

УТВЕРЖДАЮ

Директор ООО «МКС «БЕЛАЯ ЛАДЬЯ»

_____ /Грейлих А.В./

«01» июня 2022г.

Положение

о порядке работы с персональными данными работников

ООО «МКС «БЕЛАЯ ЛАДЬЯ».

1. Общие положения

1.1. Настоящее Положение принято в ООО «МКС «БЕЛАЯ ЛАДЬЯ» (далее - Организация) для обеспечения сохранности и конфиденциальности персональных данных работников Организации в соответствии с требованиями действующего законодательства Российской Федерации, а также в целях регламентации порядка работы с персональными данными работников Организации.

1.2. Настоящее Положение разработано в соответствии с Уставом Организации и:

Конституцией Российской Федерации от 12 декабря 1993 г.;

Указом Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Трудовым кодексом Российской Федерации от 30.12.2001 N 197-ФЗ

Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Приказом Роскомнадзора от 24.02.2021 N 18 "Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения";

1.3. Организация обрабатывает персональные данные субъектов персональных данных, исключительно в целях их трудоустройства, оформления трудовых отношений, получения ими образования и продвижения по службе, контроля количества и качества выполняемой ими работы, обеспечения безопасности субъектов персональных данных и сохранности имущества.

2. Основные понятия, используемые в Положении

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

Оператор 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) с персональными данными, совершаемые с использованием средств автоматизации или без их использования.

Обработка персональных данных включает в себя в том числе:

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

Субъекты персональных данных: работники Организации, кандидаты на замещение вакантных должностей, а также родственники работников;

Персональные данные, разрешенные субъектом персональных данных для распространения - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 N 152-ФЗ "О 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.

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

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

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с Федеральным законодательством не распространяется требование соблюдения конфиденциальности.

2. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

2.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в разделе 3 настоящего Положения.

2.2. Организация обрабатывает персональные данные следующих категорий субъектов персональных данных.

2.2.1. Кандидаты для приема на работу в Организацию:

- фамилия, имя, отчество;
- пол;
- гражданство;

- дата и место рождения;
- номер контактного телефона или сведения о других способах связи;
- сведения об образовании, опыте работы, квалификации;
- иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах.

2.2.2. Работники Организации:

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата и место рождения;
- изображение (фотография);
- паспортные данные;
- адрес регистрации по месту жительства;
- адрес фактического проживания;
- номер контактного телефона или сведения о других способах связи;
- индивидуальный номер налогоплательщика (ИНН);
- страховой номер индивидуального лицевого счета (СНИЛС);
- полис обязательного медицинского страхования;
- сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации;
- семейное положение, наличие детей, родственные связи;
- сведения о трудовой деятельности, в том числе наличие поощрений, наградений и (или) дисциплинарных взысканий;
- данные о регистрации брака;
- сведения о воинском учете;
- сведения об инвалидности;
- сведения об удержании алиментов;

- сведения о доходе с предыдущего места работы;
- наличие (отсутствии) судимости;
- наличие (отсутствие) медицинских противопоказаний для работы;
- номер индивидуального лицевого счета, дата его открытия, номер банковской карты;
- иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.

2.2.3. Члены семьи работников Организации:

- фамилия, имя, отчество;
- степень родства с работником Организации;
- год рождения;
- иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.

2.3. Организацией не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных».

2.3. Обработка Организацией биометрических персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность) осуществляется в соответствии с законодательством Российской Федерации.

2.4. К биометрическим персональным данным работника относится фотоизображение и видеоизображение работника необходимое для размещения в информационно-телекоммуникационной сети Интернет на корпоративном сайте Организации.

2.5. Биометрические данные обрабатываются Организацией только при наличии письменного согласия работника.

2.6. При приеме на работу работник должен быть ознакомлен с Положением под подпись до подписания трудового договора.

3. Порядок и условия сбора, получения и обработки персональных данных

3.1. Под получением (сбором) персональных данных понимается последовательность действий, связанных с установлением достоверности соответствующих данных, а также размещением их в информационных системах.

Сбор персональных данных осуществляется в пределах установленного объема,

необходимого для каждой категории субъектов, с которыми взаимодействует Организация, и не может превышать указанный объем.

3.2. Обработка персональных данных должна осуществляться на законной и справедливой основе. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.3. Обработка персональных данных осуществляется в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- ведение бухгалтерского учета;
- начисления заработной платы;
- исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления Организацией установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ;
- предоставления сведений в кредитную организацию для оформления банковской карты и перечисления на нее заработной платы;
- предоставления налоговых вычетов;
- обеспечения безопасности субъекта персональных данных;
- контроля количества и качества выполняемой работы;
- обеспечения сохранности имущества Организации
- повышения профессиональной репутации работников
- осуществление пропускного режима.

