка.

Приложение №7 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Правила
рассмотрения запросов субъектов персональных данных или их представителей в ГБУ СО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов

1. Общие положения

1.1. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), Трудовым кодексом Российской Федерации и определяют порядок обработки поступающих в ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов (далее - Учреждение) обращений субъектов персональных данных.

2. Права субъектов персональных данных

2.1. В соответствии с действующим законодательством субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

2.1.1. Подтверждение факта обработки персональных данных Учреждением.

2.1.2. Правовые основания и цели обработки персональных данных Учреждением.

2.1.3. Цели и применяемые Учреждением способы обработки персональных данных.

2.1.4. Наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора (контракта) с Учреждением или на основании Федерального закона № 152-ФЗ.

2.1.5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом.

2.1.6. Сроки обработки персональных данных, в том числе сроки их хранения.

2.1.7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ.

2.1.8. Информацию об осуществленной или о предполагаемой трансграничной передаче данных.

2.1.9. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу.

2.1.10. Иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

2.2. Право субъекта персональных данных на доступ к его персональным данным ограничивается в соответствии с федеральными законами, в том числе в случаях, предусмотренных ч.8 ст.14 Федерального закона № 152-ФЗ.

2.3. Субъект персональных данных вправе требовать от Учреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Если субъект персональных данных считает, что Учреждение осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Учреждения в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

2.4. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3. Порядок работы с запросами, уведомлениями и иными обращениями субъектов персональных данных или их представителей

3.1. При поступлении запроса, уведомления или иного обращения субъекта персональных данных или его представителя уполномоченными должностными лицами Учреждения осуществляется его регистрация в журнале учета обращений субъектов персональных данных.

3.2. Уполномоченные должностные лица Учреждения обязаны сообщить в порядке, предусмотренном ст. 14 Федерального закона № 152-ФЗ, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

3.3. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или его персональных данных, субъекту персональных данных или его представителю при их обращении, либо при получении запроса субъекта персональных данных или его представителя, уполномоченные должностные лица Учреждения обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение п. 8 ст. 14 Федерального закона№ 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3.4. Уполномоченные должностные лица Учреждения обязаны предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица Учреждения обеспечивают внесение в них необходимых изменений. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица Учреждения обязаны уничтожить такие персональные данные. Уполномоченные должностные лица Учреждения обязаны уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.5. Уполномоченные должностные лица Учреждения обязаны сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

3.6. Во всем ином, что не урегулировано настоящими Правилами, при работе с запросами, уведомлениями и иными обращениями по вопросам обработки персональных данных уполномоченные должностные лица Учреждения руководствуются действующим законодательством.

Приложение №8 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Обязательство
специалиста ГБУСО ЯО Гаврилов – Ямского
дома – интерната для престарелых и инвалидов
непосредственно осуществляющего обработку персональных данных

Я, _____,
(*Ф.И.О.*)
исполняющий (-ая) должностные обязанности по должности _____
_____,
(*должность, наименование структурного подразделения Учреждения*)
предупрежден (-а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные.

Приступая к обработке персональных данных, добровольно принимаю на себя обязательства:

- не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;
- в случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать об этом непосредственному руководителю;
- не использовать информацию, содержащую персональные данные, с целью получения выгоды;
- беспрекословно и аккуратно выполнять требования положений, порядков, приказов, инструкций, касающихся вопросов обращения с персональными данными и обеспечения их безопасности, выполнять требования правовых актов, регламентирующих вопросы защиты персональных данных;
- немедленно сообщать лицу, ответственному за организацию обработки персональных данных, об утрате или недостаче документов, машинных носителей, черновиков, содержащих персональные данные, удостоверений, ключей от сейфов или помещений, а также о других событиях, которые могут нарушить права граждан при обработке их персональных данных;
- немедленно сообщать лицу, ответственному за организацию обработки персональных данных, о причинах и условиях возможного нарушения порядка обращения с персональными данными или их безопасности, а также обо всех случаях попыток посторонних лиц или организаций получить к ним доступ;
-пресекать действия других лиц, которые могут привести к нарушению безопасности персональных данных
- в случае увольнения, перевода на другую должность, не связанную с обработкой персональных данных, прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей, а также передать лицу, ответственному за организацию обработки персональных данных, все имеющиеся у меня носители персональных данных;

