УТВЕРЖДАЮ

Главный врач
ОГБУЗ «Чухломская ЦРБ»

_____ Одинцов А.А.
«25» марта 2024 г.

Политика обработки и защиты персональных данных
ОГБУЗ «Чухломская ЦРБ»

1. Общие положения

1.1. Настоящая Политика обработки и защиты персональных данных (далее – Политика) определяет порядок обработки персональных данных (далее – ПДн) и меры по обеспечению безопасности персональных данных в ОГБУЗ «Чухломская ЦРБ» с целью защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, гарантируемых Конституцией.

1.2. Настоящая Политика является локальным нормативным актом ОГБУЗ «Чухломская ЦРБ» (далее – Организация) и разработана в соответствии с Федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных» и от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; постановлениями Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; приказом ФСТЭК от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», главы 14 ТК РФ.

1.3. Настоящая Политика раскрывает принципы, порядок и условия обработки ПДн физических лиц при обращении за медицинской помощью в Организацию.

Кроме того, обработка ПДн осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (гл. 14 ТК), в связи с реализацией своих прав и обязанностей как юридического лица.

1.4. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.5. Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Организации по адресу: г. Чухлома, ул. Калинина, д. 64, электронная версия Политики – на сайте по адресу: https://chuhlomacrb.dzo44.ru/

1.7. Персональные данные обрабатывают с использованием средств автоматизации и без них.

1.8. Организация до начала обработки персональных данных обязана уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных согласно частям 1 и 3 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.9. Приказом руководителя Организации от 14.11.2023 № 22ответственным лицом за организацию обработки персональных данных в соответствии с пунктом 1 статьи 18.1 Закона № 152-ФЗ назначен инженер по работе с персональными данными Григорьев Е.В.

2. Термины и принятые сокращения

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

2.2. Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом.

2.3. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

2.4.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.

2.5. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

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

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

2.9. 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.

2.10.Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

2.12.Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

2.13.Медицинская деятельность – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

2.14. Лечащий врач – врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Организация руководствуется следующими принципами:

3.2.1. Законность – защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн.

3.2.2. Системность – обработка ПДн в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.

3.2.3. Комплексность – защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты.

3.2.4. Непрерывность – защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ.

3.2.5. Своевременность – меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки.

3.2.6. Преемственность и непрерывность совершенствования – модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации.

3.2.7. Персональная ответственность – ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн.

3.2.8. Минимизация прав доступа – доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей.

3.2.9. Гибкость – обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых ПДн.

3.2.10. Специализация и профессионализм – реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт.

3.2.11. Эффективность процедур отбора кадров – кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн.

3.2.12. Наблюдаемость и прозрачность – меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль.

3.2.13. Непрерывность контроля и оценки – устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

3.3. Безопасность ПДн, обрабатываемых Организацией, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты ПДн.

3.4. Меры по обеспечению безопасности ПДн включают в себя, в частности:

- назначение ответственного за организацию обработки ПДн;
- издание локальных правовых актов, регулирующих права и обязанности оператора ПДн, описывающих систему мер по защите ПДн, определяющих доступ к информационным системам ПДн;
- определение угроз безопасности ПДн при их обработке в информационных системах ПДн;
- применение методов (способов) защиты информации;
- оценку эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;
- учет машинных носителей ПДн;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к ПДн, обрабатываемым в информационной системе ПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в информационной системе ПДн;
- контроль принимаемых мер по обеспечению безопасности ПДн и уровня защищенности информационных систем ПДн.

3.5. В Организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПНд уничтожаются или обезличиваются.

3.6. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

4. Порядок обработки персональных данных в Организации

4.1. Категории ПДн

В Организации обрабатываются следующие ПДн:

- фамилия, имя, отчество (при наличии), а также прежние фамилия, имя, отчество (при наличии), дата и место их изменения (в случае изменения);
- пол;

