Приложение 1

УТВЕРЖДЕНО
Приказом № _____от «_____»_____2019 г.

Генеральный директор
ООО «ЛДЦ «Семейная клиника «МЕДА»
_____ /Маслов Г.А./

ПОЛИТИКА
ОБРАБОТКИ и ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ЛЕЧЕБНО-ДИАГНОСТИЧЕСКИЙ ЦЕНТР «СЕМЕЙНАЯ КЛИНИКА «МЕДА»

г. Санкт-Петербург
2019 год

Часть 1. Общие положения

1.1. Целью разработки документа «Политика обработки и защиты персональных данных» (далее – «Политика»), является обеспечение соблюдения требований Федерального закона от 27.06.2006г. № 152-ФЗ «О персональных данных», установление правил по обработке и защите персональных данных Работников Общества с ограниченной ответственностью «ЛДЦ «семейная клиника «МЕДА» (далее – «Оператор»), а также персональных данных третьих лиц от несанкционированного доступа, неправомерного их использования или утраты, а также обеспечение законных прав и интересов Оператора, его Работников и третьих лиц в связи с необходимостью получения (сбора), систематизации, хранения, передачи сведений составляющих персональные данные Работников и третьих лиц.

1.2. **Правовые основания обработки персональных данных**

1.2.1. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных.

1.2.2. Оператор обрабатывает персональные данные на основании: статей Конституции РФ, Трудового кодекса Российской Федерации; Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, Федерального закона «О персональных данных». Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» и принятых на его основе нормативно-правовых актов, регулирующих отношения, связанные с оказанием медицинских услуг; иных федеральных законов и прочих нормативных правовых актов; устава Оператора; договоров, заключаемых между Оператором и субъектами персональных данных; согласий на обработку персональных данных.

1.3. *Персональные данные Работника* - любая информация, относящаяся к конкретному Работнику (субъекту персональных данных) и необходимая Оператору в связи с трудовыми отношениями.

Персональные данные третьих лиц – любая информация, относящаяся к конкретному физическому лицу и необходимая Оператору для исполнения своих договорных обязательств, а также для оказания услуг клиентам.

1.4. Сведения о персональных данных Работников и третьих лиц относятся к числу конфиденциальных (составляющих охраняемую законом тайну Оператора). Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания
- по истечении 75 лет срока их хранения
- в других случаях, предусмотренных федеральными законами

1.5. Настоящая Политика утверждается, вводится в действие и изменяется Приказом Генерального директора, является обязательным для исполнения всеми Работниками Оператора.

1.6. С Политикой должны быть ознакомлены все Работники Оператора под личную подпись. Работники, имеющие доступ к персональным данным, подписывают «Обязательство об обеспечении конфиденциальности персональных данных сотрудниками ООО «ЛДЦ «Семейная клиника «МЕДА».

1.7. Для целей настоящей Политики используются следующие основные понятия:

персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных

данных) (п. 1 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ)

оператор персональных данных (оператор) – учреждение, самостоятельно или совместно с другими лицами организующее и(или) осуществляющее обработку персональных данных, а так же, определяющее цели обработки, 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 (п. 3 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ)

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники; (п. 4 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ)

распространение персональных данных - действия, направленные на раскрытие персональных данных Работников неопределенному кругу лиц (п. 5 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ)

предоставление персональных данных - действия, направленные на раскрытие персональных данных Работников определенному лицу или определенному кругу лиц (п. 6 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ)

блокирование персональных данных - временное прекращение обработки персональных данных Работников (за исключением случаев, если обработка необходима для уточнения персональных данных) (п. 7 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ)

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных Работников и (или) в результате которых уничтожаются материальные носители персональных данных Работников (п. 8 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ)

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному Работнику (п. 9 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ)

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу (п. 11 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ)

информационная система персональных данных – совокупность содержащихся в базе данных и обеспечивающих их обработку информационных технологий и технических средств

информация - сведения (сообщения, данные) независимо от формы их представления

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить

такую информацию или ее материальный носитель

субъект персональных данных – физическое лицо, данные которого обрабатываются

конфиденциальность персональных данных – обязательное для оператора и иных лиц, получивших доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом

1.8. **Основные права и обязанности Оператора персональных данных**

1.8.1. Оператор при сборе персональных данных обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных.

1.8.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

1.8.3. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети интернет, Оператор обязан обеспечить 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 Федеральном законе «О персональных данных».

1.8.4. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

1.8.5. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике, к сведениям о реализуемых требованиях к защите персональных данных. Оператор в случае осуществления сбора персональных данных с использованием информационно-телекоммуникационных сетей обязан опубликовать в соответствующей информационно-телекоммуникационной сети Политику и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием соответствующей информационно-телекоммуникационной сети.

1.8.6. 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.