Я ознакомлен(а) с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении

Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Я предупрежден (а), что в случае нарушения данных обязательств могу быть привлечен (а) к дисциплинарной, административной или уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

_____ _____
(фамилия, инициалы) (подпись)

"____" _____ 20__ г.

Приложение №9 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Директору ГБУ СО ЯО Гаврилов – Ямского
дома – интерната для престарелых и инвалидов
от _____
(Ф.И.О. заявителя)
_____
(замещаемая должность)

Типовая форма
согласия работника на обработку персональных данных
в ГБУ СО ЯО Гаврилов – Ямского
дома – интерната для престарелых и инвалидов

Я, _____, проживающий(ая) по
(фамилия, имя, отчество)
адресу _____, основной документ,
удостоверяющий личность (паспорт)
_____
(серия, номер, дата выдачи документа, наименование выдавшего органа)
в соответствии со статьей 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" даю свое согласие
_____
(наименование Учреждения и адрес оператора, получающего
_____
согласие субъекта персональных данных)
на обработку своих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы;
- исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ;
- предоставления сведений в банк для оформления банковской карты и перечисления на нее заработной платы;
- предоставления налоговых вычетов;
- обеспечения моей безопасности;
- контроля количества и качества выполняемой мной работы;
- обеспечения сохранности имущества работодателя

Если мои персональные данные можно получить только у третьей стороны, то я должен(а) быть уведомлен об этом заранее с указанием целей, предполагаемых источников и

способов получения персональных данных. Для обработки указанных данных также должно быть получено мое согласие.

Даю свое согласие ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов в соответствии со статьей 9 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 статьи 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных".

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный);
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством;
- отношение к воинской обязанности;
- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;
- СНИЛС;
- ИНН;
-размещение информации в сети Интернет/информационный сайт учреждения/

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Мне разъяснены мои права и обязанности, связанные с обработкой персональных данных, в том числе, моя обязанность проинформировать оператора в случае изменения моих персональных данных, а также мое право в любое время отозвать свое согласие путем направления соответствующего письменного заявления оператору.

Я вправе отозвать данное согласие на обработку своих персональных данных, письменно уведомив об этом оператора.

В случае моего отзыва на обработку своих персональных данных в письменной форме (если иной порядок отзыва не предусмотрен действующим законодательством) оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных оператор обязан уведомить меня.

_____

(подпись субъекта персональных данных)

_____

(число, месяц, год)

Приложение №10 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Директору ГБУ СО ЯО Гаврилов – Ямского
дома – интерната для престарелых и инвалидов
от _____

(Ф.И.О. заявителя)

_____

Типовая форма
согласия получателя социальных услуг на обработку персональных данных
в ГБУСО ЯО Гаврилов – Ямского
дома – интерната для престарелых и инвалидов

Я, _____, проживающий(ая) по
(фамилия, имя, отчество)
адресу _____, основной документ,
удостоверяющий личность (паспорт)
_____
(серия, номер, дата выдачи документа, наименование выдавшего органа)
в соответствии со статьей 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" даю свое согласие

_____
(наименование Учреждения и адрес оператора, получающего
_____
согласие субъекта персональных данных)
на обработку своих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, в целях:

- обеспечения моих прав и свобод как человека и гражданина, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
- в целях обеспечения моей личной безопасности
- предоставления социальных услуг, оптимального исполнения своих обязанностей Учреждения передо мной;

В процессе предоставления учреждением мне социальных услуг, я предоставляю право передавать мои персональные данные, содержащие врачебную тайну , другим должностным лицам Учреждения в моих интересах.