3.4. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

3.5. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

3.6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

3.7. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено Организации:

- непосредственно;
- с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

3.8. Согласие субъекта персональных данных должно включать в себя, в частности:

- фамилию, имя, отчество,
- адрес субъекта персональных данных,
- номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес Организации, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Организации, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Организацией способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено Федеральным законодательством;
- подпись субъекта персональных данных.

3.9. Организация должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

3.10. Организация осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

3.11. К обработке персональных данных допускаются работники Организации, в должностные обязанности которых входит обработка персональных данных.

3.12. Обработка персональных данных осуществляется путем:

- получения персональных данных в устной и письменной форме непосредственно от

субъектов персональных данных;

- получения персональных данных из общедоступных источников;
- внесения персональных данных в журналы, реестры и информационные системы Организации;
- использования иных способов обработки персональных данных.

3.13. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

3.14. Организация осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом или локально-нормативными актами Организации.

3.15. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Организация обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Федеральном законе 152-ФЗ «О персональных данных».

4. Порядок и условия передачи, блокирования, хранения и уничтожения персональных данных

4.1. Под передачей персональных данных понимается операция:

- по адресному размещению соответствующих данных на носителях и серверах, доступ к которым имеют работники Организации либо третьи лица;
- по размещению персональных данных в источниках внутрикорпоративного документооборота;
- по опубликованию в интересах Организации персональных данных о работнике в СМИ или на серверах Интернета в соответствии с нормами законодательства Российской Федерации.

4.2. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

4.3. Передача персональных данных работника осуществляется с учетом специфики конкретной информационной системы:

- в цифровой информационной системе (предназначенной для автоматизированной обработки персональных данных) передача данных осуществляется по защищенным каналам связи, а также при задействовании средств криптозащиты;

- в информационной системе на основе бумажных носителей передача данных осуществляется посредством перемещения или копирования содержимого данных носителей при участии работников Организации, имеющих доступ к соответствующей информационной системе, который устанавливается отдельным локальным правовым актом.

4.4. Передача персональных данных субъектов персональных данных третьим лицам осуществляется Организацией только с письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в других случаях, предусмотренных федеральным законодательством.

4.5. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

4.6. Организация обязана обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на распространение персональных данных.

4.7. В случае если из предоставленного субъектом персональных данных согласия на распространение персональных данных не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются Организацией без права распространения.

4.8. В случае если из предоставленного субъектом персональных данных согласия на передачу персональных данных не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных или не указал категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, Организация обрабатывает такие персональные данные без возможности передачи (распространения, предоставления, доступа) неограниченному кругу лиц.

4.9. В согласии на распространение персональных данных субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных Организации неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ Организации в установлении субъектом персональных данных запретов и условий не допускается.

4.10. Организация обязуется в срок не позднее трех рабочих дней с момента получения согласия субъекта персональных данных на распространение персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных пациента для распространения.

4.11. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по его требованию. Данное требование должно включать в себя

фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению.

4.12. Действие согласия субъекта персональных данных на распространение персональных данных, прекращается с момента поступления Организации требования.

4.13. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или обратиться с таким требованием в суд.

Организация или третье лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования пациента или в срок, указанный во вступившем в законную силу решении суда. Если такой срок в решении суда не указан, то Организация или третье лицо обязано прекратить передачу персональных данных пациента в течение трех рабочих дней с момента вступления решения суда в законную силу.

4.14. Организация обеспечивает ведение Журнала учета передачи персональных данных субъектов персональных данных по запросам третьих лиц, в котором регистрируются поступившие запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных, а также отмечается, какая именно информация была передана.

4.15. В случае если лицо, обратившееся с запросом, не уполномочено Федеральным законодательством на получение персональных данных субъекта персональных данных, либо отсутствует письменное согласие субъекта персональных данных на передачу его персональных данных, Организация обязана отказать в предоставлении персональных данных. В данном случае лицу, обратившемуся с запросом, выдается мотивированный отказ в предоставлении персональных данных в письменной форме, копия отказа хранится в Организации.

4.16. Под блокированием персональных данных понимается временный запрет на осуществление каких-либо операций с персональными данными, которые находятся в информационных системах Организации, в случаях, предусмотренных положениями локальных правовых актов Организации и законодательства Российской Федерации.

4.17. Блокирование персональных данных в Организации осуществляется с учетом специфики конкретной информационной системы:

- в цифровой информационной системе блокирование данных осуществляется посредством закрытия доступа к файлам при задействовании средств криптозащиты;

- в информационной системе на основе бумажных носителей блокирование данных осуществляется посредством закрытия доступа к соответствующей информационной системе для определенных групп работников.