1.8.7. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

1.9. **Основные права и обязанности субъекта персональных данных**

1.9.1. Субъект персональных данных вправе требовать от Оператора уточнения его

персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
1.9.2. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных.
1.9.3. Принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы разрешается только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.
1.9.4. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.
1.9.5. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
1.9.6. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
1) подтверждение факта обработки персональных данных оператором;
2) правовые основания и цели обработки персональных данных;
3) цели и применяемые оператором способы обработки персональных данных;
4) наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;
5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6) сроки обработки персональных данных, в том числе сроки их хранения;
7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
10) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.
1.9.7. Указанные выше сведения должны быть предоставлены субъекту персональных данных Оператором в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
1.9.8. Сведения, указанные в пункте 1.9.6., предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе сведения, подтверждающие участие субъекта

персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

1.9.9. В случае если сведения, указанные в пункте 1.9.6, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 1.9.6., и ознакомления с такими персональными данными не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

1.9.10. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 1.9.6., а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 1.9.9., в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 1.9.6., должен содержать обоснование направления повторного запроса.

1.9.11. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 1.9.8. и 1.9.9. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

1.9.12. Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 дней с даты получения запроса субъекта персональных данных или его представителя.

1.9.13. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

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

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

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

1.9.17. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если

обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки.
1.9.18. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.
1.9.19. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.
1.9.20. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.
1.9.21. В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.
1.9.22. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) 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 Оператора) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого,

выгодоприобретателем или поручителем
по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.
1.9.23. В случае отсутствия возможности уничтожения персональных данных в течение указанных сроков Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

1.10. **Цели сбора персональных данных**

1.10.1. Оператор обрабатывает персональные данные в целях:
– оформления трудовых отношений, ведения кадрового делопроизводства, содействия в трудоустройстве, обучении, повышении по службе, пользовании различными льготами и гарантиями, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и сохранности имущества;
– заключения, исполнения и прекращения гражданско-правовых договоров;
– оказания медицинских услуг, в том числе идентификации пациентов (заказчиков), отражения информации в медицинской документации, предоставления сведений страховым компаниям (в случае оплаты ими оказываемых услуг), предоставления установленной законодательством отчетности в отношении оказанных медицинских услуг;
– выполнения требований действующего законодательства;
– в иных случаях, установленных в законе, уставе Оператора.
1.10.2. Обработка персональных данных должна осуществляться на законной и справедливой основе.
1.10.3. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
1.10.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
1.10.5. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
1.10.6. 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.

1.11. Категории субъектов персональных данных

1.11.1. Категории субъектов персональных данных, чьи данные обрабатываются.
1.11.2. Работники Оператора, бывшие работники, кандидаты на трудоустройство, а также члены семьи работников.
1.11.3. Пациенты, законные представители пациентов.
1.11.4. Прочие клиенты и контрагенты Оператора (физические лица).
1.11.5. Представители/работники клиентов и контрагентов Оператора (юридических лиц).

1.12. Доступ к персональным данным Работника имеют следующие уполномоченные лица:

- Генеральный директор
- Главный врач
- Сотрудники Оператора или лицо (организация), с которыми Оператором заключен договор на выполнение бухгалтерских услуг
- Сотрудники Оператора или лицо (организация), с которыми Оператором заключен договор на ведение кадрового учета

- Сотрудники Оператора или лицо (организация), с которыми Оператором заключен договор на обслуживание ИТ – инфраструктуры
- Сотрудники Оператора, наделенные полномочиями в соответствии с соответствующими внутренними локальными нормативными актами

1.13. Доступ к персональным данным третьих лиц, поступивших в распоряжение Оператора, ограничивается Работниками Оператора и не подлежит передаче за пределы территории Оператора без письменного согласия субъектов персональных данных.

1.14. Оператор организует обработку персональных данных в следующем порядке:
1) назначает ответственного за организацию обработки персональных данных, устанавливает перечень лиц, имеющих доступ к персональным данным;
2) издает настоящую Политику, локальные акты по вопросам обработки персональных данных;
3) применяет правовые, организационные и технические мер по обеспечению безопасности персональных данных;
4) осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Оператора;
5) осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяет соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом;
6) знакомит работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политики, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

1.15. Порядок обработки персональных данных в информационных системах
1.15.1. Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.
1.15.2. Обеспечение безопасности при обработке персональных данных, содержащихся в информационных системах органов и подведомственных организаций, осуществляется в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.
1.15.3. Уполномоченному работнику, имеющему право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными обязанностями работника.
1.15.4. Информация может вноситься как в автоматическом режиме при получении персональных данных с официального сайта в сети интернет, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

1.15.5. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах органов, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.
1.15.6. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.
1.15.7. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:
– идентификация и аутентификация субъектов доступа и объектов доступа;
– управление доступом субъектов доступа к объектам доступа;
– ограничение программной среды;
– защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
– регистрация событий безопасности;
– антивирусная защита; – обнаружение (предотвращение) вторжений;
– контроль (анализ) защищенности персональных данных;
– обеспечение целостности информационной системы и персональных данных;
– обеспечение доступности персональных данных;
– защита среды виртуализации и технических средств;
– защита информационной системы, ее средств, систем связи и передачи данных;
– выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
– управление конфигурацией информационной системы и системы защиты персональных данных.
1.15.8. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.
Угрозы первого типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.
Угрозы второго типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.
Угрозы третьего типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.
Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных».
1.15.9. В соответствии с пунктом 11 статьи 19 Федерального закона «О персональных данных» под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
При обработке персональных данных в информационных системах устанавливаются четыре уровня защищенности персональных данных.