Если мои персональные данные можно получить только у третьей стороны, то я должен(а) быть уведомлен об этом заранее с указанием целей, предполагаемых источников и способов получения персональных данных. Для обработки указанных данных также должно быть получено мое согласие.

Даю свое согласие ГБУСО ЯО Гаврилов –Ямского дома – интерната для престарелых и инвалидов в соответствии со статьей 9 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 статьи 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных".

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;

- паспортные данные;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона родственников (домашний, мобильный);
- сведения о профессиональной деятельности;
- семейное положение, сведения о составе семьи,
- сведения о трудовом стаже,
- СНИЛС;
-данные о состоянии моего здоровья, заболеваниях при условии, что их обработка осуществляется лицом, профессионально занимающимся социальной деятельностью;
- даты и номера индивидуальной программы предоставления социальных услуг;
-сведения о размере моей пенсии

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Мне разъяснены мои права и обязанности, связанные с обработкой персональных данных, в том числе, моя обязанность проинформировать оператора в случае изменения моих персональных данных, а также мое право в любое время отозвать свое согласие путем направления соответствующего письменного заявления оператору.

Я вправе отозвать данное согласие на обработку своих персональных данных, письменно уведомив об этом оператора.

_____

(подпись субъекта персональных данных)

_____

(число, месяц, год)

Приложение №11 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159
Директору ГБУ СО ЯО Гаврилов – Ямского
дома – интерната для престарелых и инвалидов
от _____
Ф.И.О.
Место жительства_____
_____
Тел_____

Типовое согласие работника на обработку персональных данных, разрешенных субъектом персональных данных для распространения в ГБУ СО ЯО Гаврилов - Ямском доме – интернате для престарелых и инвалидов

Настоящим я,_____, руководствуясь статьей 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», заявляю о согласии на распространение ГБУ СО ЯО Гаврилов-Ямским домом-интернатом для престарелых и инвалидов моих персональных данных в следующем порядке:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да/нет)	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Условия и запреты	Дополнительные условия
персональные данные	фамилия				
	имя				
	отчество				
	адрес регистрации/ жительства				
	паспортные данные				
	дата рождения/число, месяц, год				
	место рождения				
	семейное положение				
	образование				
	профессия				
	ИНН, СНИЛС				
специальные категории персональных данных	состояние здоровья				
	сведения о судимости				
	сведения о наличии инвалидности				
	сведения о воинском учёте				
биометрические персональные данные	цветное цифровое фотографическое изображение лица				

Сведения об информационных ресурсах Оператора, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
Любая накопленная информация об окружающей действительности, зафиксированная на материальных носителях, обеспечивающих передачу информации во времени и пространстве между потребителями для решения конкретных задач.	Предоставление сведений неограниченному кругу лиц

Настоящее согласие дано мной добровольно и действует до отзыва в установленном законом порядке.

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования Оператор обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

«_____» _____ _____ года _____(Ф.И.О.)

Приложение №12 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Типовая форма
разъяснения субъекту персональных данных юридических
последствий отказа предоставить свои персональные данные

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)
проживающий(ая) по адресу _____
_____,
(адрес места жительства субъекта персональных данных)
основной документ, удостоверяющий личность _____
_____
(наименование и номер основного документа, удостоверяющего личность,
сведения о дате выдачи указанного документа и выдавшем его органе)
в соответствии с ч.2 ст. 18 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» настоящим подтверждаю, что мне разъяснены юридические последствия отказа предоставить свои персональные данные.

В соответствии со статьями 57,65 Трудового кодекса Российской Федерации и «Правилами обработки персональных данных в ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов», утвержденными приказом директора _____ от «__» _____ 201_ г. № _____, определён перечень персональных данных, которые субъект персональных данных обязан предоставить уполномоченным лицам в связи с заключением трудового договора и начислением заработной платы.

Я предупрежден (-а), что в случае отказа предоставить свои персональные данные уполномоченным лицам со мной не может быть заключен трудовой договор.

