

**Общество с ограниченной ответственностью
«Санаторий «Евромед» ИНН:5528052944
(ООО «Санаторий «Евромед»)**

ПРИКАЗ

«01» августа 2024 г.

№161-О/Д

Омская область, Омский район, п. Ачаирский

«Об утверждении Политики
об обработке персональных данных
в обществе с ограниченной ответственностью
«Санаторий «Евромед» (ООО «Санаторий «Евромед»)

В целях обеспечения безопасности персональных данных в ООО «Санаторий «Евромед», во исполнение требований Трудового Кодекса РФ, Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Политику обработки персональных данных в Обществе с ограниченной ответственностью «Санаторий «Евромед» (ООО «Санаторий «Евромед») (Приложение 1).
2. Системному администратору Петрову А.П. обеспечить размещение Положения об обработке и защите персональных данных ООО «Санаторий «Евромед» на информационных стендах и официальном сайте <https://semo55.ru/>.
3. Начальнику отдела кадров Поповой Н.А. обеспечить ознакомление работников ООО «Санаторий «Евромед» с настоящим приказом.
4. Настоящий приказ вступает в действие с даты подписания.
5. Контроль за исполнением данного приказа оставляю за собой.

Управляющий



А.В. Федосеева

ПОЛИТИКА
обработки персональных данных в Обществе с ограниченной ответственностью
«Санаторий «Евромед»
(ООО «Санаторий «Евромед»)

1. Общие положения.

1.1. Настоящая Политика обработки персональных данных (далее - Политика) ООО «Санаторий «Евромед» ИНН 5528052944, 644544, Омская обл, м.р-н Омский, с.п. Комсомольское, п.Ачаирский, ул. Курортная, стр.8/2 (далее – Общество, Оператор) разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», иными федеральными законами и нормативно-правовыми актами.

1.2. Политика разработана с целью обеспечения защиты прав и свобод субъекта персональных данных при обработке его персональных данных (далее ПДн).

2. Цели обработки персональных данных.

ПДн обрабатываются Оператором в следующих целях:

1) Обработка персональных данных необходима для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей, в частности:

— выполнение требований законодательства в сфере труда и налогообложения;

— ведение текущего бухгалтерского и налогового учёта, формированию, изготовлению и своевременной подаче бухгалтерской, налоговой и статистической отчётности.

2) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных (работник или клиент), в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

3) Обработка персональных данных осуществляется в медико-профилактических целях, оказания медицинских, медико-социальных и санаторно-курортных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну, а также работники, в служебные обязанности которых, входит обработка первичной медицинской документации, содержащей сведения, составляющие врачебную тайну.

4) Обработка персональных данных необходима для защиты жизни, здоровья, или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

3. Правовое основание обработки персональных данных

Обработка ПДн осуществляется на основании следующего:

— Федеральный закон РФ от 24 июля 2009 года № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования»;

— Федеральный закон от 01 апреля 1996 года № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

— Федеральный закон от 6 декабря 2011 года № 402-ФЗ «О бухгалтерском учете»;

— Федеральный закон РФ от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

- Федеральный закон от 02 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Законом РФ от 07 февраля 1992 года № 2300-1 «О защите прав потребителей»;
- Постановление Правительства РФ от 11.05.2023 № 736 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг, внесении изменений в некоторые акты Правительства Российской Федерации и признании утратившим силу постановления Правительства Российской Федерации от 4 октября 2012 г. №1006»;
- Гражданский Кодекс РФ (ст. 152);
- Трудовой Кодекс РФ от 30 декабря 2001 года № 197-ФЗ;
- постановление Правления ПФР от 31 июля 2006 года № 192п «О формах документов индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования и инструкции по их заполнению»;
- постановление Государственного комитета Российской Федерации по статистике от 5 января 2004 года № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;
- иные нормативно-правовые акты, определяющие порядок оказания отдельных видов медицинских услуг, случаи и порядки обработки ПДн;
- Устав ООО «Санаторий «Евромед»;
- Лицензия на осуществление медицинской деятельности № Л041-01165-55/00889667 от 20.11.2023 г., выдана Министерством здравоохранения Омской области.
- Договоры, заключаемые между ООО «Санаторий «Евромед» и субъектом персональных данных;
- Согласие на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям ООО «Санаторий «Евромед»).

4. Перечень действий с персональными данными.