1.15.9.1. Необходимость обеспечения первого уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:
а) для информационной системы актуальны угрозы первого типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;
б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.
1.15.9.2. Необходимость обеспечения второго уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:
а) для информационной системы актуальны угрозы первого типа и информационная система обрабатывает общедоступные персональные данные;
б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;
в) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает биометрические персональные данные;
г) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные персональные данные более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;
д) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;
е) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.
1.15.9.3. Необходимость обеспечения третьего уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:
а) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные персональные данные сотрудников Оператора или общедоступные персональные данные менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;
б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;
в) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;
г) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает биометрические персональные данные;
д) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.
1.15.9.4. Необходимость обеспечения четвертого уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:
а) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает общедоступные персональные данные;
б) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора

или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.
1.15.10. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

1.16. К системным администраторам применяются следующие требования:

1.16.1. В обязанности системного администратора входит управление учетными записями пользователей информационных систем, содержащих персональные данные, поддержание штатной работы таких систем, обеспечение резервного копирования таких данных, а также установка и конфигурирование аппаратного и программного обеспечения информационных систем, не связанного с обеспечением безопасности персональных данных в системах, кроме следующих соблюдения следующих требований:

- Требования конфиденциальности
- Требования целостности и доступности, предъявляемые к конкретной системе
- Требования безопасности, установленные действующим законодательством

1.16.2. В обязанности системного администратора входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации информационных систем, учет и хранение машинных носителей персональных данных, периодический аудит и анализ защищенности систем, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности персональных данных.

1.16.3. Квалификационные требования и детальный перечень прав и обязанностей системного администратора закрепляются в должностной инструкции, с которой сотрудник должен быть ознакомлен под личную подпись.

1.17. На общей территории медицинского центра Оператора, расположенного по адресу: 196601, Санкт-Петербург, Пушкин, ул. Архитектора Данини, 11/6, помещения 23-Н,25-Н ведется видеонаблюдение, все телефонные разговоры записываются.

Часть 2. Персональные данные Работников

2.1. Обработка персональных данных Работников

2.1.1. В состав персональных данных Работника входят:

- анкетные и биографические данные
- образование
- сведения о трудовом и общем стаже
- сведения о составе семьи
- паспортные данные
- данные СНИЛС, ИНН
- сведения о воинском учете
- сведения о заработной плате сотрудника
- сведения о социальных льготах
- специальность
- занимаемая должность
- наличие судимостей
- адрес места жительства
- домашний и мобильный телефоны
- содержание трудового договора
- состав декларируемых сведений о наличии материальных ценностей
- содержание декларации, подаваемой в налоговую инспекцию
- подлинники и копии приказов по личному составу
- личные дела и трудовые книжки сотрудников
- основания к приказам по личному составу
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям
- копии отчетов, направляемые в органы статистики
- и иная информация, позволяющая идентифицировать Работников

2.1.2. Документы, содержащие сведения, перечисленные в п. 2.1.1. являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

2.1.3. При оформлении Работника на работу в обработку Оператора могут попадать следующие анкетные и биографические данные Работника:

- общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные)
- сведения о воинском учете
- данные о приеме на работу
- сведения об аттестации
- сведения о повышенной квалификации
- сведения о профессиональной переподготовке
- сведения о наградах (поощрениях), почетных званиях
- сведения об отпусках
- сведения о социальных гарантиях
- сведения о месте жительства и о контактных телефонах

2.1.4. Персональные данные родственников работников обрабатываются в объеме, переданном работником и необходимом для предоставления гарантий и компенсаций работнику, предусмотренных трудовым законодательством:
– фамилия, имя, отчество;

– дата и место рождения;
– серия и номер документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
– серия и номер свидетельства о рождении ребенка, сведения о выдаче указанного документа и выдавшем его органе;
– серия и номер свидетельства о заключении брака, сведения о выдаче указанного документа и выдавшем его органе.

Источником информации обо всех персональных данных Работника является непосредственно Работник. Если персональные данные возможно получить только у третьей стороны, то Работник должен быть заранее в письменной форме уведомлен об этом и от него должно быть получено письменное согласие. Работодатель обязан сообщить Работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа Работника дать письменное согласие на их получение.

2.1.5. Оператор (Работодатель) не имеет права получать и обрабатывать персональные данные Работника о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ Работодатель вправе получать и обрабатывать данные о частной жизни Работника только с его письменного согласия.

2.1.6. В случае, если с письменного согласия Работника его персональные данные, такие как фамилия, имя, отчество, год и место рождения, адрес, сведения о профессии и иные персональные данные были включены в общедоступные источники персональных данных (справочники, адресные книги, социальные сети, иные источники в сети Интернет), такие данные являются общедоступными персональными данными, т. е. данными, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.1.7 . Обработка персональных данных Работников Обществом возможна без их согласия только в следующих случаях:

- персональные данные являются общедоступными
- персональные данные относятся к состоянию здоровья Работника, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия Работника невозможно
- по требованию полномочных государственных органов - в случаях, предусмотренных федеральным законом

2.1.8. Работодатель вправе обрабатывать персональные данные Работников только с их письменного согласия.