4.18. Под хранением персональных данных понимается совокупность операций, направленных на обеспечение целостности соответствующих персональных данных.

4.19. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом № 152-ФЗ «О персональных данных», договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

4.20. Хранение осуществляется в следующих формах: на бумажном носителе и посредством их размещения в информационных системах Организации.

4.21. Хранение персональных данных осуществляется с учетом специфики конкретной информационной системы:

- в цифровой информационной системе хранение данных осуществляется на ПК руководителя Организации или главного бухгалтера Организации, а также на облачных серверах;

- в информационной системе на основе бумажных носителей хранение данных осуществляется в архиве Организации или главного бухгалтера Организации, в помещениях предназначенных для этих целей и защищенных от несанкционированного доступа.

4.22. Под уничтожением персональных данных понимается операция по изъятию соответствующих данных из информационных систем Организации, а также обеспечению невозможности их восстановления.

4.23. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законодательством.

4.24. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Организация обязана прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Организацией и пациентом, либо если Организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом 152-ФЗ «О персональных данных» или Федеральным законодательством.

4.25. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Организация осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен Федеральным законодательством.

4.26. Уничтожение персональных данных осуществляется с учетом специфики конкретной информационной системы:

- в цифровой информационной системе ликвидация данных осуществляется посредством их удаления с ПК руководителя Организации или главного бухгалтера Организации, а также серверов;

- в информационной системе на основе бумажных носителей уничтожение данных осуществляется посредством уничтожения соответствующих носителей с помощью специальных технических средств.

4.27. Организация обеспечивает ведение Журнала учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных.

5. Организация доступа к персональным данным

5.1. Доступ к персональным данным субъектов персональных данных имеют:

- руководитель Организации;
- главный бухгалтер;
- старший администратор;
- субъект персональных данных;

5.2. Доступ к персональным данным субъектов персональных данных Организации для иных лиц может быть разрешен только отдельным распоряжением руководителя Организации.

5.3. Работники Организации и другие лица, имеющие доступ к персональным данным, обязаны:

- осуществлять операции с персональными данными при соблюдении норм, установленных настоящим Положением, а также действующим законодательством Российской Федерации;
- информировать своего непосредственного руководителя и руководителя Организации о нештатных ситуациях, связанных с операциями с персональными данными;
- обеспечивать конфиденциальность операций с персональными данными;
- обеспечивать сохранность и неизменность персональных данных в случае, если выполняемая задача не предполагает их корректировки или дополнения.

5.4. Лица, получившие доступ к персональным данным субъектов персональных данных в обязательном порядке подписывают обязательство о неразглашении персональных данных субъекта персональных данных, полученных в рамках своих должностных обязанностей.

6. Защита персональных данных субъекта персональных данных

6.1. Организация при обработке персональных данных субъектов персональных данных обязана 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.

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

6.3. Обеспечение безопасности персональных данных субъекта персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;
- назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Организации;
- создает необходимые условия для работы с персональными данными;
- организует учет документов, содержащих персональные данные;
- 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; применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных; обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 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; контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.4. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона № 152-ФЗ «О персональных данных».

6.5. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона 152-ФЗ «О персональных данных».

6.6. Для обеспечения безопасности персональных данных субъекта персональных данных при неавтоматизированной обработке предпринимаются следующие меры:

- определяются места хранения персональных данных, которые оснащаются средствами защиты: в кабинетах, где осуществляется хранение документов, содержащих персональные данные субъектов персональных данных, имеются сейфы, шкафы, стеллажи, тумбы; дополнительно кабинеты, где осуществляется хранение документов, оборудованы замками и системами охранной (пультовая) и пожарной сигнализаций, обеспечивающих защиту от несанкционированного доступа;

- передача информации, содержащей сведения о персональных данных субъекта персональных данных, по телефону, факсу, электронной почте без письменного согласия субъекта персональных данных запрещается.

- организация использует услуги вневедомственной охраны.

6.7. Все действия по неавтоматизированной обработке персональных данных субъекта персональных данных осуществляются должностными лицами, для кого предусмотрен допуск к ним согласно решению руководителя Организации в объеме, необходимом данным лицам для выполнения своей трудовой функции.

6.8. При обработке персональных данных на материальных носителях не допускается фиксация на одном материальном носителе тех данных, цели обработки которых заведомо не совместимы.

6.9. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если не имеется возможности осуществлять их отдельно, должны быть приняты следующие меры:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) только копия;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Эти меры применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

6.10. 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).

6.11. Персональные данные субъекта персональных данных, содержащиеся на материальных носителях уничтожаются по Акту об уничтожении персональных данных.