При обработке ПДн оператор осуществляет следующие действия с ПДн:

- блокирование;
- запись;
- извлечение;
- использование;
- накопление;
- обезличивание;
- передачу (распространение, предоставление, доступ);
- сбор;
- систематизация;
- удаление;
- уничтожение персональных данных
- уточнение (обновление, изменение);
- хранение.

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

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.

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.

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

Запись - документальное фиксирование данных, полученных от самого субъекта персональных данных или из иных источников. Запись предполагает не только фиксацию сведений на бумажных носителях, но и документирование данных в виде графических, рисованных, фотографических или иных изображений, как на бумаге, так и в цифровом виде на электронных носителях информации.

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

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.

Систематизирование - приведение в систему, наведение определенного порядка.

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. Медицинская документация постоянно дополняется новыми данными обследования, данными изменения состояния здоровья пациента и результатами медицинских вмешательств. Все данные, полученные из различных источников, используются, в соответствии с законодательством РФ, исключительно в интересах пациента, для уточнения диагноза его заболевания и повышения эффективности проводимой терапии.

Уточнение - предполагает изменение, обновление сведений, отражающих изменение состояние пациента в процессе выполнения медицинского вмешательства. Поскольку процесс оказания медицинской помощи динамичный, постоянно меняющийся, то и эти данные по мере их поступления уточняются (обновляются, изменяются), что позволяет менять тактику лечения, использовать более эффективные методы терапии, выполнять более информативные методы диагностики.

Хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является субъект персональных данных.

Уничтожение или выдача медицинской документации по просьбе (заявлению) клиента не допускается, более того, как указывалось ранее, документация должна храниться в архиве учреждения в течение строго определенного срока, установленного законодательными актами. Учитывая указанные требования действующего законодательства РФ и ведомственные нормативно-правовые акты, первичные медицинские документы должны быть оформлены и сданы в архив (без права дальнейшей обработки) в течение 3-х рабочих дней, со дня даты поступления заявления клиента.

5. Состав обрабатываемых персональных данных

5.1 Обработке Оператором подлежат ПДн следующих субъектов ПДн:

1) ПДн кандидатов при трудоустройстве на работу в составе:

- фамилия, имя, отчество, число, месяц, год и место рождения;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- пол;
- гражданство;
- владение иностранными языками, степень владения;
- семейное положение;
- данные документа, удостоверяющего личность (паспорт или документ его заменяющий (серия, номер, кем и когда выдан));

- адрес регистрации и фактического места жительства, дата регистрации;
- контактный телефон (домашний, мобильный);
- адрес электронной почты;
- выполняемая работа с начала трудовой деятельности (включая учебу в высших и средних специальных учебных заведениях, военную службу, работу по совместительству и т.п.) (месяц и год поступления/ухода, должность с указанием организации);
- фотографии;
- рекомендации, характеристики;
- данные об образовании, в том числе данные об организациях, осуществляющих образовательную деятельность по реализации профессиональных образовательных программ медицинского образования;
 - данные о документах об образовании и (или) о квалификации (когда и какие учебные заведения окончили, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому), а также данные о сертификате специалиста или о прохождении аккредитации специалиста;
 - послевузовское профессиональное образование: интернатура, ординатура, аспирантура, адъюнктура, докторантура (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
 - сведения о дате защиты и теме диссертации, диплома;
 - сведения о прохождении за последние пять лет повышения квалификации или профессиональной переподготовки или стажировки;
 - данные о квалификационной категории, ученой степени, ученого звания и почетного звания;
 - сведения о дополнительных навыках;
 - сведения о наградах/поощрениях; государственные награды, иные награды, почетные и знаки отличия;
 - результаты медицинского обследования, справки и заключения медицинского осмотра для осуществления трудовых обязанностей;
 - сведения о привлечении к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности;
 - наличие (отсутствие) судимости;
- 2) ПДн работников в составе:
 - фамилия, имя, отчество, число, месяц, год и место рождения;
 - прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
 - пол;
 - гражданство;
 - владение иностранными языками, степень владения;
 - семейное положение, свидетельство о браке, справка о заключении брака, свидетельство о расторжении брака;
 - свидетельство о рождении детей, сведения о составе семьи: степень родства, фамилия, имя, отчество, год, число, месяц рождения близких родственников (отца, матери, супруги (супруга) и детей), контактные телефоны близких родственников;
 - данные документа, удостоверяющего личность (паспорт или документ его заменяющий (серия, номер, кем и когда выдан);
 - адрес регистрации и фактического места жительства, дата регистрации;
 - сведения воинского учета: отношение к воинской обязанности, воинское звание, сведения о воинском учете (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
 - контактный телефон (домашний, мобильный);
 - адрес электронной почты;
 - трудовые книжки и сведения о трудовой деятельности;