2.1.9. Письменное согласие Работника на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных
- 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, а также порядок его отзыва

2.1.10. Согласие Работника не требуется в следующих случаях:
- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия Работодателя
- обработка персональных данных в целях исполнения трудового договора
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов Работника, если получение его согласия невозможно

2.1.11. Работник Оператора представляет в структуру, осуществляющую кадровый учет, достоверные сведения о себе. Оператор имеет право проверять достоверность сведений.

2.1.12. В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина руководитель Оператора и его законные, полномочные представители при обработке персональных данных Работника должны выполнять следующие общие требования:

2.1.12.1. Обработка персональных данных может осуществляться **исключительно в целях** обеспечения соблюдения законов или иных правовых актов, содействия Работникам в трудоустройстве, получении образования и профессиональном продвижении, обеспечения личной безопасности Работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.1.12.2. При определении объема и содержания обрабатываемых персональных данных Оператор (Работодатель) должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.

2.1.12.3. При принятии решений, затрагивающих интересы Работника, Оператор (Работодатель) не имеет права основываться на персональных данных, полученных о нем исключительно в результате их автоматизированной обработки или электронного получения. Оператор (Работодатель) учитывает личные качества Работника, его добросовестный и эффективный труд.

2.1.12.4. Защита персональных данных Работника от неправомерного их использования, утраты обеспечивается Оператором (Работодателем) за счет его средств в порядке, установленном федеральным законом.

2.1.13. Во всех случаях отказ Работника от своих прав на сохранение и защиту тайны недействителен.

2.1.14. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

2.1.15. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении,

о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

2.2. Передача персональных данных

2.2.1. При передаче персональных данных Работника Оператор (Работодатель) должен соблюдать следующие требования:

2.2.1.1. Не сообщать персональные данные Работника третьей стороне без письменного согласия Работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника, а также в случаях, установленных федеральным законом.

2.2.1.2. Не сообщать персональные данные Работника в коммерческих целях без его письменного согласия. Обработка персональных данных Работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия. Предварительное согласие может быть также выражено путем подписания трудового договора на определенную должность, если должностной инструкцией предусмотрены продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов и передача персональных данных таких Работников для возможности последующей связи с ним или идентификации.

2.2.1.3. Предупредить лиц, получивших персональные данные Работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные Работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными Работников в порядке, установленном федеральными законами.

2.2.1.4. Осуществлять передачу персональных данных Работников в пределах территории Оператора в соответствии с настоящим Положением.

2.2.1.5. Разрешать доступ к персональным данным Работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

2.2.1.6. Не запрашивать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Работником трудовой функции.

2.2.1.7. Передавать персональные данные Работника его законным, полномочным представителям в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции.

2.2.2. Персональные данные Работников обрабатываются и хранятся в подразделении, ведущем кадровый учет.

2.2.3. Персональные данные Работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

2.2.4. При получении персональных данных не от самого Работника (за исключением случаев, если персональные данные являются общедоступными) Оператор (Работодатель) до начала обработки таких персональных данных обязан предоставить Работнику следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя
- цель обработки персональных данных и ее правовое основание
- предполагаемые пользователи персональных данных
- установленные федеральными законами права субъекта персональных данных

2.2.5. Без письменного согласия Работника передача персональных данных может осуществляться в следующие органы и организации:

- **налоговые органы**
- **правоохранительные органы**
- **военкоматы**
- **Фонд социального страхования**
- **Пенсионный фонд**
- **Фонд обязательного медицинского страхования**
- **Государственные инспекции труда**
- а также иным органам, организациям и лицам, которые в соответствии с действующим законодательством вправе запрашивать информацию, содержащую персональные данные Работника

2.2.6. В случае обращения к Оператору (Работодателю) любых третьих лиц за информацией о персональных данных Работника (за исключением тех, кто указан в п. 2.2.5. Положения), такая информация может быть представлены только с письменного согласия Работника.

2.2.7. В случае необходимости, персональные данные Работников могут быть переданы за пределы РФ. Трансграничная передача возможна лишь после получения согласия Работника в письменном виде.

2.2.8. **Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу**. В случае если Работник желает получить кредит в каком-либо банке, то он самостоятельно должен предупредить Работодателя о том, что его персональные данные могут быть переданы по телефону сотрудникам банка во избежание отказа в выдаче кредита из-за не подтверждения сведений, указанных Работником в анкете банка. Работник заранее должен дать Работодателю разрешение в письменном виде с указанием тех данных, которые могут быть переданы по телефону лицам, которых Работодатель не имеет реальной возможности идентифицировать.

2.3. Доступ к персональным данным

2.3.1. Указанные в п. 1.12. лица имеют право обрабатывать персональные данные в целях, указанных в п. 2.1.12.1. настоящей Политики с соблюдением законодательства РФ и настоящего документа.