_____ _____
подпись Ф.И.О.

"___" _____ 20__ г.

Приложение №13 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Типовая форма
разъяснения субъекту персональных данных юридических
последствий отказа предоставить свои персональные данные
(для получателей социальных услуг)

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)
проживающий(ая) по адресу _____
_____,
(адрес места жительства субъекта персональных данных)
основной документ, удостоверяющий личность _____
_____
(наименование и номер основного документа, удостоверяющего личность,
сведения о дате выдачи указанного документа и выдавшем его органе)
в соответствии с ч.2 ст. 18 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» настоящим подтверждаю, что мне разъяснены юридические последствия отказа предоставить свои персональные данные.

В соответствии с «Правилами обработки персональных данных в ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов», утвержденными приказом директора _____ от «__» _____ 201_ г. № _____, определён перечень персональных данных, которые субъект персональных данных обязан предоставить уполномоченным лицам в связи с заключением договора на предоставление социальных услуг.

Я предупрежден (-а), что в случае отказа предоставить свои персональные данные уполномоченным лицам со мной не может быть заключен договор на *предоставление социальных услуг*, в связи с чем предоставление социальных услуг не может быть выполнено в полном объеме.

_____ _____
подпись Ф.И.О.

"___" _____ 20__ г.

Приложение №14 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Порядок
обработки конфиденциальной информации в автоматизированных информационных системах ГБУСО ЯО Гаврилов – Ямского дома – интерната для престарелых и инвалидов

1.При обработке конфиденциальной информации в автоматизированных информационных системах (далее – АИС) Учреждения пользователи обязаны:

- знать и соблюдать ограничения, связанные с обработкой конфиденциальной информации (далее – ОКИ);
- знать и соблюдать правила работы с персональными компьютерами (далее – ПК) и другими средствами вычислительной техники, правила работы в локально-вычислительных сетях;
- знать и соблюдать меры по защите конфиденциальной информации (далее – ЗКИ) в АИС;
- знать и исполнять требования эксплуатационной документации на АИС;
- при работе с АИС выполнять только служебные задания;
- при работе с машинными носителями использовать только учтенные в установленном порядке машинные носители (дискеты, флэш-карты и т. п.);
- перед началом работы на ПК проверить свои рабочие папки на жестком магнитном диске, рабочие съёмные машинные носители информации на отсутствие вирусов с помощью штатных средств антивирусной защиты, убедиться в исправности ПК. При необходимости использования съёмных машинных носителей, поступивших из других сторонних организаций, прежде всего, провести проверку этих носителей на отсутствие вирусов. При сообщениях тестовых программ о появлении вирусов немедленно прекратить работу, доложить специалисту по компьютерным вопросам (далее - Программисту) и своему непосредственному руководителю;
- выполнять предписания Программиста;
- сохранять в тайне свой индивидуальный пароль, периодически изменять его и не сообщать другим лицам. Вводить пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;
- располагать дисплей таким образом, чтобы исключить несанкционированное ознакомление лиц, не допущенных к обработке конфиденциальной информации, с отображаемыми сведениями;
- учет, размножение, обращение печатных материалов, содержащих сведения конфиденциального характера и имеющих гриф «Для служебного пользования», проводить в соответствии с требованиями Положения о порядке обращения со служебной информацией ограниченного распространения;
- при обнаружении различных неисправностей в работе компьютерной техники или локально-вычислительной сети, недокументированных свойств в программном обеспечении, несоответствии номеров на аппаратных средствах сообщить непосредственному руководителю и Программисту.