- выполняемая работа с начала трудовой деятельности (включая учебу в высших и средних специальных учебных заведениях, военную службу, работу по совместительству и т.п.) (месяц и год поступления/ухода, должность с указанием организации);
- сведения о государственном пенсионном страховании;
- идентификационный номер налогоплательщика;
- фотографии;
- рекомендации, характеристики;
- данные об образовании, в том числе данные об организациях, осуществляющих образовательную деятельность по реализации профессиональных образовательных программ медицинского образования;
- данные о документах об образовании и (или) о квалификации (когда и какие учебные заведения окончили, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому), а также данные о сертификате специалиста или о прохождении аккредитации специалиста;
- послевузовское профессиональное образование: интернатура, ординатура, аспирантура, адъюнктура, докторантура (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
- сведения о дате защиты и теме диссертации, диплома;
- сведения о прохождении за последние пять лет повышения квалификации или профессиональной переподготовки или стажировки;
- данные о квалификационной категории, ученой степени, ученого звания и почетного звания;
- сведения о дополнительных навыках;
- сведения о наградах/поощрениях; государственные награды, иные награды, почетные и знаки отличия;
- результаты медицинского обследования, справки и заключения медицинского осмотра для осуществления трудовых обязанностей;
- сведения о привлечении к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности;
- наличие (отсутствие) судимости;
- сведения о размере заработной платы и иных дополнительных выплатах;
- сведения об отчислениях в Федеральную налоговую службу;
- сведения об отчислениях в Фонд пенсионного и социального страхования РФ;
- сведения о начислениях и удержаниях;
- сведения о налоговых вычетах;
- сведения о социальных льготах;
- данные листка временной нетрудоспособности;
- номер лицевого счета в банке;
- подразделение;
- должность;
- табельный номер;
- сведения трудового договора (номер, дата, испытательный срок);
- график работы;
- сведения об инвалидности;
- сведения об отпусках и командировках;
- материалы служебных расследований;
- иные сведения, необходимые работодателю в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

- 3) ПДн потребителей в составе:
- фамилия, имя, отчество;
- число, месяц, год рождения;
- возраст;
- пол;

- СНИЛС;
- контактный телефон;
- данные документа, удостоверяющего личность (паспорт или документ его заменяющий (серия, номер, кем и когда выдан);
- гражданство;
- адрес регистрации и фактического места жительства, дата регистрации полис ОМС (серия и номер, дата действия);
- полис ДМС (серия и номер, дата действия);
- сведения об оплате;
- медицинские сведения.
- 4) ПДн контрагентов:
- Фамилия, имя, отчество;
- число, месяц, год рождения;
- паспортные данные;
- идентификационный номер налогоплательщика;
- адрес;
- контактный телефон;
- сведения о договоре;
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования:

- иные сведения при необходимости.

5) Персональные данные Пользователя сайта:

- фамилия, имя, отчество;
- – число, месяц, год рождения;
- – адрес регистрации и фактического места жительства;
- – контактный телефон;
- – адрес электронной почты;
- – IP-адрес Пользователя;
- – географическое положение;
- – информация о браузере и виде операционной системы;
- – сведения о предпочтениях и поведении на Сайте.

5.2. На сайтах Организации используются файлы «Cookie», которые получаются автоматически при доступе Пользователя к Сайту.

«Cookie» представляет собой набор сведений, таких как логин, IP-адрес Пользователя, географическое положение, сведения о предпочтениях и поведении на Сайте, информации о браузере и виде операционной системы и собираются с целью:

- аналитическая деятельность по исследованию предпочтений Пользователя Сайта;
- статистика по активности Пользователей на Сайте/сайтах, в т.ч. с помощью сервисов Интернет-статистики таких, как «Яндекс.Метрика», «Пиксель VK Рекламы» (дополнительные сведения о сборе данных сервисами располагаются по адресам https://yandex.ru/legal/metrika_termsfuse/, <https://vk.com/privacy>);
- повышение производительности и эффективности Сайта;
- аналитика и исправление ошибок Сайта (в т.ч. и с точки зрения безопасности), улучшение работы всех ресурсов Сайта;
- предоставление доступа в личный кабинет;
- персонализация маркетинговых кампаний.

