ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «МНОГОПРОФИЛЬНЫЙ ЦЕНТР СОВРЕМЕННОЙ МЕДИЦИНЫ «ЕВРОМЕД»

ПРИКАЗ

«1» февраля 2024 г. №24.02012/ОД

г. Омск

Об утверждении Положения
об обработке и защите персональных данных
в обществе с ограниченной ответственностью
«Многопрофильный центр современной медицины «Евромед»
(ООО «МЦСМ «Евромед»)

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

ПРИКАЗЫВАЮ:

1. Утвердить Положение об обработке и защите персональных данных в обществе с ограниченной ответственностью «Многопрофильный центр современной медицины «Евромед» (ООО «МЦСМ «Евромед») (Приложение 1).
2. Руководителю отдела регистратуры и справочной службы Донец Е.Д. обеспечить размещение Положение об обработке и защите персональных данных ООО «МЦСМ «Евромед» на информационных стендах.
3. Начальнику отдела маркетинга и связей с общественностью Зародовой К.А. обеспечить размещение Положение об обработке и защите персональных данных ООО «МЦСМ «Евромед» на официальном сайте https://euromed-omsk.ru/ и сайтах https://euromedosmotr.ru/, https://emdental.ru/, https://hair.euromed-omsk.ru/.
4. Начальнику отдела кадров Поповой Н.А. обеспечить ознакомление работников Общества с настоящим приказом.
5. Настоящий приказ вступает в действие с даты подписания.
6. Признать Положение об обработке и защите персональных данных работников, утв. Приказом № 02/1-ОД от 09.01.2019 года утратившим силу.
7. Контроль за исполнением данного приказа в части деятельности подразделений,

– находящихся по адресу: г. Омск, пр. Маркса 15, г. Омск, ул. Старозагородная Роща, д. 8, г. Омск, ул. Кемеровская, д. 13, отделением скорой медицинской помощи, отделением медицинской реабилитации оставить за управляющим Нацаренус Т.А.;

– находящихся по адресу: г. Омск, ул. Съездовская, д. 29/3, г. Омск, ул. Лукашевича, д. 21Б, а также малых клиник и центров лабораторной диагностики оставить за управляющим Шрейдер Т.Ф.

Управляющий Т.Ф. Шрейдер

Приложение № 1
к приказу ООО «МЦСМ «Евромед»
от 01.02.2024 г. № 24.02.01-2/ОД

Положение
об обработке и защите персональных данных
в обществе с ограниченной ответственностью «Многопрофильный центр современной медицины «Евромед» (ООО «МЦСМ «Евромед»)

1. Общие положения

1.1. Настоящее положение регламентируется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных) и иными нормативными правовыми актами в области обработки и защиты персональных данных.

1.2. К субъектам, персональные данные которых обрабатываются в Обществе в соответствии с Положением, относятся:

- кандидаты при трудоустройстве на работу в Общество;
- работники Общества;
- бывшие работники Общества;
- члены семей работников Общества - в случаях, когда согласно законодательству сведения о них предоставляются работником;
- лица, персональные данные которых Общество обязано обрабатывать в соответствии с трудовым законодательством и иными актами, содержащими нормы трудового права;
- пациенты, в т.ч. физические лица, обратившихся за медицинской помощью, работники, подлежащие обязательным медицинским обследованиям;
- контрагенты;
- посетители сайта.

1.3. 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;
- принятие решения о приеме на работу или об отказе в приеме на работу;
- индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования;
- 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, в целях установления медицинского диагноза, оказания медицинских и медико-социальных 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.

5) Обработка персональных данных осуществляется в целях аналитической деятельности по исследованию предпочтений Пациентов, клиентов, Пользователей/Посетителей Сайта, статистики по активности Пользователей на Сайте, в т.ч. с помощью сервисов Интернет-статистики таких, как «Яндекс.Метрика», «Пиксель VK Рекламы», повышения производительности и эффективности Сайта, аналитики и исправления ошибок Сайта (в т.ч. и с точки зрения безопасности), улучшения работы всех ресурсов Сайта, предоставления доступа в личный кабинет, персонализации маркетинговых кампаний, оценки и повышения качества услуг.