2. Пользователю при работе запрещается:

- предоставлять свой ПК в пользование другим работникам, посторонним лицам, кроме случаев, связанных с техническим обслуживанием техническими специалистами, осуществляющими эксплуатацию средств информатизации или осуществлением контрольных функций Программистом;
- передавать другим лицам персональные пароли;
- самостоятельно устанавливать компьютерные программы на свой ПК;
- перенастраивать программное обеспечение ПК;
- самостоятельно вскрывать ПК и другие средства вычислительной техники;
- запускать на своем ПК любые системные или прикладные программы, кроме установленных техническими специалистами, осуществляющими эксплуатацию средств информатизации;
- оставлять включенным без присмотра свой ПК, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было в доступном для других лиц месте свое персональное устройство идентификации (при наличии), машинные носители и распечатки, содержащие конфиденциальную информацию;
- запрашивать и получать из сети «Интернет» материалы развлекательного характера (игры, клипы и т. д.), кроме случаев их использования в служебных целях;
- запрашивать и получать из сети «Интернет» программные продукты, базы данных, обновления программных продуктов и баз данных, кроме случаев, связанных с исполнением служебных обязанностей;
- использовать в личных целях сведения конфиденциального характера, ставшие известными вследствие выполнения служебных обязанностей.

3.Защита информации от специальных программ вирусов

1. В целях съема информации, ее разрушения, нарушения нормального функционирования СВТ и АС создаются специальные программы-вирусы.
2. Пути проникновения вирусов в СВТ и АС:
- проникновение вирусов на рабочие станции при использовании на рабочей станции инфицированных файлов с переносимых источников (компакт-диски и т.п.);
- заражение вирусами с помощью инфицированного программного обеспечения, полученного из Интернет и проинсталлированного на локальной рабочей станции;
- проникновение вирусов при подключении к локальной вычислительной сети (далее – ЛВС) инфицированных рабочих станций удаленных или мобильных пользователей;
- заражение вирусами с удаленного сервера, подсоединенного к ЛВС и обменивающегося инфицированными данными с ее серверами;
- распространение электронной почты, содержащей в приложениях файлы Excel и Word, инфицированные макровирусами.
3. Организация антивирусной защиты информации на объектах информатизации достигается путем:
- внедрения и применения средств антивирусной защиты информации;
- обновления баз данных средств антивирусной защиты информации;
- спланированных действий должностных лиц при обнаружении заражения информационных ресурсов программными вирусами.
4. Система антивирусной защиты должна разрабатываться с учетом особенностей конкретных ЛВС и, в общем случае, должна включать в себя:
- антивирусную защиту рабочих станций;
- возможность автоматического обновления антивирусных баз и версий.
5. Порядок применения средств антивирусной защиты устанавливается с учетом необходимости выполнения следующих требований:
а) операторами (пользователями) информационной системы:
- периодическая проверка жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе съемных дисков перед началом работы с ними на отсутствие программных вирусов;
- внеплановая проверка магнитных носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

б) специалистом по компьютерному обеспечению, осуществляющего эксплуатацию объектов информатизации:
- обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации машинных носителей информации, информационных массивов, программных средств общего и специального назначения;
- восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

6. К использованию допускаются только лицензированные антивирусные средства, централизованно закупленные у разработчиков указанных средств либо их официальных дилеров. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

7. Порядок применения средств антивирусной защиты, учитывающий особенности объекта информатизации и выполняемых на данном объекте работ, определяется инструкцией по антивирусной защите конфиденциальной информации, разрабатываемой совместно подразделением, осуществляющим эксплуатацию объектов информатизации, и работником по защите информации.

В общем случае инструкция по антивирусной защите конфиденциальной информации должна включать в себя разделы, определяющие порядок защиты конфиденциальной информации на рабочих станциях ЛВС.

8. При обнаружении программных вирусов пользователь обязан прекратить все работы на ПЭВМ, поставить в известность Программиста, осуществляющего эксплуатацию объектов информатизации, и совместно с его специалистами принять меры к локализации и удалению вирусов с помощью имеющихся антивирусных средств защиты.

При функционировании ПЭВМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

Ликвидация последствий воздействия программных вирусов осуществляется подготовленными представителями подразделения, осуществляющего эксплуатацию объектов информатизации.

