

Общество с ограниченной ответственностью
«ЛадаМед»

УТВЕРЖДАЮ

Директор ООО «ЛадаМед»

 Е.Г. Дегтярева

(приложение № 1 к Приказу № _____
от « 21 » марта 2023г.



ПОЛИТИКА
информационной безопасности информационных систем
персональных данных ООО «ЛадаМед»

Сыктывкар, 2023

Оглавление

1. Общие положения.....	3
1.1. Назначение документа.....	3
1.2. Область действия.....	3
1.3. Вступление в силу документа.....	3
2. Сведения об Обществе.....	3
2.1. Реквизиты.....	3
2.2. Исполнение политики.....	4
3. Понятие и состав персональных данных.....	4
3.2. Субъекты персональных данных:.....	4
3.3. Состав.....	4
3.4. Цели обработки.....	6
3.5. Биометрические персональные данные.....	7
3.6. Специальные категории персональных данных.....	8
4. Обработка персональных данных.....	8
4.1. Общие сведения.....	8
4.2. Сбор.....	8
4.3. Хранение.....	9
4.4. Передача.....	9
4.5. Трансграничная передача.....	10
4.6. Общедоступные источники.....	10
4.7. Поручение обработки.....	10
5. Права сторон.....	10
5.1. Права субъектов персональных данных.....	10
5.2. Права Общества.....	11
6. Защита персональных данных.....	12
7. Заключительные положения.....	14

1. Общие положения

1.1. Назначение документа

1.1.1. Важнейшим условием реализации деятельности Общества является обеспечение необходимого и достаточного уровня информационной безопасности персональных данных (далее по тексту ПДн) и процессов, в рамках которых они обрабатываются.

1.1.2. Обеспечение безопасности ПДн является одной из приоритетных задач ООО «ЛадаМед» (далее по тексту – Общества/ООО).

1.1.3. Обработка и обеспечение безопасности ПДн, осуществляется в ООО в соответствии с законодательством РФ, в частности Федеральным законом №152 от 27.06.2006г. «О персональных данных», Постановлением Правительства РФ №1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК №21 от 18.02.2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Область действия

1.2.1. Настоящая Политика определяет принципы, порядок и условия обработки ПДн различных категорий субъектов, чьи ПДн обрабатываются в ООО, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2.2. Положения настоящей Политики распространяются на весь объем ПДн, обрабатываемых Обществом, полученных как до, так и после вступления ее в силу, а также на всех субъектов ПДн.

1.3. Вступление в силу документа

1.3.1. Настоящая Политика вступает в силу с момента ее утверждения и действует бессрочно до замены ее новой Политикой.

1.3.2. В соответствии с п.2 ст.18.1 ФЗ «О персональных данных»: доступ к настоящему документу не может быть ограничен.

1.3.3. Настоящая Политика подлежит изменению, дополнению в случае внесения изменений в действующие законодательные акты и появления новых законодательных актов, и специальных нормативных документов по обработке и защите ПДн, но не реже одного раза в 5 (пять) лет.

2. Сведения об Обществе

2.1. Реквизиты

2.1.1. Полное наименование: Общество с ограниченной ответственностью «ЛадаМед»

2.1.2. ИНН / КПП: 1101073215 / 110101001.

2.1.3. Юридический адрес: 167000, Республика Коми, г. Сыктывкар, ул.

Орджоникидзе, д.33/45.

2.1.4. Телефон: 8(8212) 39-13-26.

2.2. Исполнение политики

2.2.1. С целью исполнения настоящей Политики директором утверждены:

- Положение об обработке и защите ПДн;
- Перечень обрабатываемых ПДн;
- Перечень работников, допущенных к неавтоматизированной обработке ПДн;
- Перечни прав доступа к ресурсам информационных системе ПДн;
- Перечень выделенных помещений для обработки ПДн;
- Списки лиц, имеющих право самостоятельного доступа выделенные помещения;
- Перечень хранилищ ПДн и их материальных носителей;
- Планы проведения резервного копирования ПДн в информационных системах ПДн;
- иные локальные нормативные акты, принимаемые во исполнение требований законодательства Российской Федерации в области обработки и защиты ПДн.

