IDM CLINIC

Российская Федерация
Общество с ограниченной ответственностью
“Информационно диагностическая медицинская клиника”
400087, г.Волгоград, ул.Невская 13А, офис 101

тел.: 8 (8442) 99-90-99
e-mail: info@idmclinic.ru
www.idmclinic.ru
ОГРН: 1183443016558

ПОЛИТИКА
в области обработки
и обеспечения безопасности персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет политику ООО “ИДМК” (далее — Общество) в отношении обработки персональных данных, декларирует систему основных принципов, применяемых в отношении обработки персональных данных в Обществе.

1.2. Настоящая Политика в области обработки и обеспечения безопасности персональных данных (далее – Политика) обязательна для ознакомления и исполнения всеми лицами, допущенными к обработке персональных данных в Обществе, а также лицами, участвующими в организации процессов обработки и обеспечения безопасности персональных данных в Обществе.
1.3. Настоящая Политика составлена в соответствии с положениями законодательства Российской Федерации, в том числе Федерального закона РФ «О персональных данных» № 152-ФЗ от 27 июля 2006 г.
1.4. Обработка сведений, составляющих врачебную тайну, которые включают в себя персональные данные, осуществляется Обществом с соблюдением требований Федерального закона от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и иных нормативных правовых актов в сфере здравоохранения.
1.5. Настоящая Политика подлежит актуализации в случае изменения законодательства РФ о персональных данных.
1.6. Настоящая Политика подлежит размещению на официальном сайте Общества.

1.7. Обработка персональных данных в Обществе основана на следующих принципах: ё

− законности целей и способов обработки персональных данных и добросовестности;
− соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Общества;
− соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

− достоверности персональных данных, их актуальности и достаточности для целей обработки, недопустимости обработки избыточных по отношению к целям сбора персональных данных;
− легитимности организационных и технических мер по обеспечению безопасности персональных данных;
− непрерывности повышения уровня знаний работников Общества в сфере обеспечения безопасности персональных данных при их обработке;
− стремления к постоянному совершенствованию системы защиты персональных данных.

1.8. Действие настоящей Политики распространяется на все операции, совершаемые в Обществе с персональными данными с использованием средств автоматизации или без таковых.

1.9. Локальные акты и другие документы, регламентирующие обработку персональных данных в Обществе, разрабатываются с учетом положений настоящей Политики.

2. ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В ПОЛИТИКЕ

2.1. В настоящем документе используются следующие понятия:

1) **персональные данные** - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

2) **субъект персональных данных** - физическое лицо, которое прямо или косвенно определено, или определяемо с помощью персональных данных;

3) **Общество** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В данной Политике под оператором понимается Общество;

4) **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;

5) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

6) **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

7) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

8) **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

9) **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

10) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

11) **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

12) **врачебная тайна** - сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении;

13) **персональные данные, разрешенные субъектом персональных данных для распространения** - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Законом № 152-ФЗ;

14) **открытые источники персональных данных** - социальные сети и иные Интернет- ресурсы,

в которых непосредственно субъектом персональных данных или третьим лицом размещены персональные данные субъекта;

15) **общедоступные источники персональных данных** – справочники, адресные книги и иные источники персональных данных, в которые с письменного согласия субъекта персональных данных включены его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные.

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Общество определило следующие цели обработки персональных данных:

- исполнение договора на оказание медицинских услуг, стороной которого является пациент;
- медико-профилактические цели (установление медицинского диагноза, оказание медицинских услуг, контроль качества оказания медицинской помощи и др.).
- ведение кадрового и бухгалтерского учета;
- обеспечение соблюдения трудового законодательства РФ;
- обеспечение соблюдения налогового законодательства РФ;
- обеспечение соблюдения пенсионного законодательства РФ;
- обеспечение соблюдения законодательства РФ в сфере здравоохранения;
- подготовка, заключение и исполнение гражданско-правового договора;
- продвижение товаров, работ, услуг на рынке;
- подбор персонала (соискателей) на вакантные должности оператора;
- организация обучения;
- организация и проведение мероприятий.

3.2. В рамках, указанных целей Общество вправе определить и отразить в согласиях на Обработку персональных данных направления обработки для обеспечения информированности Субъекта о том каким образом будут обрабатываться его данные в рамках цели.

3.3. Общество вправе определять иные цели Обработки персональных данных, которые на момент вступления в силу настоящей Политики не были определены, они могут закрепляться в локальных нормативных актах Общества, а также непосредственно в согласиях на обработку персональных данных.

4. КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Общество осуществляет обработку различных категорий персональных данных:

- специальные категории персональных данных;
- персональные данные, разрешённые субъектами для опубликования (распространения);
- иные персональные данные, которые в соответствии с действующим законодательством не отнесены к специальным категориям персональных данных, биометрическим персональным данным, данным, разрешенным субъектом для опубликования (распространения).

4.2. Общество в своей деятельности не осуществляет обработку биометрических персональных данных, за исключением случаев наличия у Общества правовых оснований для соответствующей обработки.

4.3. Обществом может осуществляться трансграничная передача персональных данных с

согласия субъекта персональных данных на такую передачу.
4.4. Персональные данные, разрешённые субъектом для опубликования, обрабатываются на основании согласия Субъекта.
4.5. Общество вправе обрабатывать персональные данные, разрешённые Субъектом для распространения, только в целях, указанных в согласии субъекта на распространение персональных данных либо в случаях получения дополнительного согласия от субъекта.

5. СУБЪЕКТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В Компании осуществляется обработка персональных данных следующих категорий субъектов:
- клиенты (пациенты);
- лица, которым в интересах пациента может быть передана информация о состоянии его здоровья;
- законные представители;
- контрагенты;
- представители контрагентов;
- выгодоприобретатели по договорам;
- соискатели на занятие вакантных должностей;
- работники;
- родственники работников;
- уволенные работники;
- учащиеся, студенты;
- посетители сайта;
- участники мероприятий.

5.2. Цели обработки персональных данных, состав и категории обрабатываемых персональных данных, сроки обработки и хранения для каждой категории субъектов персональных данных определены (изложены) в Приложении №1 к настоящей Политике.

5.3. Субъект персональных данных имеет право:
5.3.1. Свободно, своей волей и в своем интересе предоставлять свои персональные данные и давать согласие на их обработку;
5.3.2. Отозвать свое согласие на обработку персональных данных;
5.3.3. Получать информацию, касающуюся обработки своих персональных данных, в том числе содержащую:
- подтверждение факта обработки персональных данных Обществом;
- правовые основания и цели обработки персональных данных (в том числе, доказательство получения Обществом согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия у Общества иных правовых оснований для обработки персональных данных субъекта);
- цели и применяемые Обществом способы обработки персональных данных; − наименование и место нахождения Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании законодательства Российской Федерации;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения; − информацию об

отсутствии трансграничной передачи данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка поручена или будет поручена такому лицу;
- информацию о способах выполнения оператором обязанностей, установленных статьей 18.1 Федерального закона РФ «О персональных данных» № 152-ФЗ;
- иные сведения, предусмотренные законодательством Российской Федерации. 5.3.4. Требовать от Общества 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;

5.3.5. Требовать прекращения обработки своих персональных данных;
5.3.6. Требовать прекращения обработки своих персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с помощью средств связи.

6. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Персональные данные обрабатываются Обществом на условиях, определенных действующим законодательством.
6.2. В случаях, когда для достижения цели обработки персональных данных требуется получение согласия Субъекта персональных данных, Общество собирает соответствующие согласия до момента начала соответствующей обработки. Согласие может быть получено в любой разрешенной применимым законодательством форме, которая обеспечит возможность сохранения подтверждения получения соответствующего согласия.
6.3. Передача персональных данных субъекта третьему лицу осуществляется только с согласия субъекта персональных данных. В согласии субъекта персональных данных указывается сведения о третьем лице (третьих лицах), которому (которым) передаются персональные данные, а также цель передачи персональных данных.
6.4. Передача персональных данных или поручение обработки персональных данных субъектов третьему лицу осуществляется на основании договора, существенными условиями которого являются соблюдение третьим лицом конфиденциальности и обеспечение безопасности персональных данных в соответствии с требованиями законодательства о персональных данных.
6.5. При передаче персональных данных третьим лицам, которые на основании договоров получают доступ или осуществляют обработку персональных данных, Общество ограничивает эту информацию только теми персональными данными, которые необходимы для выполнения указанными лицами их функций (услуг, работ).
6.6. Общество осуществляет распространение персональных данных медицинских работников, а именно: фамилия, имя, отчество (при наличии), занимаемая должность, сведения об образовании, квалификации, профессиональном опыте, стаж работы, фотография, график работы и часы приема с целью предоставления пользователям сайта информации о медицинской организации и ее работниках на основании и с соблюдением требований Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и иных нормативных правовых актов в сфере здравоохранения, а также на основании согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения (в части сведений, не указанных в соответствующих нормативных правовых актах).
6.7. Обработка персональных данных осуществляется Компанией с использованием средств

