

УТВЕРЖДАЮ

ген. директор

ООО «Байкальский Медицинский Легион»

Корниенко В.Н.

ПОЛИТИКА

ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И РЕАЛИЗУЕМЫХ ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящая Политика обработки персональных данных и реализуемых требований к защите персональных данных (далее — Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных и действует в отношении всей информации, которую ООО «Байкальский Медицинский Легион» может получить в рамках осуществления своей деятельности. Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и предназначена для ознакомления неограниченного круга лиц.

Политика разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом российской Федерации, Гражданским кодексом российской Федерации, Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными федеральными и нормативно-правовыми актами.

В Политике определены требования к персоналу оператора, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных (ИСПДн) оператора.

ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является обеспечение безопасности объектов защиты оператора в информационных системах от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационных систем.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для субъектов.

Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в главе II «Правовой режим обработки персональных данных», подлежащих защите.

Область действия:

Требования настоящей Политики распространяются на всех работников оператора (штатных, временных, работающих по контракту и т.п. физических лиц и их законных представителей).

ОСНОВНЫЕ ПОНЯТИЯ

В настоящей Политике используются следующие основные понятия:

- **персональные данные работника** - любая информация, относящаяся к прямо или косвенно определенному или определяемому на основании такой информации сотруднику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;

- **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, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, удаление, уничтожение персональных данных работников ООО «Байкальский Медицинский Легион»;

- **конфиденциальность персональных данных** - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять

персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

- **использование персональных данных действия** - (операции) с персональными данными, совершаемые сотрудником ООО «Байкальский Медицинский Легион» в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников, пациентов и их законных представителей либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных сотрудников, пациентов и их законных представителей, и (или) в результате которых уничтожаются материальные носители персональных данных сотрудников;

- **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия работника, пациента и их законных представителей или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

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

I ПРАВОВОЙ РЕЖИМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Сведения об обработке персональных данных

Обработка персональным данными осуществляется Оператором на законной и справедливой основе, правовым основанием для обработки являются:

- Конституция российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
- Федеральный закон от 06.12.2001 № 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

- Федеральный закон от [5 12 2010] № [67-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

- Федеральный закон от 16.07 1999 № 165-ФЗ «Об основах обязательного социального страхования»;

- Федеральный закон от 29.12.2006 № 225-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;

- Постановлением Правительства РФ от 04.10.2012 № 1006 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг»;

- Лицензия № ЛО41-01108-38/00288131 от 24.12.2020 выданная Министерством здравоохранения Иркутской области; согласием на обработку персональных данных, локальными актами организации;

- Устав ООО «Байкальский Медицинский Легион»;

- Иные нормативно-правовые акты Российской Федерации.

2. Категории субъектов персональных данных

В ООО «Байкальский Медицинский Легион» обрабатываются персональные данные следующих категорий субъектов персональных данных:

- работников (лиц, состоящих в трудовых отношениях с ООО «Байкальский Медицинский Легион»;

- пациентов и их законных представителей, обратившихся в ООО «Байкальский Медицинский Легион»;

- иных лиц, давших согласие на обработку своих персональных данных, либо сделавших общедоступными свои персональные данные или чьи персональные данные получены из общедоступного источника, а также в других случаях, предусмотренных законодательством Российской Федерации.

3. Категории обрабатываемых персональных данных

ООО «Байкальский Медицинский Легион» обрабатывает следующие категории персональных данных:

3.1. Работники: фамилия, имя, отчество; год рождения, месяц рождения, дата рождения, место рождения; адрес; семейное положение; образование; профессия; паспортные данные: серия, номер паспорта, кем и когда выдан; гражданство; адрес регистрации и фактического проживания; телефонный номер (домашний, рабочий, сотовый); сведения о составе семьи; идентификационный номер налогоплательщика (ИНН); СНИЛС; трудовая деятельность до приема на работу, сведения о трудовом и общем стаже, место работы, занимаемая должность;

наличие судимостей; данные о трудовом договоре; данные личных дел, данные трудовой книжки: номер, серия, и дата заполнения трудовой книжки; сведения о квалификации, сведения о переподготовке, ученая степень, ученое звание, данные о повышении квалификации, информация о знании иностранных языках; сведения о наличии специальных знаний или специальной подготовки; сведения о воинском учете; данные о орденах, наградах, медалях, поощрениях, почетных званиях; сведения о заработной плате; социальных льготах, временная нетрудоспособность и иные документы, предусмотренные локальными актами и действующим законодательством.

3.2. Пациенты, граждане, получающие медицинские услуги: фамилия, имя, отчество; год рождения, месяц рождения, дата рождения, место рождения; адрес; пол, паспортные данные: серия, номер паспорта, кем и когда выдан, гражданство, адрес места жительства, телефонный номер (домашний, рабочий, сотовый), данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью,

4. Цели обработки персональных данных

4.1. Исполнение положений нормативных правовых актов.

4.2. Оформление трудовых отношений, ведение кадрового учета, начисление и выплата заработной платы.

4.3. Обеспечение соблюдения законов и иных нормативных правовых актов.

4.4. Предоставление медицинских услуг.

4.5. Реализация обязательств, принятых ООО «Байкальский Медицинский Легион» по соглашениям и договорам.