3. Понятие и состав персональных данных

3.1. Понятия и определения

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

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

3.2. Субъекты персональных данных:

ООО осуществляет обработку ПДн следующих субъектов ПДн:

- работники Общества;
- пациенты Общества/ законные представители пациента

3.3. Состав

Обществом обрабатываются следующие категории ПДн:

3.3.1. ПДн работников:

Первичные сведения

- ФИО;

- Дата рождения;
- Место рождения;
- Адрес прописки;
- Гражданство;
- Номера телефонов.

Сведения о реквизитах документов

- Паспортные данные (серия, номер, кем и когда выдан);
- ИНН;
- СНИЛС;
- Страховой медицинский полис (серия, номер, дата);
- Номер расчетного (лицевого) счета.

Сведения о трудовой деятельности

• Трудовой стаж (места работы, должности, периоды работы, причины увольнения);

- Сведения о трудовой книжке (№, серия, дата выдачи, записи в ней);
- Должность;
- Табельный номер;
- Сведения о повышении квалификации, переподготовке;
- Сведения о трудовом договоре;
- Сведения о командировках, отпусках;
- Сведения о временной нетрудоспособности;
- Сведения о поощрениях и наградах.

Сведения о социальном положении

- Семейное положение;
- Состав семьи;
- Сведения о социальном статусе;
- Сведения о социальных льготах.

Сведения об образовании

- Уровень образования;
- Наименование образовательного учреждения;
- Сведения о документах, подтверждающих образование (наименование, номер, дата выдачи);
- Специальность;
- Квалификация;
- Форма профессионального послевузовского образования;
- Ученая степень;
- Ученое звание.

Сведения о финансовом обеспечении

- Тарифная ставка (оклад);
- Надбавка;
- Данные о начисленных денежных средствах (заработная плата и т.д.);
- Тип и сумма налогового вычета.

Дополнительные сведения

- Сведения о состоянии на воинском учете;
- Специальные знания и специальные подготовки.

3.3.2. ПДН пациентов:

Первичные сведения

- ФИО;
- Адрес и место жительства;
- Адрес и место работы;
- Номера телефонов;
- Сведения о социальных льготах.

Сведения о реквизитах документов

- СНИЛС;
- Страховой медицинский полис (серия, номер, дата);
- Паспортные данные;

Сведения о трудовой деятельности

- Место работы;
- Структурное подразделение;
- Должность.

Медицинские сведения

- Сведения об ограниченных возможностях здоровья;
- Хронические и острые заболевания;
- Противопоказания и медотводы;
- Сведения об аллергии;
- Сведения о медосмотрах, обследованиях;
- Снимки/ графики (рентген/кардиограмма).

3.3.3. ПДН законных представителей пациента:

Первичные сведения

- ФИО;

Сведения о реквизитах документов

- Паспортные данные;
- Сведения документов, подтверждающих, что субъект является законным представителем пациента;
- Номер телефонов.

3.4. Цели обработки

3.4.1. Обработка ПДн **работников** ООО осуществляется исключительно в целях:

- обеспечения соблюдения конституционных прав работников, а также норм и требований законодательства РФ о государственной социальной помощи, о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях, трудового законодательства;
- исполнения обязательств и функций работодателя;
- содействия в осуществлении трудовой (служебной) деятельности и учета результатов исполнения договорных обязательств;
- обучения, повышения квалификации и продвижения по службе;
- предоставления льгот;
- контроля количества и качества выполняемой работы;
- обеспечения личной безопасности.
- Обработка ПДн работников ООО осуществляется на основании Соглашения на обработку ПДн, Трудового кодекса РФ, Постановления Государственного Комитета РФ по статистике от 5 января 2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты».

• Обработка ПДн работников прекращается в случаях:

- достижения целей обработки ПДн;
- расторжения трудового договора (служебного контракта) или по его окончании.

3.4.2. Обработка ПДн **пациентов** осуществляется в целях:

- создание условий для обеспечения гарантий прав граждан на оказание медицинской помощи надлежащего качества и в соответствующем объеме, а также профилактики заболеваний, сохранения и укрепления физического и психического здоровья каждого человека, поддержания его долголетней активной жизни, предоставления ему медицинской помощи;
- создание условий для осуществления контроля за использованием средств обязательного медицинского страхования, а так же оборотом медицинских аппаратов;
- определение потребности в объемах медицинской помощи;
- предупреждение распространения опасных заболеваний, представляющих угрозу безопасности граждан РФ.