Программные средства общего и специального назначения объекта информатизации, осуществляющего обработку служебной информации ограниченного доступа, подлежат обязательной переустановке с рабочих копий эталонных дискет независимо от результатов по удалению выявленных программных вирусов имеющимися средствами антивирусной защиты.

4.Защита информации от несанкционированного доступа

Защита доступа к компьютеру осуществляется программными, программно-аппаратными средствами и чисто аппаратными комплексами. Это обеспечивает:
- наличие в компьютерах специалистов только той информации и тех программ, которые необходимы работникам для повседневной деятельности;
- постоянный контроль за конфиденциальной информацией, при котором всегда можно узнать, кто и когда к ней обратился;
- ознакомление с историей работы пользователя на компьютере.

5. Инструкция по работе со съемными носителями, содержащими персональные данные

5.1. Съемными накопителями являются:
- USB-накопители (флеш-диски);
- съемные накопители на жестких магнитных дисках (НЖМД);
- дискеты;
- диски;
- и т.д.

5.2. Съемные накопители применяются для хранения электронных баз данных персональных данных в сейфах или других местах хранения, передачи персональных данных в вышестоящие организации, в филиалы оператора или в сторонние организации. Так же съемные накопители могут служить для переноса персональных данных на автономное рабочее место ИСПДн.

5.3. Перед использованием съемный носитель должен быть проверен антивирусными средствами на наличие вирусов.

5.4. Хранение съемных накопителей должно осуществляться в местах не доступных для посторонних лиц, также для должностных лиц оператора, не имеющих полномочий на обработку персональных данных для выполнения должностных обязанностей.

5.5. Учет съемных накопителей должен вестись в Журнале учета (Приложение 1).

5.6. Уничтожение съемных носителей персональных данных должно проводиться комиссионно с оформлением Акта уничтожения.

Приложение 1

Форма Журнала учета съемных носителей

№	Уч.№ носителя	Назначение носителя	Дата начала использования носителя	Дата уничтожения носителя	№ и дата Акта уничтожения носителя	Подпись АБ

Приложение №15 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Требования
к защите персональных данных при их обработке в информационных системах персональных данных в ГБУ СО ЯО Гаврилов – Ямском доме-интернате для престарелых и инвалидов

1. Настоящий документ устанавливает требования к защите персональных данных в ГБУ СО ЯО Гаврилов – Ямском доме-интернате для престарелых и инвалидов (далее по тексту - Учреждение) при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных.

2. Безопасность персональных данных субъектов Учреждения при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных".

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3. Безопасность персональных данных при их обработке в информационной системе Учреждения обеспечивает оператор этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором (Учреждением) в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных".

5. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья субъектов персональных данных.

Информационная система Учреждения является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора (Учреждения), если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

6. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

8. При обработке персональных данных в информационных системах устанавливаются уровни защищенности персональных данных субъектов Учреждения.

9. Необходимость обеспечения уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

10. Для обеспечения уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система Учреждения, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

11. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

12. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных

пунктом 14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

13. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Приложение №16 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

Правила оценки возможного вреда субъектам персональных данных в ГБУ СО ЯО Гаврилов-Ямского дома-интерната для престарелых и инвалидов

1.Общие требования

1.1. Настоящие Правила оценки возможного вреда субъектам персональных данных и принятие мер по его предотвращению (далее – Правила) определяют порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона 152- ФЗ « О персональных данных», и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом 152- ФЗ « О персональных данных».

2.Основные понятия

2.1. В настоящих Правилах используются основные понятия:
2.1.1. Информация - сведения (сообщения, данные) независимо от формы их представления.
2.1.2. Безопасность информации-состояние защищенности информации, при котором обеспечены её конфиденциальность, доступность и целостность.
2.1.3. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.
2.1.4. Целостность информации - состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.
2.1.5. Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут регулировать их беспрепятственно.
2.1.6. Убытки – расходы, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а так же неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.
2.1.7. Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими по принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.
2.1.8. Оценка возможного вреда – определение уровня вреда на основании учёта причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

3. Цель правил

2.1.Настоящие правила приняты в целях обеспечения соответствия требований Федерального закона152- ФЗ « О персональных данных».