1.4. Персональные данные работника - информация, необходимая обществу с ограниченной ответственностью «Многопрофильный центр современной медицины «Евромед» (ООО «МЦСМ «Евромед) (далее - Общество, работодатель) в связи с трудовыми отношениями и касающаяся конкретного работника.

К персональным данным работника относятся:

- 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 категорий, 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.

1.5. Персональные данные пациента - информация, полученная Обществом при первоначальном поступлении пациента, при заключении с пациентом договора на оказание медицинских услуг, а также информация, полученная в процессе оказания медицинской помощи.

К персональным данным пациента относятся:

– Фамилия, имя, отчество;

– дата рождения;

– место рождения;

– возраст;

– пол;

– СНИЛС;

– номер телефона;

– документ удостоверяющий личность (тип документа, серия, номер дата выдачи, кем выдан);
– гражданство;
– социальный статус;
– место работы;
– место учебы;
– должность;
– адрес прописки;
– адрес проживания;
– полис ОМС (серия и номер, дата действия);
– номер договора;
– ЛПУ прикрепления;
– полис ДМС (серия и номер, дата действия);
– сведения об оплате;
– медицинские сведения:
– анамнез;
– диагноз;
– сведения об организации, осуществляющей медицинскую деятельность;
– вид оказанной медицинской помощи;
– условия оказания медицинской помощи;
– сроки оказания медицинской помощи;
– объем оказанной медицинской помощи, включая сведения об оказанных медицинских услугах;
– результат обращения за медицинской помощью;
– номер листка нетрудоспособности;
– сведения о проведенных медицинских экспертизах, медицинских осмотрах и медицинских освидетельствованиях и их результаты;
– иные сведения, необходимые медицинской организации в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

1.6. Персональные данные контрагента:
– Фамилия, имя, отчество;
– число, месяц, год рождения;
– паспортные данные;
– идентификационный номер налогоплательщика;
– адрес;
– контактный телефон;
– сведения о номере и серии страхового свидетельства государственного пенсионного страхования:
– иные сведения при необходимости.

1.7. Персональные данные Пользователя сайта:
– логин;
– IP-адрес Пользователя;
– географическое положение;
– информация о браузере и виде операционной системы;
– сведения о предпочтениях и поведении на Сайте.

1.8. Все персональные сведения о работниках и пациентах, контрагентах и иных лицах общество может получить только от них самих. В случаях, когда Общество получает необходимые

персональные данные у третьего лица, Общество уведомляет об этом работников, пациентов, иных лиц и получает от них письменное согласие.

1.9. Общество сообщает работникам, пациентам, иным лицам о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работников и пациентов дать письменное согласие на их получение.

1.10. Персональные данные работников, пациентов, иных лиц являются конфиденциальной информацией и не могут быть использованы в личных целях.

1.11. При определении объема и содержания персональных данных Общество руководствуется настоящим положением, Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами.

Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям обработки.

2. Обработка, хранение и передача персональных данных

2.1. Обработка персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работнику в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работника и сохранности имущества, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, ведения кадрового и бухгалтерского учета, оформлении награждений и поощрений, предоставлении со стороны Общества установленных законодательством условий труда, гарантий и компенсаций, заполнении и передаче в уполномоченные органы требуемых форм отчетности, осуществлении контроля за количеством и качеством выполняемой работы.

2.2. Обработка персональных данных пациента осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, установления медицинского диагноза и оказания медицинских услуг. Обработка специальных категорий персональных данных, в частности сведений, касающихся состояния здоровья, осуществляется без согласия субъектов персональных данных в случаях, предусмотренных законодательством в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну.

2.3. Обработка персональных данных иных лиц осуществляется в целях исполнение договоров с субъектами персональных данных.

2.4. Обработка персональных данных в Обществе 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.

2.5. Меры по обеспечению безопасности персональных данных при их обработке

2.5.1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать 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.

2.5.2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых

обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.6. 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.