Обработка ПДн пациентов осуществляется на основании:

- соглашения на обработку ПДн;
- п. 2 – п. 11 ч. 1, ст. 6 и ч. 2 ст. 10 Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных»;

- ч. 4 ст. 13 Федерального закона №323-ФЗ от 21.11.2011 г. «Об охране здоровья граждан в Российской Федерации».

Обработка ПДн пациентов прекращается в случаях достижения целей обработки ПДн.

3.5. Биометрические персональные данные

3.5.1. Сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн) Обществом не обрабатываются.

3.6. Специальные категории персональных данных

3.6.1. Сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни (специальные категории ПДн) Обществом обрабатываются в соответствии с пп. 1, 2.3, 3, 4 п. 2 статьи 10 ФЗ №152-ФЗ от 27.07.2006г. «О персональных данных».

4. Обработка персональных данных

4.1. Общие сведения

4.1.1. Обработка ПДн в ООО осуществляется на основе принципов:

- законности и справедливости целей и способов обработки ПДн;
- соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям ООО;
- соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих ПДн;
- хранения ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
- уничтожения по достижении целей обработки ПДн или в случае утраты необходимости в их достижении, если иное не предусмотрено федеральным законом.

4.1.2. Общество осуществляет обработку ПДн с использованием средств автоматизации, в том числе с использованием информационных технологий и технических средств, включая средства вычислительной техники, средства и системы передачи, приема и обработки ПДн, программные средства, средства

защиты информации, применяемые в информационных системах, а также без использования средств автоматизации.

4.2. Сбор

4.2.1. ПДн субъектов ПДн Общество получает напрямую от субъектов ПДн или их законных представителей.

4.2.2. В случае возникновения необходимости получения ПДн субъекта ПДн от третьей стороны, Общество извещает об этом субъекта ПДн заранее и сообщает ему о целях, предполагаемых источниках и способах получения ПДн.

4.2.3. Для получения ПДн субъекта ПДн от третьей стороны Общество сначала получает его письменное согласие.

4.3. Хранение

4.3.1. Общество хранит ПДн и их материальные носители в порядке, исключающем их утрату, неправомерное использование или несанкционированный доступ к ним.

4.3.2. Общество хранит ПДн субъектов ПДн и их материальные носители не дольше, чем этого требуют цели их обработки и требования действующего законодательства Российской Федерации, и уничтожает их по истечению установленных сроков хранения.

4.3.3. Сроки хранения документов, содержащих ПДн субъектов ПДн, а также сроки хранения сведений, содержащих ПДн субъектов ПДн в электронном виде (электронные документы, записи баз данных) определяются Перечнем обрабатываемых ПДн в соответствии с Приказом Росархива от 20.12.2019 №236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», номенклатурой дел, сроком исковой давности, а также иными требованиями законодательства Российской Федерации. Сроки хранения первичной медицинской документации установлены согласно приказу Минздрава СССР от 04.10.1980 г. Об утверждении форм первичной медицинской документации учреждений здравоохранения, действующему на основании письма Минздравсоцразвития РФ от 30.11.2009 N14-6/242888.

4.3.4. При обработке ПДн на бумажных носителях Обществам обеспечивается выполнение требований «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденного постановлением Правительства РФ от 15 сентября 2008 г. №687.

4.3.5. При обработке ПДн на машинных носителях или в информационных системах ПДн Обществам обеспечивается выполнение «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства РФ от 1

ноября 2012 г. №1119.

4.4. Передача

4.4.1. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки ПДн, а также в интересах субъектов ПДн, Общество в ходе своей деятельности предоставляет ПДн субъектов ПДн следующим организациям:

- Федеральная налоговая служба России;
- Социальный фонд России;
- Негосударственные пенсионные фонды;
- Органы социального страхования;
- Банки;
- Государственные и муниципальные органы управления;
- Территориальные органы федеральных органов исполнительной власти;
- Страховые компании;
- Медицинские учреждения;
- Военкомат;
- Правоохранительные органы;
- Органы прокуратуры и ФСБ;
- Органы лицензирования и сертификации;
- Органы государственной статистики;
- Министерство здравоохранения Республики Коми.