- дата (число, месяц, год) и место рождения;
- фотографическое изображение;
- сведения о гражданстве;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- страховой номер индивидуального лицевого счета (СНИЛС);
- идентификационный номер налогоплательщика (ИНН);
- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;
- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);
- сведения об образовании и (или) квалификации или наличии специальных знаний (в том числе наименование образовательной и (или) иной организации, год окончания, уровень образования, квалификация, реквизиты документа об образовании, обучении);
- информация о владении иностранными языками;
- сведения об отношении к воинской обязанности, о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документа, наименование органа, выдавшего его);
- сведения о трудовой деятельности, а также информация о предыдущих местах работы, периодах и стаже работы;
- сведения, содержащиеся в документах, дающих право на пребывание и трудовую деятельность на территории РФ (для иностранных граждан, пребывающих в РФ);
- сведения, содержащиеся в разрешении на временное проживание, разрешении на временное проживание в целях получения образования (для иностранных граждан, временно проживающих в РФ), виде на жительство (для иностранных граждан, постоянно проживающих в РФ);
- сведения о доходах, обязательствах по исполнительным документам;
- номера расчетного счета, банковской карты;
- сведения о состоянии здоровья (для отдельных категорий работников);
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (для отдельных категорий работников);
- иные персональные данные, содержащиеся в документах, представление которых предусмотрено законодательством, если обработка этих данных соответствует цели обработки, предусмотренной п. 3.1 настоящей Политики;
- иные персональные данные, которые работник пожелал сообщить о себе и обработка которых соответствует цели обработки, предусмотренной п. 3.1 настоящей Политики.

4.2. Цели обработки ПДн:

4.2.1. Обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с законами от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан Российской

Федерации», от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств» и от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства от 04.10.2012 № 1006.

4.2.2. Осуществление трудовых отношений.

4.2.3. Осуществление гражданско-правовых отношений.

4.3. Категории субъектов ПДн

4.3.1. В Организации обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с Организацией в трудовых отношениях;
- физические лица, являющие близкими родственниками сотрудников Организации;
- физические лица, уволившиеся из Организации;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с Организацией в гражданско-правовых отношениях;
- физические лица, обратившиеся в Организацию за медицинской помощью.

4.4. ПДн, обрабатываемые Организацией

4.4.1. В Организации обрабатываются ПДн:

- полученные при осуществлении трудовых отношений;
- полученные для осуществления отбора кандидатов на работу в Организацию;
- полученные при осуществлении гражданско-правовых отношений;
- полученные при оказании медицинской помощи.

Полный список ПДн представлен в перечне ПДн, утвержденном главным врачом Организации.

4.3. Получение ПДн

4.3.1. Все ПДн следует получать от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

4.3.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.3.3. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн в Организации осуществляются посредством:

- получения оригиналов документов либо их копий (трудовая книжка, медицинское заключение, характеристика и т. д.);
- копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и т. д.);
- внесения сведений в учетные формы на бумажных и электронных носителях;
- создания документов, содержащих персональные данные, на бумажных и электронных носителях;
- внесения ПДн в информационные системы ПДн.

4.4. Обработка ПДн

4.4.1. Обработка персональных данных осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, обезличивания, блокирования, удаления, уничтожения персональных данных, в том числе с помощью средств вычислительной техники.

4.4.2. До начала обработки ПДн Организация обязана уведомить Роскомнадзор о намерении осуществлять обработку ПДн.

4.4.3. Обработка персональных данных в Организации выполняется следующими способами:

- неавтоматизированная обработка ПДн;
- автоматизированная обработка ПДн с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка ПДн.

4.4.4. Обработка персональных данных осуществляется:

4.4.4.1. С согласия субъекта пДн на обработку его ПДн, если иное не предусмотрено законодательством в области ПДн.

4.4.4.2. В случаях, когда обработка ПДн необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей.

4.4.4.3. В случаях, когда осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе (далее – ПДн, сделанные общедоступными субъектом ПДн).

4.4.4.4. Обработка ПДн, разрешенных субъектом ПДн для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 Федерального закона 27.07.2006 № 152-ФЗ. Согласие на обработку таких ПДн оформляется отдельно от других согласий на обработку ПДн. Согласие предоставляется субъектом ПДн лично либо в форме электронного документа, подписанного электронной подписью, с использованием информационной системы Роскомнадзора.

4.4.4.5. Обработка биометрических ПДн допускается только при наличии письменного согласия субъекта ПДн. Исключение составляют ситуации, предусмотренные ч. 2 ст. 11 Федерального закона 27.07.2006 № 152-ФЗ.

4.4.5. В Организации для обработки ПДн используются следующие информационные системы:

- корпоративная электронная почта;
- система электронного документооборота;
- система поддержки рабочего места пользователя;
- система нормативно-справочной информации;
- система управления персоналом;
- система контроля за удаленным доступом;
- информационный портал.