2.3.2. Список лиц может изменяться Приказом Генерального директора Оператора. Список лиц, имеющих доступ к персональным данным, должен поддерживаться в актуальном состоянии.

2.3.3. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

2.4. Хранение персональных данных

2.4.1. Хранение персональных данных Работников осуществляется на бумажных и электронных носителях и должно происходить в порядке, исключающем их утрату или их неправомерное использование.

2.4.2. Документы на бумажных носителях, содержащие персональные данные Работника (копии паспорта, диплома, военного билета, водительского удостоверения, заграничного паспорта и т.п.), автобиография, заявления, Трудовая книжка, заполненная форма Т-2, экземпляр трудового договора (экз. работодателя), приказ о приеме на работу и т.д. хранятся у Оператора (Работодателя).

Оператор (Работодатель и его представители) обязан обеспечить каждому Работнику возможность ознакомления с документами и материалами, непосредственно связанными с трудовой деятельностью Работника.

2.4.3. Выдача Работнику копий документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы; выписки из трудовой книжки; справки о заработной плате, о начисленных и фактически уплаченных страховых взносах на обязательное пенсионное страхование, о периоде работы у данного Работодателя и другое), осуществляется по письменному заявлению Работника Работодателем (его представителями) не позднее трех рабочих дней со дня подачи этого заявления. Копии документов, связанных с работой, должны быть заверены надлежащим образом и предоставляться Работнику безвозмездно.

2.4.4. Оператор (Работодатель) обеспечивает безопасное хранение персональных данных на бумажных носителях, содержащихся в личных карточках Работников, в запирающемся шкафу, расположенном в запирающемся кабинете. Трудовые книжки Работников хранятся в сейфе. Оператор (Работодатель) обеспечивает безопасное хранение персональных данных в электронном виде на персональных компьютерах Генерального директора, главного врача, сотрудников отдела бухгалтерии и отдела кадров с ограниченным доступом. Пользование такой информацией на компьютерах осуществляется только при введении имени пользователя и пароля. Инструкция по применению парольной политики в информационных системах персональных данных утверждена Приказом №____ от «___» _____ 20__ г.

2.5. Защита персональных данных

2.5.1. Все меры конфиденциальности при сборе, обработке и хранении персональных данных Работника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

2.5.2. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

2.5.3. Защита персональных данных Работника от неправомерного их использования или утраты обеспечивается Оператором (Работодателем) за счет его средств в порядке, установленном федеральным законом.

2.5.4. Для обеспечения внутренней защиты персональных данных Работников Оператор осуществляет ряд мер:

- ограничение и регламентация состава Работников, функциональные обязанности которых связаны с доступом к персональным данным
- строгое избирательное и обоснованное распределение документов и информации между Работниками
- рациональное размещение рабочих мест Работников, при котором исключалось бы бесконтрольное использование защищаемой информации
- знание Работником требований нормативно-методических документов по защите информации и сохранении тайны
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных
- организация порядка уничтожения информации или передачи в архив
- своевременное выявление нарушения требований разрешительной системы доступа к персональным данным Работников
- проведение обучения для Работников, имеющих доступ к персональным данным Работников Оператора, по разъяснению норм действующего законодательства о персональных данных для предупреждения нарушений при работе с персональными данными и конфиденциальными документами. Обучение проводиться ежегодно с проставлением отметок в Журнал обучения
- установление специального пароля для доступа к персональным данным, хранящимся на электронных носителях
- контроль за работой Работников, имеющих доступ к персональным данным
- разработана Инструкция по работе пользователей информационных систем, содержащих персональные данные
- разработана Инструкция по работе с носителями персональных данных
- разработана Инструкция по организации антивирусной защиты информационных систем, содержащих персональные данные
- разработана Инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем, содержащих персональные данные
- разработана Инструкция по работе ответственного за организацию обработки персональных данных
- разработана Инструкция по применению парольной политики в информационных системах персональных данных

2.5.5. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

2.5.6. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, посетители, Работники других отделов. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

2.5.7. Внешняя защита осуществляется путем установления:

- порядка приема, учета и контроля деятельности посетителей
- технических средств охраны, сигнализации
- порядка охраны помещений
- требований к защите информации при интервьюировании и собеседованиях

2.5.8. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны не разглашать персональные данные Работников.

2.5.9. По возможности персональные данные обезличиваются.

2.5.10. Кроме мер защиты персональных данных, установленных законодательством, работодатели, Работники и их представители могут вырабатывать совместные меры защиты персональных данных Работников.

2.6. Права и обязанности Работников

2.6.1. В целях защиты персональных данных, хранящихся у Работодателя, Работник имеет право:

- требовать исключения или исправления неверных, или неполных персональных данных
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения
- определять своих представителей для защиты своих персональных данных
- на сохранение и защиту своей личной и семейной жизни

2.6.2. Работник обязан:

- передавать Оператору (Работодателю) или его представителю комплекс достоверных документированных персональных данных, состав которых установлен Трудовым кодексом РФ и иными федеральными законами
- своевременно сообщать Оператору (Работодателю) об изменении своих персональных данных

2.6.3. В случае внесения изменений и (или) дополнений в персональные данные Работника Оператор (Работодатель) обязан уведомить об этом Работника или его законного представителя, а также третьих лиц, которым персональные данные этого Работника были переданы.