4.5. Трансграничная передача

4.5.1. Передача ПДн на территорию иностранных государств, органам власти иностранных государств, иностранным физическим или юридическим лицам (трансграничная передача ПДн) Обществом не осуществляется.

4.6. Общедоступные источники

4.6.1. Общество не осуществляет формирование общедоступных источников ПДн (справочников, адресных книг).

4.7. Поручение обработки

4.7.1 Общество вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

4.7.2 Общество самостоятельно осуществляет обработку ПДн субъектов ПДн и не поручает ее третьим лицам.

5. Права сторон

5.1. Права субъектов персональных данных

5.1.1. Субъект ПДн имеет право на получение сведений об обработке его ПДн Обществом.

5.1.2. Субъект ПДн вправе требовать от ООО уточнения своих ПДн, их

блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.1.3. Субъекты ПДн имеют право запрашивать у ООО следующие сведения:

- подтверждение факта обработки ПДн Обществом;
- правовые основания и цели обработки ПДн;
- используемые Обществом способы обработки ПДн;
- наименование и адрес местонахождения ООО, сведения о лицах (за исключением работников ООО), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Обществом или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных законодательством Российской Федерации;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению ООО, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные законодательством Российской Федерации.

5.1.4. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами.

5.1.5. Для реализации своих прав и защиты законных интересов субъект ПДн имеет право обратиться в Общество. Общество рассматривает любые обращения и жалобы со стороны субъектов ПДн, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

5.1.6. Субъект ПДн вправе обжаловать действия или бездействие ООО в уполномоченный орган по защите прав субъектов ПДн (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Управление по защите прав субъектов ПДн) или в судебном порядке.

5.1.7. Субъект ПДн имеет право на защиту своих прав и законных

интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

5.1.8. Субъект ПДн имеет право в любое время отозвать свое согласие на обработку ПДн, обратившись в Общество.

5.2. Права Общества

5.2.1. Общество, как оператор ПДн, вправе:

- отстаивать свои интересы в суде;
- предоставлять ПДн субъектов государственным и иным уполномоченным органам, если это предусмотрено действующим законодательством РФ (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении ПДн в случаях предусмотренных законодательством РФ;
- обрабатывать ПДн субъекта без его согласия, в случаях предусмотренных законодательством РФ.

6. Защита персональных данных

6.1. Общество гарантирует конфиденциальность ПДн и предоставляет доступ к ним только уполномоченным работникам, подписавшим обязательство о неразглашении ПДн.

6.2. Все работники ООО, имеющие доступ к ПДн, соблюдают правила их обработки и выполняют требования по их защите.

6.3. Общество принимает все необходимые правовые, организационные и инженерно-технические меры, достаточные для защиты ПДн от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

6.4. Обеспечение безопасности ПДн достигается в частности:

- назначением ответственных за организацию обработки и защиты ПДн;
- разработкой документов, определяющих порядок обработки и защиты ПДн;
- определением порядка доступа в помещения, где обрабатываются ПДн, а также порядка доступа к ресурсам информационных систем ПДн;
- определением актуальных угроз безопасности ПДн и возможного вреда субъектам ПДн;
- резервированием ПДн, а также определением порядка их восстановления;
- использованием средств защиты информации в информационных системах ПДн;

- учетом машинных носителей, содержащих ПДн;
- определением мест хранения носителей ПДн;
- осуществлением внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, локальным актам;
- ознакомлением работников ООО, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, локальными актами в отношении обработки ПДн, и (или) обучением указанных работников, сбором обязательств о неразглашении ПДн;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационных систем ПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- регистрацией и учетом всех действий, совершаемых с ПДн в информационных системах ПДн;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн.

7. Заключительные положения

7.1. Настоящая Политика является внутренним документом и подлежит размещению в общедоступном месте.

7.2. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки ПДн в Обществе.

7.3. Ответственность должностных лиц ООО, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн, определяется в соответствии с законодательством Российской Федерации, и внутренними документами ООО.

7.4. Все вопросы и предложения по внесению изменений или дополнений в настоящую Политику следует направлять на имя ответственного за организацию обработки ПДн. Ответственный за организацию обработки ПДн назначается приказом Общества.