4.4.6. Передача (распространение, предоставление, доступ) ПДн субъектов ПДн осуществляется в случаях и в порядке, предусмотренных законодательством в области ПДн и настоящей Политикой.

4.4.7. Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

4.5. Хранение ПДн

4.5.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.5.2. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. Исключение – случаи, когда срок хранения ПДн установлен федеральным законом, договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект ПДн.

4.5.3. ПДн на бумажных носителях хранятся в Организации в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения, утв. приказом Росархива от 20.12.2019 № 236).

4.5.4. Срок хранения ПДн, обрабатываемых в информационных системах ПДн, соответствует сроку хранения ПДн на бумажных носителях.

4.5.5. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа (регистратура).

4.5.6. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.5.7. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.6. Прекращение обработки ПДн

4.6.1. Обработка ПДн в Организации прекращается в следующих случаях:

- при выявлении факта неправомерной обработки ПДн. Срок прекращения обработки – в течение трех рабочих дней с даты выявления такого факта;
- при достижении целей обработки ПДн (за некоторыми исключениями);
- по истечении срока действия или при отзыве субъектом ПДн согласия на обработку его ПДн (за некоторыми исключениями), если в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ их обработка допускается только с согласия;
- при обращении субъекта ПДн к Организации с требованием о прекращении обработки ПДн (за исключением случаев, предусмотренных ч. 5.1 ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ). Срок прекращения обработки – не более 10 рабочих дней с даты получения требования (с возможностью продления не более чем на пять рабочих дней, если направлено уведомление о причинах продления).

4.7. Блокирование и уничтожение ПДн

4.7.1. Организация блокирует ПДн в порядке и на условиях, предусмотренных законодательством в области ПДн.

4.7.2. При достижении целей обработки ПДн или в случае утраты необходимости в достижении этих целей ПДн уничтожаются либо обезличиваются. Исключение может предусматривать федеральный закон.

4.7.3. Незаконно полученные ПДн или те, которые не являются необходимыми для цели обработки, уничтожаются в течение семи рабочих дней со дня представления субъектом ПДн (его представителем) подтверждающих сведений.

4.7.4. ПДн, обработка которых прекращена из-за ее неправомерности и правомерность обработки которых невозможно обеспечить, уничтожаются в течение 10 рабочих дней с даты выявления факта неправомерной обработки.

4.7.5. ПДн уничтожаются в течение 30 дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект ПДн, иным соглашением между ним и Организацией либо если Организация не вправе обрабатывать ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами.

4.7.6. При достижении максимальных сроков хранения документов, содержащих ПДн, ПДн уничтожаются в течение 30 дней.

4.7.7. ПДн уничтожаются (если их сохранение не требуется для целей обработки ПДн) в течение 30 дней с даты поступления отзыва субъектом ПДн согласия на их обработку. Иное может предусматривать договор, стороной которого

(выгодоприобретателем или поручителем по которому) является субъект ПДн, иное соглашение между ним и Организацией. Кроме того, ПДн уничтожаются в указанный срок, если Организация не вправе обрабатывать их без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами.

4.7.8. Отбор материальных носителей (документы, жесткие диски, флеш-накопители и т.п.) и (или) сведений в информационных системах, содержащих ПДн, которые подлежат уничтожению, осуществляют подразделения Организации, обрабатывающие ПДн.

4.7.9. Уничтожение персональных данных осуществляет комиссия, созданная приказом руководителя Организации.

4.7.9.1. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих ПДн, которые подлежат уничтожению.

4.7.9.2. Уничтожение документов (носителей), содержащих ПДн, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

ПДн на физических электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4.7.9.3. Комиссия подтверждает уничтожение ПДн, указанных в пунктах 4.7.4 – 4.7.7. настоящей Политики согласно Требованиям к подтверждению уничтожения ПДн, утвержденным приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении ПДн – если данные обрабатываются без использования средств автоматизации;
- актом об уничтожении ПДн и выгрузкой из журнала регистрации событий в информационной системе ПДн – если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, которые должны содержаться в указанных документах, утверждаются приказом руководителя Организации.

4.7.9.4. После составления акта об уничтожении ПДн и выгрузки из журнала регистрации событий в информационной системе ПДн комиссия передает их в общий отдел для последующего хранения.