2.6.4. В целях защиты частной жизни, личной и семейной тайны Работники не должны отказываться от своего права на обработку персональных данных, поскольку это может повлечь причинение морального, материального вреда.

2.7. Уничтожение персональных данных Работников

2.7.1. Бумажные носители информации, содержащие персональные данные Работников Оператора, при достижении целей обработки, или при наступлении иных законных оснований, (например, увольнения), подлежат уничтожению в соответствии с законодательством РФ. В случаях, если Оператор предполагает, что персональные

данные по каким-либо причинам могут потребоваться в будущем, то носители, содержащие такие данные, подлежат отправке в Архив, на основании Приказа.

2.7.2. Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются. Уничтожение информации на электронных носителях происходит путем стирания или физического воздействия, вызывающего разрушение носителя.

2.7.3. Уничтожение производится в присутствии комиссии, состоящей минимум из трех человек, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (состав комиссии утверждается Приказом).

2.7.4. После уничтожения материальных носителей членами комиссии подписывается Акт в двух экземплярах (Приложение 1), в описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

Часть 3. Персональные данные третьих лиц

3.1. Оператор может получать персональные данные третьих лиц любым законным способом. Персональные данные третьих лиц – информация, относящаяся к:

- Кандидатам для приема на работу
- Учредителям Оператора (Общества)
- Лицам, связанным с Работниками Оператора и учредителями, персональные данные которых стали известны для исполнения требований законодательства
- Клиентам
- Сотрудникам контрагентов
- Иным физическим лицам, персональные данные которых получены законным способом

В состав персональных данных третьих лиц входит любая информация, ставшая известной Оператору на законных основаниях, способная идентифицировать конкретного человека.

3.2. В отношении пациентов обрабатываются:
– фамилия, имя, отчество;
– пол;
– возраст;
– дата и место рождения;
– адреса места жительства и регистрации;
–серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
– данные страхового свидетельства государственного пенсионного страхования;
– гражданство;
– данные о состоянии здоровья, в том числе биометрические персональные данные;
– семейное и социальное положение;
– контактный телефон;
– адрес электронной почты;
– реквизиты полиса обязательного медицинского страхования;
– реквизиты полиса (договора) добровольного медицинского страхования;
– тип занятости;
– место работы;
– должность.

3.3. В отношении категорий «Прочие клиенты и контрагенты Оператора (физические лица)» и «Представители/работники клиентов и контрагентов Оператора (юридических лиц)» обрабатываются:
– фамилия, имя, отчество;
– пол;
– возраст;
– дата и место рождения;
– адреса места жительства и регистрации;
– контактный телефон;
– адрес электронной почты;
– серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе.

3.4. В отношении законных представителей или представителей по доверенности указанных лиц обрабатываются:
– фамилия, имя, отчество;
– пол;
– возраст;

– дата и место рождения;
– адреса места жительства и регистрации;
– контрактный телефон;
– адрес электронной почты;
– серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
– сведения о документе, который подтверждает полномочия представителя.
– данные страхового свидетельства государственного пенсионного страхования;
– гражданство;
– данные о состоянии здоровья, в том числе биометрические персональные данные;
– семейное и социальное положение;
– контактный телефон;
– адрес электронной почты;
– реквизиты полиса обязательного медицинского страхования;
– реквизиты полиса (договора) добровольного медицинского страхования;
– тип занятости;
– место работы;
– должность.

3.5. Заключая договора с контрагентами, Оператор возлагает обязанность по получению разрешения на передачу/получение персональных данных сотрудников контрагента и третьих лиц на самого контрагента, тем самым, уменьшая риск незаконного распоряжения персональными данными в рамках исполнения условий заключенного договора.

3.6. Оператор передает персональные данные третьих лиц другим третьим лицам для исполнения каких-либо целей предусмотренных договором между Оператором и третьим лицом, получающим данные. Договор должен содержать условия хранения персональных данных получаемой стороной, а также требования не передачи полученных данных другим лицам.

3.7. Использование персональных данных третьих лиц ограничивается целями, для которых такие данные получены. Цели обработки персональных данных сотрудников контрагентов регулируется договорами с контрагентами. Цели обработки персональных данных третьих лиц включают, но не ограничиваются следующими целями: маркетинговое продвижение товаров и услуг Оператора и партнеров Оператора; информирование по телефону, электронной почте, по почте по адресу о товарах, работах, услугах Оператора и партнеров Оператора; и т.д.

3.8. Соискатели на вакансии Оператора при заполнении анкет должны предоставлять свое согласие на обработку персональных данных, указанных в анкетах, так как на момент прохождения собеседования и заполнения анкеты трудовых отношений между Оператором и соискателем еще нет.