Сайт/сайты Организации, при доступе к определенным местам, сохраняет файлы «Cookie» на компьютере, с которого был выполнен вход на Сайт, Пользователей Сайта/Сайтов в случае согласия со стороны Пользователя Сайта.

Данные обрабатываются в совокупном и обезличенном виде и не содержат информации о персональных данных, но при этом позволяют связать Пользователя с его персональной информацией, сообщенной Пользователем на Сайте.

При входе на Сайт Пользователь должен подтвердить свое согласие на использование файлов «Cookie». Подтверждение вышеуказанного согласия выполняется путем продолжения

пользования Сайтом компании. Для информирования Пользователя Сайта о необходимости дать такое согласие на Сайте размещается всплывающий баннер с соответствующим текстом.

Пользователь сайта в любой момент может самостоятельно ограничить или полностью отключить файлы «Cookie» через настройки в используемом Пользователем Сайта браузере. При этом Компания не может гарантировать стабильную работу Сайта.

5.3. На сайте/сайтах установлено программное средство Яндекс.Метрика, использование функционала которого позволяет определить уникального посетителя Сайта, формировать сведения о его предпочтениях и поведении на сайте.

5.4. Обработка персональных данных осуществляется с согласия субъекта ПДн (работники, пациенты, контрагенты) на обработку его персональных данных.

5.5. Содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки. Обрабатываемые ПДн не являются избыточными по отношению к заявленным целям обработки.

6. Порядок и условия обработки персональных данных.

6.1. Обработка персональных данных Оператором выполняется следующими способами:

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

6.2. Обработка персональных данных включает в себя перечень действий, определенных в пункте 4 настоящей Политики обработки.

6.3. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных.

6.4. Оператор не вправе обрабатывать персональные данные субъекта персональных данных без его письменного согласия, за исключением случаев, предусмотренных статьей 6 Федерального закона «О персональных данных».

6.5. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

6.6. Письменное согласие субъекта персональных данных должно включать: – фамилию, имя, отчество; – адрес субъекта персональных данных; – номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе; – наименование и адрес Оператора; – цель обработки персональных данных; – перечень персональных данных, на обработку которых дается согласие субъекта персональных данных; – перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных; – срок, в течение которого действует согласие; – способ его отзыва; – подпись субъекта персональных данных.

6.7. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры, в том числе: 1) определяет угрозы безопасности персональных данных при их обработке в информационных системах персональных данных; 2) применяет организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных; 3) применяет прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации; 4) оценивает эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных; 5) учитывает машинные носители персональных данных; 6) обнаруживает факты несанкционированного доступа к персональным данным и принимает меры; 7) восстанавливает персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним; 8) устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в

информационной системе персональных данных; 9) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.8. В целях обеспечения сохранности и конфиденциальности персональных данных все операции с персональными данными должны выполняться только работниками Оператора, осуществляющими данную работу в соответствии с трудовыми обязанностями.

6.9. Оператор получает персональные данные непосредственно от субъектов персональных данных или их представителей, наделенных соответствующими полномочиями. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном виде при заключении договора с Оператором, а также в случаях, установленных федеральным законом.

6.10. Запрещается хранение документов с персональными данными и их копий на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода работника из рабочего помещения.

6.11. В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специально отведенных для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.

6.12. При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

7. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации (неавтоматизированная обработка персональных данных).

7.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

7.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

7.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных законодательством, а также локальными правовыми актами организации (при их наличии).

7.4. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

7.5. 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.

7.6. Обществом обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

8. Особенности обработки персональных данных в информационных системах.

8.1. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании

закключаемого с этим лицом договора.

8.2. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

8.3. Состав и содержание мер по защите информации в информационных системах зависят от установленного уровня защищенности информационной системы. Обработка и защита в информационных системах с использованием средств автоматизации персональных данных с учетом определенного типа угроз безопасности и уровня защищенности персональных данных (прилагается).

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

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

8.6. Доступ к персональным данным в информационных системах персональных данных разрешается после обязательного прохождения процедуры идентификации и аутентификации.

8.7. Лицами, ответственными за обеспечение безопасности персональных данных, должно быть обеспечено:

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

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

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

г) постоянный контроль за обеспечением уровня защищенности персональных данных;

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

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

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

з) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

8.8. В случае выявления нарушений порядка обработки персональных данных в информационных системах принимаются меры по установлению причин нарушений и их устранению.