5. Условия обработки, передачи и хранения персональных данных

5.1. ООО «Байкальский Медицинский Легион», при осуществлении своей деятельности в части обработки персональных данных руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

5.2. ООО «Байкальский Медицинский Легион» не осуществляет трансграничную передачу персональных данных (передачу персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

5.3. ООО «Байкальский Медицинский Легион» обрабатывает и хранит персональные данные субъектов в соответствии с внутренними нормативными документами, разработанными согласно законодательству РФ.

5.4. ООО «Байкальский Медицинский Легион» обеспечивает конфиденциальность персональных данных в отношении всех субъектов персональных данных. Передача ПДн третьим лицам осуществляется только при выполнении функции предоставления медицинской услуги - в рамках установленной процедуры.

5.5. Оператор может поручить обработку персональных данных другому лицу при выполнении следующих условий:

- получено согласие субъекта на поручение обработки другому лицу;
- обработка персональных данных осуществляется на основании заключаемого с этим лицом договора.

6. Перечень действий с персональными данными

ООО «Байкальский Медицинский Легион» осуществляет обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, уничтожение персональных данных с использованием средств автоматизации, а также без использования таких средств.

ООО «Байкальский Медицинский Легион» может поручить обработку персональных данных третьим лицам в случаях, если:

- субъект дал согласие на осуществление таких действий (при наличии условий в договоре с третьим лицом о соблюдении им принципов и правил обработки персональных данных, предусмотренных Федеральным законом «О персональных данных»);
- для осуществления и выполнения возложенных законодательством Российской Федерации на ООО «Байкальский Медицинский Легион» функций, полномочий и обязанностей;
- в других случаях, предусмотренных законодательством Российской Федерации.

7. Права субъекта

Субъект персональных данных, согласно законодательству Российской Федерации, имеет право:

- получать информацию, касающуюся обработки своих персональных данных;
- требовать уточнения своих 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;
- требовать прекращения обработки своих персональных данных в случаях, предусмотренных законодательством Российской Федерации;
- обжаловать действия или бездействие ООО «Байкальский Медицинский Легион» в судебном порядке;

- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

8. Условия прекращения обработки

Срок или условие прекращения обработки персональных данных в ООО «Байкальский Медицинский Легион»:

- ликвидация или реорганизация ООО «Байкальский Медицинский Легион»;
- прекращение договорных отношений с работниками;
- расторжение договоров об оказании услуг, заключенных с физическими лицами, в связи с окончанием оказания указанных услуг;
- отзыв согласия на обработку своих персональных данных;
- достижение цели обработки персональных данных.

9. ООО «Байкальский Медицинский Легион» принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных граждан - субъектов персональных данных

К мерам, применяемым для защиты персональных данных относятся:

- назначение сотрудника, ответственного за организацию обработки персональных данных;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону «О персональных данных»;
- разработка документов, определяющих политику ООО «Байкальский Медицинский Легион» в отношении обработки персональных данных, локальные документы по вопросам обработки персональных данных;
- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, с требованиями к защите персональных данных, с документами, определяющими политику ООО «Байкальский Медицинский Легион» в отношении обработки персональных данных, локальными документами по вопросам обработки персональных данных;
- опубликование в сети Интернет документа, определяющего политику ООО «Байкальский Медицинский Легион» в отношении обработки персональных данных;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение, прошедшей в установленном порядке, процедуры оценки соответствия средств защиты информации;

- систематическое осуществление оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе;
- осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

10. Методы защиты персональных данных

К методам защиты персональных данных относятся:

- реализация разрешительной системы допуска к обработке персональных данных;
- ограничение доступа в помещения, где размещены технические средства, осуществляющие обработку персональных данных, а также хранятся носители информации,
- разграничение доступа к персональным данным;
- регистрация действий сотрудников, контроль несанкционированного доступа к персональным данным;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, использование защищенных каналов связи,

II ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ

1. Сотрудники ООО «Байкальский Медицинский Легион», являющиеся пользователями информационных систем персональных данных (ИСПДн), должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ГИДн.

2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗГИДн.

4. Сотрудники оператора, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей, логинов и паролей) и не допускать несанкционированный доступ (НСД) к ним, а так же возможность их утери или

использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

5. Сотрудники оператора должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

6. Сотрудники оператора должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам.

9. При работе с ПДн в ИСПДн сотрудники оператора обязаны обеспечить отсутствие возможности просмотра ГДн третьими лицами с мониторов,

10. При завершении работы с ИСПДн сотрудники обязаны защитить монитор с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

11. Сотрудники ООО «Нейропсихотерапевтический Центр» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили политику и процедуры безопасности ПДн.

12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности

13. Ответственность сотрудников ООО «Байкальский Медицинский Легион»:

13.1. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем,

неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 Уголовного Кодекса Российской Федерации).

13.2. Сотрудники оператора несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

13.3. При нарушениях сотрудниками ООО «Нейропсихотерапевтический Центр» правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

1. Изменение Политики

ООО «Байкальский Медицинский Легион» имеет право вносить изменения в настоящую Политику. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее утверждения и размещения в общедоступном месте, если иное не предусмотрено новой редакцией Политики.

2. Обратная связь

Юридический адрес ООО «Байкальский Медицинский Легион»: 664022, Иркутская область, город Иркутск, ул. Байкальская, д. 102.

Место нахождения организации: 664022, Иркутская область, город Иркутск, ул. Байкальская, д. 102.