4.7.9.5. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

4.7.9.6. Уничтожение персональных данных, не указанных в пункте 4.7.9.3 настоящей Политики, подтверждается актом, который оформляется непосредственно после уничтожения таких данных. Форма акта утверждается приказом руководителя Организации.

4.8. Передача ПДн

4.8.1. Организация передает ПДн третьим лицам, если субъект ПДн выразил свое согласие на такие действия или передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.8.2. Перечень третьих лиц, которым передаются ПДн:

- Социальный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- судебные и правоохранительные органы в случаях, установленных законодательством;
- бюро кредитных историй (с согласия субъекта);
- юридические компании, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта)

4.8.3. Организация не осуществляет трансграничную передачу ПДн.

4.9. Доступ к ПДн

4.9.1. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Организацией, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Организации.

4.9.2. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Организации.

4.9.3. Допущенные к обработке ПДн Работники под подпись знакомятся с документами организации, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

5. Защита персональных данных

5.1. Подсистема защиты ПДн

5.1.1. В соответствии с требованиями нормативных документов Организацией создана система защиты ПДн (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.1.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.1.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.1.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

5.2. Основные меры защиты ПДн

Основными мерами защиты ПДн, используемыми Организацией, являются:

5.2.1. Назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением Организацией и ее работниками требований к защите ПДн.

5.2.2. Определение актуальных угроз безопасности ПДн при их обработке в ИСПД и разработка мер и мероприятий по защите ПДн.

5.2.3. Разработка политики в отношении обработки ПДн.

5.2.4. Установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн в ИСПД.

5.2.5. Установление индивидуальных паролей доступа работников в информационную систему в соответствии с их производственными обязанностями.

5.2.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности.

5.2.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

5.2.8. Сертифицированное программное средство защиты информации от несанкционированного доступа.

5.2.9. Сертифицированные межсетевой экран и средство обнаружения вторжения.

5.2.10. Соблюдение условий, обеспечивающих сохранность ПДн и исключающих несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн.

5.2.11. Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер.

5.2.12. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.2.13. Обучение работников Организации, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о ПДн, в том числе требованиям к защите ПДн, документам, определяющим политику Организации в отношении обработки ПДн, локальным актам по вопросам обработки ПДн.

5.2.14. Осуществление внутреннего контроля и аудита.

5.2.15. Работники Организации, непосредственно осуществляющие обработку пДн, должны быть ознакомлены под подпись до начала работы с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, настоящей Политикой и изменениями к ней, локальными актами по вопросам обработки ПДн.

5.3. Процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений

5.3.1. Без письменного согласия субъекта ПДн Организация не раскрывает третьим лицам и не распространяет ПДн, если иное не предусмотрено федеральным законом.

5.3.2. Запрещено раскрывать и распространять ПДн субъектов ПДн по телефону.

5.3.3. С целью защиты ПДн в Организации приказами руководителя назначаются (утверждаются):

- работник, ответственный за организацию обработки ПДн;
- перечень должностей, при замещении которых обрабатываются ПДн;
- перечень ПДн, к которым имеют доступ работники, занимающие должности, предусматривающие обработку ПДн;
- порядок доступа в помещения, в которых ведется обработка ПДн;
- порядок передачи ПДн в пределах Организации;
- форма согласия на обработку ПДн, форма согласия на обработку ПДн, разрешенных субъектом персональных данных для распространения;
- порядок защиты ПДн при их обработке в информационных системах ПДн;
- порядок проведения внутренних расследований, проверок;
- иные локальные нормативные акты, принятые в соответствии с требованиями законодательства в области ПДн.

5.3.4. Работники, которые занимают должности, предусматривающие обработку ПДн, допускаются к ней после подписания обязательства об их неразглашении.

5.3.5. Материальные носители ПДн хранятся в шкафах, запирающихся на ключ. Помещения Организации, в которых они размещаются, оборудуются запирающими устройствами. Выдача ключей от шкафов и помещений осуществляется под подпись.

5.3.6. Доступ к персональной информации, содержащейся в информационных системах Организации, осуществляется по индивидуальным паролям.

5.3.7. В Организации используется сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

5.3.8. Работники Организации, обрабатывающие ПДн, периодически проходят обучение требованиям законодательства в области ПДн.