4.Область применения правил

3.1.Настоящий документ обязаны знать и использовать в работе члены Комиссии по обеспечению персональных данных.

5. Методика оценки возможного вреда субъектам персональных данных.

5.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а так же от иных неправомерных действий в отношении персональных данных.
5.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:
5.3. Неправомерное предоставление, распространение и копирование персональных являются нарушением конфиденциальности персональных данных.
5.4. Неправомерное уничтожение и блокирование персональных данных является нарушением целостности персональных данных.
5.5. Неправомерное изменение персональных данных является нарушением целостности персональных данных.
5.6.Нарушение права субъекта требовать от оператора уничтожения его персональных данных, их блокировки является нарушением целостности информации.
5.7. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных.
5.8. Обработка персональных данных, выходящая за рамки установленных целей обработки, в объёме больше необходимого для достижения установленных целей и законных и дольше установленных сроков является нарушением конфиденциальности персональных данных.
5.9. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных.
5.10. Принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных лил непредусмотренные федеральным законами, является нарушением конфиденциальности персональных данных.
5.2.1. Субъекту персональных данных может быть причинен ущерб в форме:
5.2.3. Убытков- расходов, которые лицо, чье право нарушено, понесло или должно понести для восстановления нарушенного права, утраты или повреждения его имущества(реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.
5.2.4. Морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные ценности, а так же в других случаях предусмотренные законом.
5.2.5. В оценке возможного вреда в ГБУ СО ЯО Гаврилов - Ямском доме интернате для престарелых и инвалидов исходит из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:
5.2.6. Низкий уровень возможного вреда- последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных.
5.2.7. Средний уровень возможного вреда- последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшие убытки и моральный вред, либо только нарушение доступности персональных данных повлекшие убытки и моральный вред, либо нарушение конфиденциальности персональных данных.
5.2.8. Высокий уровень возможного вреда - во всех остальных случаях.

6. Порядок проведения оценки возможного вреда субъекту персональных данных

6.1. Оценка возможного вреда субъекту персональных данных осуществляется лицом, ответственным в ГБУ СО ЯО Гаврилов-Ямском доме- интернате для престарелых и инвалидов за организацию обработки персональных данных, в соответствии с методикой

Оценка вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых мер

№ п/п	Требования закона « О персональных данных» которые могут быть нарушены	Возможные нарушение безопасности информации и причинённый субъекту вред	Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных
1.	Порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке,	1. Убытки и моральный вред. 2. Целостность 3. Доступность 4. Конфиденциальность	Средний	В соответствии с законодательством в области защиты информации и документами, определяющими политику в отношении

	необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных			обработки персональных данных в учреждении
2.	Порядок и условия применения средств защиты информации	1. Убытки и моральный вред. 2. Целостность 3. Доступность 4. Конфиденциальность	Средний	В соответствии с технической документацией на систему защиты и утвержденной политикой учреждения
3.	Состояние учета съемных носителей персональных данных	1. Убытки и моральный вред. 2. Целостность 3. Доступность 4. Конфиденциальность	Низкий	Журнал по учету съемных носителей информации
4.	Соблюдение правил доступа к персональным данным	1. Убытки и моральный вред. 2. Целостность 3. Доступность 4. Конфиденциальность	Высокий	В соответствии с правилами доступа к персональным данным установленными в учреждении
5.	Наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер	1. Убытки и моральный вред. 2. Целостность 3. Доступность 4. Конфиденциальность	Средний	Мониторинг средств защиты информации на наличие фактов доступа к ним.
6.	Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	1. Убытки и моральный вред. 2. Целостность 3. Доступность 4. Конфиденциальность	Низкий	Применение резервного копирования
7.	Осуществление мероприятий по обеспечению целостности персональных данных	1. Убытки и моральный вред. 2. Целостность 3. Доступность 4. Конфиденциальность	Низкий	Организация доступа к техническим и программным средствам