9. Обеспечение защиты персональных данных при их обработке Оператором

9.1 Оператор принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определил состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Приказом ФСТЭК от 18 февраля 2013 года № 21 «Об утверждении Составы и содержания организационных и технических мер по

обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами, если иное не предусмотрено федеральными законами. К таким мерам относятся:

- назначение Оператором ответственного за организацию обработки персональных данных;
- издание Оператором документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону "О персональных данных" и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, локальным актам оператора;
- определение оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
- ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

9.2 Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие 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.

10. Сроки обработки и хранения персональных данных.

10.1 Обработка персональных данных в Обществе прекращается в следующих случаях:

- при выявлении факта неправомерной обработки персональных данных. Срок прекращения обработки - в течение трех рабочих дней с даты выявления такого факта;
- при достижении целей их обработки (за некоторыми исключениями);
- по истечении срока действия или при отзыве субъектом персональных данных согласия на обработку его персональных данных (за некоторыми исключениями), если в соответствии с Законом о персональных данных их обработка допускается только с согласия;
- при обращении субъекта персональных данных к Обществу с требованием о прекращении обработки персональных данных (за исключением случаев, предусмотренных Законом о персональных данных). 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).

10.2. Персональные данные хранятся в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Исключение - случаи, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных.

10.3. Персональные данные на бумажных носителях хранятся в Обществе 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)).

10.4.Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

11. Защита персональных данных. Процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений.

11.1. Без письменного согласия субъекта персональных данных Общество не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

11.2. С целью защиты персональных данных в Обществе приказами руководителя назначаются (утверждаются):

- работник, ответственный за организацию обработки персональных данных;
- перечень должностей, допущенных к обработке персональных данных;
- форма согласия на обработку персональных данных, форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения и др.;

- иные локальные акты, принятые в соответствии с требованиями законодательства в области персональных данных.

11.3. Работники, которые занимают должности, предусматривающие обработку персональных данных, допускаются к ней после подписания соглашения/обязательства об их неразглашении.

11.4. Личные дела и документы, содержащие персональные данные субъектов, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

11.5. Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

11.6. Работник, ответственный за организацию обработки персональных данных, осуществляет внутренний контроль:

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

11.7. Внутреннее расследование проводится, если выявлен факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных (далее - инцидент).

12. Порядок уничтожения, блокирования персональных данных.

12.1. Общество блокирует персональные данные в порядке и на условиях, предусмотренных законодательством в области персональных данных.

12.2. При достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей персональные данные уничтожаются либо обезличиваются, за исключением случаев, предусмотренных законодательством.

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

12.4. Персональные данные, 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.

12.5. Персональные данные уничтожаются в течение 30 дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иным соглашением между ним и Обществом либо если Общество не вправе обрабатывать персональные данные без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

12.6. При достижении максимальных сроков хранения документов, содержащих

персональные данные, персональные данные уничтожаются в течение 30 дней.

12.7. Персональные данные уничтожаются (если их сохранение не требуется для целей обработки персональных данных) в течение 30 дней с даты поступления отзыва субъектом персональных данных согласия на их обработку. Иное может предусматривать договор, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иное соглашение между ним и Обществом. Кроме того, персональные данные уничтожаются в указанный срок, если Общество не вправе обрабатывать их без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

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

12.9. Уничтожение персональных данных осуществляет комиссия, созданная приказом руководителя Общества.

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

12.11. Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на 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.

12.12. Комиссия подтверждает уничтожение персональных данных, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденным Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

12.12.1. актом об уничтожении персональных данных - если данные обрабатываются без использования средств автоматизации;

12.12.2. актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных - 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.

12.13. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

13. Порядок обезличивания персональных данных.

13.1. Общество может обезличивать персональные данные в статистических или иных исследовательских целях, по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

13.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- замена части данных идентификаторами;
- обобщение, изменение или удаление части данных;
- деление данных на части и обработка в разных информационных системах;
- перемешивание данных;
- другие способы.

В случае достижения целей обработки персональных данных или в случае утраты необходимости в достижении этих целей способом обезличивания является уменьшение перечня обрабатываемых данных.

13.3. Решение о необходимости обезличивания персональных данных и способе обезличивания принимает ответственный за организацию обработки персональных данных.