5.3.9. В должностные инструкции работников Организации, обрабатывающих ПДн, включаются, в частности, положения о необходимости сообщать о любых случаях несанкционированного доступа к ПДн.

5.3.10. В Организации проводятся внутренние расследования в следующих ситуациях:

- при неправомерной или случайной передаче (предоставлении, распространении, доступе) ПДн, повлекшей нарушение прав субъектов ПДн;
- в иных случаях, предусмотренных законодательством в области ПДн.

5.3.11. Работник, ответственный за организацию обработки ПДн, осуществляет внутренний контроль:

- за соблюдением работниками, уполномоченными на обработку ПДн, требований законодательства в области ПДн, локальных нормативных актов;
- соответствием указанных актов требованиям законодательства в области ПДн.

Внутренний контроль проходит в виде внутренних проверок.

5.3.12. Внутренние плановые проверки осуществляются на основании ежегодного плана, который утверждается руководителем Организации.

5.3.13. Внутренние внеплановые проверки осуществляются по решению работника, ответственного за организацию обработки ПДн. Основанием для них служит информация о нарушении законодательства в области ПДн, поступившая в устном или письменном виде.

5.3.14. По итогам внутренней проверки оформляется докладная записка на имя руководителя Организации. Если выявлены нарушения, в документе приводится перечень мероприятий по их устранению и соответствующие сроки.

5.3.15. Внутреннее расследование проводится, если выявлен факт неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн (далее – инцидент).

5.3.16. В случае инцидента Организация в течение 24 часов уведомляет Роскомнадзор:

- об инциденте;
- его предполагаемых причинах и вреде, причиненном правам субъекта (нескольким субъектам) ПДн;
- принятых мерах по устранению последствий инцидента;
- представителе Организации , который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом.

При направлении уведомления нужно руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными приказом Роскомнадзора от 14.11.2022 № 187.

5.3.17. В течение 72 часов Организация обязана сделать следующее:

- уведомить Роскомнадзор о результатах внутреннего расследования;
- предоставить сведения о лицах, действия которых стали причиной инцидента (при наличии).

При направлении уведомления также необходимо руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными приказом Роскомнадзора от 14.11.2022 № 187.

5.3.18. В случае предоставления субъектом ПДн (его представителем) подтвержденной информации о том, что ПДн являются неполными, неточными или неактуальными, в них вносятся изменения в течение семи рабочих дней. Организация уведомляет в письменном виде субъекта ПДн (его представителя) о внесенных изменениях и сообщает (по электронной почте) о них третьим лицам, которым были переданы ПДн.

5.3.19. Организация уведомляет субъекта ПДн (его представителя) об устранении нарушений в части неправомерной обработки ПДн. Уведомляется также Роскомнадзор, если он направил обращение субъекта ПДн (его представителя) либо сам сделал запрос.

5.3.20. В случае уничтожения ПДн, которые обрабатывались неправомерно, уведомление направляется в соответствии с пунктом 5.3.19 настоящей Политики.

5.3.21. В случае уничтожения персональных данных, незаконно полученных или не являющихся необходимыми для заявленной цели обработки, Организация уведомляет субъекта персональных данных (его представителя) о принятых мерах в письменном виде. Организация уведомляет по электронной почте также третьих лиц, которым были переданы такие персональные данные.

6. Права субъекта ПДн

6.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые оператором способы обработки ПДн;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн 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 27.07.2006 № 152-ФЗ;
- 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;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ или другими федеральными законами.

6.2. Субъект ПДн вправе требовать от оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7. Обязанности Организации

7.1. Организация обязана:

- при сборе ПДн предоставить информацию субъекту об обработке его ПДн;
- в случаях, если ПДн были получены не от субъекта ПДн, уведомить субъекта;
- при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;
- давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн;

- не сообщать персональные данные субъекта ПДн третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом или иными федеральными законами;
- не сообщать персональные данные субъекта ПДн в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих ПДн субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;
- разрешать доступ к персональным данным субъекта ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн субъекта ПДн, которые необходимы для выполнения конкретных функций.

8. Ответственность за нарушение норм, регулирующих обработку и защиту ПДн

8.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области ПДн при обработке ПДн субъектов ПДн, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

8.2. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, а также несоблюдения требований к их защите, установленных Федеральным законом от 27.07.2006 № 152-ФЗ, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.