3.9. Получение согласия на обработку персональных данных клиентов по гражданско-правовым договорам не требуется, если субъектом персональных данных является сам клиент как сторона по договору. Однако, в случае получения от субъекта заявки на бронирование до момента подтверждения брони в виде заключения договора, договорных отношений с Оператором еще не возникает, в связи с этим, Оператор должен получать согласие субъекта на обработку его персональных данных.

3.10. В случае, если договор, заключаемый между Оператором и клиентом предусматривает предоставление услуг иным лицам, кроме клиента непосредственно подписавшего договор, то согласие на обработку персональных данных должно быть получено непосредственно у этого лица (родственника, сопровождающего и .т.д.). Клиент должен оказывать Оператору содействие в получении такого согласия у третьего лица.

3.11. Обработка персональных данных детей в возрасте до 18 лет возможна лишь с согласия их родителей или иных законных представителей.

3.12. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни допускается лишь в случае, если субъект персональных данных дал согласие в письменном виде на обработку таких данных.

3.13. Работники обязуются получать и обрабатывать специальные категории персональных данных третьих лиц, в том числе данные о состоянии здоровья, только с письменного согласия субъекта, полученного в письменной форме.

3.14. В случае формирования и направления заявки на бронирование услуг Оператора через официальный сайт Оператора, Оператор обязан получать согласие на обработку персональных данных субъектов. Это может быть сделано путем проставления знака «V», подтверждающего согласие, во всплывающем окне (Чек-боксе), содержащем текст согласия на обработку персональных данных, непосредственно перед направлением заявки Оператору. Кроме того, на сайте Оператора должен быть размещен текст Политики конфиденциальности, с которым посетитель сайта может ознакомиться перед отправкой своей заявки на бронирование услуг.

3.15. Вне зависимости от того, получил ли Оператор согласие на обработку персональных данных субъекта в электронном виде, Оператор должен впоследствии получить такое согласие в письменном виде в случае, если субъект становиться клиентом и/или передает Оператору какие-либо сведения о состоянии своего здоровья и интимной жизни, расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждениях.

3.16. Контрагент Оператора, а также субъект персональных данных имеют право требовать от Оператора подтверждение факта защиты переданных персональных данных, а также подтверждение того, что переданные персональные данные используются только для тех целей, для которых они получены.

3.17. Хранение персональных данных клиентов на бумажных носителях (договоры, согласия, амбулаторные карты, заключения) осуществляется в медицинском центре Общества в помещениях № 25-Н, а именно на архивных полках. Хранение и обработка персональных данных клиентов в электронном виде осуществляется на компьютерах, на каждом из которых установлен логин и пароль. Доступ к персональным данным третьих лиц в электронной форме имеют только те сотрудники, у которых есть соответствующие обязанности согласно должностной инструкции.

3.18. Общество прикладывает усилия для предотвращения несанкционированного доступа к персональным данным посторонними лицами путем внедрения мероприятий по внешней защите, перечисленных в п. 2.5.7. Положения. Кроме того, внутренняя защита обеспечивается с помощью регламентов, содержащихся в:

- Инструкции по работе пользователей информационных систем, содержащих персональные данные
- Инструкции по работе с носителями персональных данных
- Инструкции по организации антивирусной защиты информационных систем, содержащих персональные данные
- Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем, содержащих персональные данные

3.19. Уничтожение персональных данных сотрудников контрагентов происходит в случае расторжения договоров оказания услуг, и/или по письменному заявлению субъекта персональных данных, и/или в случае утраты необходимости в достижении цели для которой эти данные получены. Уничтожение персональных данных третьих лиц происходит в случае отзыва персональных данным самими субъектами. До отзыва согласия, Общество не уничтожает персональные данные третьих лиц в течение 20 лет, если иное не утверждено приказом Генерального директора с указанием целей продления или сокращения срока обработки персональных данных.

3.20. Согласие может быть отозвано субъектом персональных данных в любой момент путем направления письменного уведомления Обществу не менее чем за 30 дней до предполагаемой даты отзыва.

3.21. В случае отзыва субъектом персональных данных своего согласия, Оператор вправе продолжить обработку персональных данных без согласия субъекта, если это необходимо для целей исполнения заключенного с этим субъектом договора, а также в случаях, предусмотренных действующим законодательством.

3.22. Уничтожение персональных данные третьих лиц производится аналогично уничтожению персональных данных Работников и регламентируется п. 2.7. Положения. В случае, если у Общества есть основания полагать, что персональные данные могут потребоваться по истечении 20 лет, то на основании Приказа Генерального директора уничтожение персональных данных третьих лиц может производиться путем передачи в личный архив в виде отдельно хранящихся подписанных запечатанных коробок.

Часть 4. Видеофиксация и запись телефонных разговоров

4.1. Видеофиксация со звукозаписывающим устройством

4.1.1. Видеофиксация ведется с целью:

- контроля качества работы Работников
- соблюдения условий безопасности в медицинском центре Оператора, являющемся общественным заведением
- предотвращения нарушений требований законодательства Работниками и третьими лицами, посещающими медицинский центр Оператора
- охраны имущества Оператора

4.1.2. При входе в медицинский центр Оператора происходит информирование всех входящих о производимой видеофиксации. Информирование заключается в наличии соответствующей вывески на видном месте.