13.4. Обезличенные персональные данные не подлежат

разглашению и нарушению конфиденциальности.

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

13.6. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

13.7. В процессе обработки обезличенных данных, при необходимости, может производиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются.

13.8. Обработка персональных данных до осуществления процедур обезличивания и после выполнения операций деобезличивания должна осуществляться в соответствии с законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

14. Порядок учета (регистрации), рассмотрения запросов субъектов ПДн или их представителей.

14.1. Организация приема и обработки Обществом запросов и осуществление контроля над приемом и обработкой запросов осуществляется лицом/лицами (работником), ответственным за организацию обработки и защиту персональных данных (далее Ответственный ООЗПДн).

При осуществлении обработки Обществом запросов всеми лицами (работниками), привлеченными Обществом к такой обработке, должна соблюдаться конфиденциальность данных, содержащихся в запросах, рабочей переписке по вопросам их рассмотрения, и ответах на запросы.

14.2. Запросы принимаются с помощью средств приема входящей корреспонденции Общества или осуществления личного приема граждан или их законных представителей (заявителей).

14.3. Лица (работники) Общества, осуществляющие прием входящей корреспонденции, проводят ее первичное рассмотрение и передают ее Ответственному ООЗПДн в следующих случаях:

а) адресатом является уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор), федеральный орган исполнительной власти, уполномоченным в области обеспечения безопасности, (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), Прокуратура РФ;

б) адресантом является Ответственный ООЗПДн;

в) в теме или в тексте письма содержатся ссылки на положения ФЗ «О ПДн»;

г) в тексте письма содержится просьба (требование) предоставить информацию, в том числе содержащую:

- подтверждение факта обработки ПДн Общества;
- правовые основания и цели обработки ПДн Обществом;
- цели и применяемые способы обработки ПДн Обществом;
- наименование и место нахождения Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Обществом или на основании Федерального закона № 152-ФЗ;

- обрабатываемые Обществом ПДн, относящиеся к автору запроса или его поручителю, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом № 152-ФЗ;

- сроки обработки Обществом ПДн, в том числе сроки их хранения;

- порядок осуществления субъектом ПДн прав, предусмотренных федеральным законом № 152-ФЗ;

- информацию об осуществленной или о предполагаемой трансграничной передаче Обществом ПДн;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Общества, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные Федеральным законом №152-ФЗ или другими федеральными законами в области персональных данных.

14.4. Инструктаж лиц (работников) Общества, осуществляющих прием входящей корреспонденции, по вопросам отнесения входящей корреспонденции к запросам по вопросам обработки Обществом персональных данных осуществляется Ответственным ООЗПДн.

14.5. Ответственный ООЗПДн осуществляет:

а) регистрацию поступающих запросов, осуществляет или обеспечивает их рассмотрение;

б) личный прием заявителей по вопросам обработки Обществом их персональных данных.

14.6. Ответственный ООЗПДн производит первичное рассмотрение запроса на предмет его соответствия требованиям ст. 14 ФЗ «О ПДн» и возможности дальнейшего рассмотрения Обществом.

14.7. Запрос может быть отклонен Ответственным ООЗПДн на стадии первичного рассмотрения по следующим причинам:

а) содержание запроса не соответствует требованиям ч. 3 ст. 14 ФЗ «О ПДн»;

б) запрос содержит требование предоставить информацию, не входящую в перечень, установленный ч. 7 ст. 14 ФЗ «О ПДн»;

в) запрос является повторным, и направлен Обществу с нарушением условий, предусмотренных частями 4 и 5 ст. 14 ФЗ «О ПДн»;

г) право заявителя на получение запрашиваемых данных ограничивается в соответствии с ч. 8 ст. 14 ФЗ «О ПДн».

14.8. В случае отклонения Ответственным ООЗПДн запроса на стадии первичного рассмотрения, в адрес заявителя направляется в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 настоящего Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати дней) со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Подготовка такого отказа осуществляется Ответственным ООЗПДн.

14.9. Ответственность за отказ в рассмотрении запроса и Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Ответственном ООЗПДн.

14.10. В случае принятия Ответственным ООЗПДн решения о дальнейшем рассмотрении запроса, Ответственный ООЗПДн определяет в компетенцию каких должностных лиц входит запрашиваемая информация или процедуры, необходимые для выполнения запроса, и направляет уполномоченным лицам (работникам) служебные запросы (записки).