6.12. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

6.13. Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6.14. Для обеспечения безопасности персональных данных субъекта персональных данных при автоматизированной обработке предпринимаются следующие меры:

- все действия при автоматизированной обработке персональных данных субъекта персональных данных осуществляются только должностными лицами, согласно Списку должностей, утвержденного приказом руководителя Организации, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

6.15. Персональные компьютеры, имеющие доступ к базам хранения персональных данных субъекта персональных данных, защищены паролями доступа.

Пароли устанавливаются специалистом IT-отдела и сообщаются индивидуально работнику, допущенному к работе с персональными данными и осуществляющему обработку персональных данных пациентов на данном ПК.

6.16. Иные меры, предусмотренные локальным актом по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

7. Права работников в части осуществления операций с персональными данными

7.1. Работник Организации, передавший Организации свои персональные данные, имеет право:

- на полную информацию о своих персональных данных и обработке этих данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на

получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством РФ. - на получение доступа к соответствующим данным в любой момент в целях осуществления необходимых операций с ними;

- требовать от Организации дополнительной обработки, блокирования или ликвидации персональных данных, если операции с ними противоречат интересам работника, осуществляются незаконно, а также в случае, если персональные данные недостоверны;

- получать от Организации информацию о лицах, имеющих доступ к персональным данным, а также о статистике обращений к персональным данным с их стороны;

- получать от Организации информацию о дополнительной обработке, блокировании или ликвидации персональных данных, осуществленных по инициативе Организации;

- на определение своих представителей для защиты своих персональных данных;

- на доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;

- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных трудовым законодательством. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия;

- обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите его персональных данных.

7.2. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом РФ.

- своевременно, в срок, не превышающий 5 дней с момента регистрации изменений персональных данных, сообщать работодателю об изменении своих персональных данных.

- соблюдать настоящее Положение.

- сохранять конфиденциальность полученных персональных данных;

7.3. Работники Организации, имеющие доступ к персональным данным работников Организации, имеют право:

- на приобретение полномочий, необходимых в целях осуществления операций с персональными данными;

- получение консультационной поддержки со стороны руководства и других компетентных работников в части осуществления операций с персональными данными;

- отдачу распоряжений и направление предписаний работникам, передающим персональными данные Организации, связанных с необходимостью предоставления дополнительной или уточняющей информации в целях обеспечения корректного осуществления операций с персональными данными.

8. Ответственность работников за нарушения правил осуществления операций с персональными данными

8.1. Работники Организации при осуществлении операций с персональными данными несут административную, дисциплинарную и уголовную ответственность за нарушения правил осуществления операций с персональными данными, установленных настоящим Положением, а также нормами федерального законодательства Российской Федерации, региональными и муниципальными правовыми актами.

8.2. Правовые последствия нарушений правил осуществления операций с персональными данными определяются исходя из локальных норм Организации, а также положений законодательства Российской Федерации.

9. Конфиденциальность персональных данных

9.1. Информация, относящаяся к персональным данным субъекта персональных данных, является конфиденциальной информацией и охраняется независимо от воли субъекта персональных данных.

Исключение составляют персональные данные, находящиеся в общедоступных базах персональных данных.

9.2. В целях обеспечения сохранности и конфиденциальности персональных данных субъектов персональных данных все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только работниками отдела кадров и бухгалтерии, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

9.3. Лица, допущенные приказом руководителя Организации к работе с персональными данными субъекта персональных данных в обязательном порядке перед началом работы подписывают соглашение о не разглашении персональных данных.

9.4. Работа с персональными данными должна осуществляться только в целях, по перечням и в сроки, которые необходимы для выполнения задач соответствующего держателя персональных данных, установленных действующим законодательством, лицензией и (или) договором.

6.5. Работа с персональными данными должна производиться с соблюдением мер обеспечения их конфиденциальности и охраны, предотвращающих нанесение вреда субъекту персональных данных.

9.6. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, в соответствии с приказами по архивному делу, или продлевается на основании заключения экспертной комиссии Организации, если иное не определено законодательством Российской Федерации.

10. Заключительные положения

10.1. Настоящее Положение вступает в действие с момента утверждения его приказом руководителя Организации и действует до утверждения нового положения.

10.2. Все изменения и дополнения к настоящему Положению должны быть утверждены приказом руководителя Организации.

10.3. Настоящее Положение распространяется на всех субъектов персональных данных Организации, а также лиц, имеющих доступ и осуществляющих перечень действий с персональными данными субъектов персональных данных.

10.4. Субъекты персональных данных и работники имеющих доступ и осуществляющих перечень действий с персональными данными субъектов персональных данных, подлежат ознакомлению с данным документом в установленном порядке под личную подпись.

10.5. Документы, определяющие порядок обработки персональных данных субъектов персональных данных, подлежат размещению на официальном сайте и/или информационном стенде Организации.