4.1.3. Видеонаблюдение ведется на всей территории медицинского центра, в том числе в кабинетах врачей, являющимися Работниками Оператора.

4.1.3. Запись видео осуществляется путем кольцевой записи на электронный носитель. Срок хранения записи – 2 недели. После окончания двухнедельного срока видеозапись стирается путем записи в память носителя новой записи.

4.1.4. Оператор имеет право пользоваться полученной информацией по своему усмотрению в пределах и в соответствии с законодательством РФ. Персональные данные, ставшие известными Оператору в результате ознакомления с видеозаписями считаются полученными с согласия субъекта персональных данных, так как, соглашаясь войти в медицинский центр Оператора и увидев соответствующее предупреждение о видеофиксации, субъект автоматически дает свое согласие на обработку его изображения и персональных данных, которые можно получить путем обработки видеоизображения.

4.1.5. Доступ к записям видеонаблюдения имеют системный администратор, Генеральный директор, главный врач и старший администратор Оператора. На основании Приказа Генерального директора фрагменты видеозаписи могут быть записаны на постоянный носитель и/ или переданы другим лицам.

4.2. Запись телефонных разговоров

4.2.1. Запись телефонных разговоров как внешних, так и внутренних производиться с целью контроля качества работы Работников, с целью охраны законных интересов Оператора с целью контроля за соблюдением коммерческой тайны.

4.2.2. При осуществлении входящего звонка на телефонные номера Оператора происходит включение автоматического информирования о том, что телефонный разговор будет записан.

4.2.3. Оставаясь на линии после прослушивания информационного сообщения о том, что разговор будет записан, звонящий субъект автоматически дает согласие на аудиофиксацию разговора с Работником Оператора. Работникам Оператора, звонящим друг другу по внутренней телефонной сети, аудиосообщение не включается для целей экономии времени.

4.2.4. Работники Оператора информируются о том, что разговоры записываются, единожды при приеме на работу.

4.2.5. Работник несет ответственность за ту информацию, которая может быть получена Обществом исходя из прослушивания телефонного разговора.

4.2.6. Срок хранения телефонных аудиозаписей – 1 год. Запись разговоров осуществляется автоматически на электронный носитель. По истечении срока хранения аудиозапись стирается.

4.2.7. Доступ к аудиозаписи имеют системный администратор, Генеральный директор, главный врач и старший администратор Оператора. На основании Приказа Генерального директора фрагменты аудиозаписи могут быть записаны на постоянный носитель и/ или переданы другим лицам.

4.2.8. Оператор имеет право пользоваться полученной информацией по своему усмотрению. Персональные данные, ставшие известными Оператору в результате прослушивания аудиозаписей телефонных разговоров считаются полученными с согласия субъекта персональных данных, так как, соглашаясь осуществить звонок, субъект автоматически дает свое согласие на обработку его голоса и тех персональных данных, которые можно получить в результате воспроизведения аудиозаписи.

Часть 5. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

5.1. Работники, имеющие доступ к персональным данным других Работников (п. 1.12. Политики) и/или третьих лиц и виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных Работников и/или третьих лиц, несут:

1) дисциплинарную ответственность, в том числе путем применения дисциплинарного взыскания – увольнения за разглашение персональных данных
2) полную материальную ответственность за разглашение персональных данных Работников
3) а также могут привлекаться к гражданско-правовой, административной и уголовной ответственности в соответствии с федеральными законами.

5.2. Иные Работники, получившие несанкционированный доступ к персональным данным других Работников и/или третьих лиц, и разгласившие эти данные 3-м лицам, тем самым нарушившие положения настоящей Политики, несут:

1) дисциплинарную ответственность
2) материальную ответственность
3) а также могут привлекаться к гражданско-правовой, административной и уголовной ответственности в соответствии с федеральными законами.

Приложение 1
к Политике обработки и защиты персональных данных работников и третьих лиц

ООО «ЛДЦ «Семейная клиника «МЕДА»,
утвержденному Приказом № ____ от «___»_____2019г.

Типовая форма
Акта об уничтожении носителей, содержащих персональные данные

Акт № _____
об уничтожении носителей, содержащих персональные данные

Комиссия в составе:
Председатель – _____
Члены комиссии – _____

провела отбор бумажных, электронных, магнитных и оптических носителей персональных данных (далее - Носители) и установила, что в соответствии с действующим законодательством Российской Федерации, они подлежит уничтожению. Комиссия составила настоящий Акт о том, что произведено уничтожение носителей персональных данных в составе:

№ п/п	Дата уничтожения	Тип носителя	Учетный номер носителя	Категория информации	Примечание

Всего носителей _____
(цифрами и прописью количество)

На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители персональных данных уничтожены путем
_____.
(разрезания/сжигания/размагничивания/физического уничтожения/ механического уничтожения / иного способа)

Председатель комиссии: _____ /_____/

Члены комиссии: _____ /_____/

_____ /_____/