14.11. В случае, если заявитель ранее не обращался в Общество по вопросам обработки его ПДн, на основе принятого к рассмотрению запроса и служебных запросов (записок) уполномоченным лицам (работникам) Общества Ответственным ООЗПДн формируется дело о рассмотрении запросов данного заявителя.

14.12. В случае если заявитель ранее обращался в Общество по вопросам обработки ПДн, новый запрос заявителя, а также служебные запросы (записки) уполномоченным лицам (работникам) Общества подшиваются в ранее созданное дело.

14.13. Работники Общества, в компетенцию которых входит запрашиваемая информация или процедуры, необходимые для выполнения запроса, при рассмотрении и разрешении запроса обязаны:

– внимательно разобраться в пределах запроса, в случае необходимости истребовать дополнительные материалы или направить сотрудников на места для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о ПДн;

– принимать по запросу законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;

– предоставлять Ответственному ООЗПДн документированные свидетельства рассмотрения запросов и предоставления запрашиваемой информации или ответов (служебные

записки и иные документы по вопросам рассмотрения запроса, и т.п.), а также осуществлять согласование ответа на запрос;

– сообщать в письменной форме заявителю о решениях, принятых по запросу, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса – разъяснять порядок обжалования принятого решения.

14.14. Ответственным ООЗПДн осуществляет контроль сроков рассмотрения и исполнения, направленных им служебных запросов (записок), осуществляет сбор и обработку документированных свидетельств рассмотрения запросов и предоставления запрашиваемой информации или ответов (служебные записки и иные документы по вопросам рассмотрения запроса, и т.п.), а также подготовку или согласование ответа на запрос.

14.15. Сроки рассмотрения запросов:

– рассмотрение запроса, связанного с реализацией заявителем права, предусмотренного ч. 1 ст. 14 ФЗ «О ПДн», а также предоставление возможность реализовать такое право (ознакомиться с ПДн) должны осуществляться не позднее, чем 30 (тридцать дней) с даты получения запроса;

– запрос, содержащий сведения, подтверждающие, что ПДн являются неполными, неточными или неактуальными, должен быть рассмотрен в срок, не превышающий семи рабочих дней со дня его получения;

– запрос, содержащий сведения, подтверждающие, что ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, должен быть рассмотрен в срок, не превышающий семи рабочих дней со дня его получения;

– запрос уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор), федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, (ФСБ России) и федерального органом исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, (ФСТЭК России), Прокуратуры РФ рассматриваются в сроки, указанные в соответствующем запросе;

– в случае подтверждения факта неправомерной обработки ПДн, указанной в запросе, рассмотрение запроса и направление ответа на него должно осуществляться в срок, не превышающий 3 (три) рабочих дня с момента получения такого запроса.

14.16. Все собранные Ответственным ООЗПДн документированные свидетельства рассмотрения запроса подшиваются в дело о рассмотрении запросов данного заявителя.

14.17. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

14.18. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудником Общества действия (бездействия), содержащего признаки административного правонарушения или состава преступления, информация доводится до руководства Общества и принимается решение о передаче сведений о правонарушении в уполномоченные органы.

14.19. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

14.20. Направление ответа на запрос выполняют лица (работники) Общества, осуществляющие обработку исходящей корреспонденции.

14.21. Письменные ответы на запросы, поступившие в виде бумажных документов печатаются на бланке организации, регистрируются Ответственным ООЗПДн, и направляются в адрес заявителя заказным письмом.

14.22. Письменные ответы на запросы, поступившие в виде электронных документов или электронного сообщения по сетям связи, оформляются в виде электронных документов, имеющих формат, не предполагающий возможность редактирования текста ответа, подписываются усиленной квалифицированной электронной подписью организации или уполномоченного лица, и передаются по сети связи способом, позволяющим получить свидетельство (электронная квитанция, электронное сообщение, иное) доставки (получения) ответа заявителем.

15. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных.

15.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, пациента, иных лиц привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном действующим законодательством Российской Федерации.

15.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Законом о персональных данных, а также требований к защите персональных данных, установленных в соответствии с названным Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных убытков.

16. Заключительные положения.

16.1. Политика является общедоступным документом.

16.2. Во исполнение требований законодательства в сфере защиты персональных данных Оператором разрабатываются и утверждаются иные локальные акты.

16.3. Ответственность лиц, имеющих доступ к персональным данным, определяется действующим законодательством Российской Федерации.