2.7. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных в Обществе осуществляются посредством:

- получения оригиналов документов либо их копий;
- копирования оригиналов документов;
- внесения сведений в учетные формы на бумажных и электронных носителях;
- создания документов, содержащих персональные данные, на бумажных и электронных носителях;
- внесения персональных данных в информационные системы персональных данных.

2.8. В Обществе используются следующие информационные системы:

- корпоративная электронная почта;
- система электронного документооборота;
- система поддержки рабочего места пользователя;
- система нормативно-справочной информации;
- система управления персоналом.

Конкретные наименования информационных систем персональных данных и цели их создания определяются Перечнем информационных систем персональных данных Общества.

2.9. Передача (распространение, предоставление, доступ) персональных данных субъектов персональных данных осуществляется в случаях и в порядке, предусмотренных законодательством в области персональных данных и Положением.

2.10. Персональные данные субъектов обрабатываются, накапливаются и хранятся в бухгалтерии, отделе кадров, юридическом отделе, отделе маркетинга, архиве на бумажных и электронных носителях с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных. Право на обработку персональных данных предоставляется работникам структурных подразделений, определенным приказом руководителя Общества.

2.11. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно - распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями.

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

3.1. 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).

3.2. 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.

3.3. 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).

3.4. 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).

3.5. 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.

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

4. Особенности обработки персональных данных в информационных системах.

4.1. 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 заключаемого с этим лицом договора.

4.2. 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.

4.3. 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).

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

4.5. 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.

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

4.7. 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.

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

5. Сроки обработки и хранения персональных данных

5.1. 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).

5.2. 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.

5.3. 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)).

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

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

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

6.2. 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.

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

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

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

6.6. 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.

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

7. Порядок уничтожения, блокирования персональных данных

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

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

7.3. 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.

7.4. 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.

7.5. 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.

7.5.1. При достижении максимальных сроков хранения документов, содержащих персональные данные, персональные данные уничтожаются в течение 30 дней.

7.6. 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.

7.7. 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.

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

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

7.8.2. Персональные данные на бумажных носителях уничтожаются с использованием шредера. 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.

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

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

7.8.4. 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.

8. Порядок обезличивания персональных данных

8.1. 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.

8.2. 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.

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

8.4. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

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

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

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

8.8. 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.

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

9.1. 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.

9.2. 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.

10. Заключительные положения

10.1. Настоящее положение вступает в силу с момента его утверждения.

10.2. Общество обеспечивает неограниченный доступ к настоящему документу путем размещения на официальном сайте.

10.3. Настоящее положение доводится до сведения всех работников персонально под подпись.

Обработка и защита в информационных системах с использованием средств автоматизации персональных данных с учетом определенного типа угроз безопасности и уровня защищенности персональных данных

Информационная система обработки персональных данных	**Уровень защищенности**
ИСПДн "1С:Бухгалтерия и ЗУП"	4 - й уровень защищенности
Медицинская информационная система "Ариадна"	2 - й уровень защищенности
Медицинская информационная система "Медея"	2 - й уровень защищенности
ИСПДн "Сбербанк-онлайн"	4 - й уровень защищенности
ИСПДн "Сбис++"	4 - й уровень защищенности
Центральный архив медицинских изображений	2 - й уровень защищенности

1. При 4-м уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечивает сохранность носителей персональных данных;
- утверждает перечень работников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

2. При 3-м уровне защищенности персональных данных работодатель дополнительно к мерам, перечисленным в пункте 1 настоящего приложения, назначает должностное лицо (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

3. При 2-м уровне защищенности персональных данных работодатель дополнительно к мерам, перечисленным в пунктах 1, 2 настоящего приложения, ограничивает доступ к содержанию электронного журнала сообщений, за исключением для должностных лиц (работников), которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

4. При 1-м уровне защищенности персональных данных работодатель дополнительно к мерам, перечисленным в пунктах 1-3 настоящего приложения:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работника по доступу к персональным данным, содержащимся в информационной системе;
- создает структурное подразделение, ответственное за обеспечение безопасности персональных данных в информационной системе, либо возлагает на одно из структурных подразделений функции по обеспечению такой безопасности.