Приложение №17 к приказу
ГБУ СО ЯО Гаврилов – Ямского дома – интерната
для престарелых и инвалидов
от 20.07.2022г. № 159

ПОЛОЖЕНИЕ
о комиссии по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных ГБУ СО ЯО Гаврилов - Ямского дома – интерната для престарелых и инвалидов

1. Общие положения

1.1. Комиссия по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее Комиссия) создается в целях работы в области обеспечения информационной безопасности в рамках Политики ГБУСО ЯО Гаврилов - Ямского дома – интерната для престарелых и инвалидов в отношении обработки персональных данных.

1.2. Состав Комиссии является постоянным и утверждается приказом директора.

1.3. Председателем Комиссии является лицо, ответственное за организацию обработки персональных данных в учреждении. Членами Комиссии могут являться руководители структурных подразделений, специалисты учреждения, имеющие соответствующую компетенцию в работе по защите персональных данных.

2. Основные функции Комиссии

Основными функциями Комиссии являются:

2.1. Разработка предложений по вопросам обеспечения информационной безопасности и защите персональных данных сотрудников учреждения и получателей услуг.

2.2. Контроль обеспечения безопасности персональных данных при их обработке с использованием средств автоматизации и без использования средств автоматизации.

2.3. Осуществление периодических проверок условий обработки персональных данных.

2.4. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2.5. Разработка матрицы доступа к персональным данным.

2.6. Разработка планов мероприятий по защите персональных данных в учреждении.

2.7. Организация и проведение процедуры уничтожения персональных данных.

2.8. Подготовка предложений по обеспечению необходимого уровня информационной безопасности в учреждении.

3. Порядок работы Комиссии

3.1. Деятельность Комиссии организуется и проводится в соответствии с Планом работы Комиссии в учреждении.

3.2. По итогам проверки составляется Протокол комиссии по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных ГБУ СО ЯО Гаврилов-Ямского дома-интерната для престарелых и инвалидов.

3.3. Приготовленные к уничтожению персональные данные (их носители), уничтожаются в учреждении по мере накопления.

3.4. 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.

3.5. Уничтожение персональных данных делится на два вида:
- плановое уничтожение конфиденциальной информации осуществляется Комиссией по мере необходимости.
- экстренное уничтожение конфиденциальной информации. Уничтожение производится экстренно под воздействием неблагоприятных событий.
3.6. В зависимости от типа носителя информации (бумажный или электронный) выделяют два способа уничтожения персональных данных:
- физическое уничтожение носителя;
- уничтожение информации с носителя.
3.7. Персональные данные, обрабатываемые и хранящиеся в учреждении, подлежат уничтожению в случае:
- достижения цели обработки персональных данных или утраты необходимости в их обработке;
- выявления неправомерных действий с персональными данными и невозможности устранения допущенных нарушений;
- отзыва субъектом персональных данных согласия на обработку своих персональных данных;
- истечения срока хранения персональных данных.
3.8. Организация уничтожения персональных данных осуществляется с соблюдением следующих условий:
3.8.1. Операторы, осуществляющие обработку персональных данных, производят отбор носителей персональных данных подлежащих уничтожению и передают их Комиссии.
3.8.2. Комиссия производит проверку персональных данных, подлежащих уничтожению с полистным просмотром.
3.8.3. При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.
3.9. После уничтожения Комиссией оформляется Акт уничтожения носителей персональных данных.

4. Права Комиссии

Комиссия вправе:
4.1. Знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на нее задач.
4.2. Проводить периодические проверки условий обработки персональных данных в учреждении.
4.3. Вносить предложения руководству учреждения по совершенствованию существующей системы защиты информации и персональных данных.
4.4. Привлекать, по согласованию с директором, к работе по созданию и совершенствованию системы защиты информации и персональных данных других специалистов учреждения.