автоматизации, а также без использования таких средств (на бумажных носителях информации).
6.8. Персональные данные граждан Российской Федерации обрабатываются с использованием баз данных, находящихся на территории Российской Федерации.
6.9. Обработка персональных данных может осуществляться работниками Общества, а также иными лицами, привлеченными Обществом на основании соответствующего соглашения (поручения).
6.10. Правовыми основаниями обработки персональных данных для достижения целей, указанных в разделе 5 настоящей Политики, являются:
1) Гражданский кодекс российской Федерации;
2) Трудовой кодекс Российской Федерации;
3) Налоговый кодекс Российской Федерации;
4) Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах»; 5) Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
6) Федеральный закон Российской Федерации от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»; 7) Федеральный закон Российской Федерации от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
8) Федеральный закон Российской Федерации от 28.12.2003 №426 «О специальной оценке условий труда»;
9) Постановление Правительства Российской Федерации от 27.11.2006 г. № 719 «Об утверждении Положения о воинском учете»;
10) Устав Общества;
11) Лицензии, полученные Обществом в установленном законодательством порядке;
12) договоры, заключаемые между Обществом и субъектами персональных данных;
13) согласие субъектов персональных данных на обработку их персональных данных;
14) уведомление об автоматическом сборе технических данных пользователей (посетителей) сайта Общества;
15) иные нормативные правовые акты, исполнение требований которых связано с обработкой персональных данных.

7. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Доступ к персональным данным ограничивается в соответствии с законодательством Российской Федерации.
7.2. Персональные данные во всех случаях, кроме персональных данных, разрешенных для опубликования в общедоступных источниках, классифицируются как строго конфиденциальная информация.
7.3. Указанный режим конфиденциальности информации применяется к персональным данным вне зависимости от наличия или отсутствия соответствующей маркировки.
7.4. Доступ к обрабатываемым персональным данным предоставляется только тем работникам Общества, которым он необходим в связи с исполнением ими своих должностных обязанностей.
7.5. Работники Общества, получившие доступ к персональным данным, принимают на себя обязательства по обеспечению конфиденциальности и безопасности обрабатываемых персональных данных.
7.6. Общество не раскрывает третьим лицам и не распространяет персональные данные без согласия на это субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.
7.7. Третьи лица, получившие доступ к персональным данным, или осуществляющие обработку персональных данных по поручению Общества, обязуются соблюдать требования договоров и соглашений с Обществом в части обеспечения конфиденциальности и безопасности

персональных данных.

8. ИСТОЧНИКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Сбор персональных данных Обществом осуществляется:

- от субъекта персональных данных;
- от третьих лиц.

8.2. При получении персональных данных от третьих лиц (в том числе по договорам) должно соблюдаться одно из следующих условий:

- субъект персональных данных должен быть уведомлен о такой передаче, а также о её целях и иных условиях, с правом отказа от передачи его данных. Уведомление осуществляется либо Обществом, либо получателем данных, в зависимости от условий письменного соглашения, на основании которого передаются персональные данные;
- лицо, предоставляющее персональные данные, гарантирует, что сбор, обработка и передача персональных данных соответствуют требованиям применимого законодательства, в частности от субъекта получено соответствующее согласие на передачу его персональных данных Обществу с возможностью последующей обработки, а также освобождает Общество от каких

либо требований и претензий третьих лиц, которые связаны с обработкой переданных персональных данных.

8.3. Общество с согласия субъекта персональных данных вправе создавать данные, которые будут использоваться для идентификации Субъекта в Общества (идентификаторы, корпоративный адрес электронной почты и др.) для целей обеспечения деятельности Субъекта в Общества, а также защиты данных и систем Общества. При этом корпоративные персональные данные, являются собственностью Общества и не должны использоваться для целей, которые не связаны с деятельностью Общества.

9. ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Хранение персональных данных в Общества осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, за исключением случаев, когда срок хранения установлен федеральным законом, договором или требованиями нормативных документов РФ.

9.2. Общество осуществляет хранение персональных данных следующими способами:

- на машинных носителях – данные, полученные в электронной форме или преобразованные в электронную форму;
- на бумажных носителях – данные, полученные в материальной форме или преобразованные в материальную форму.
- хранение на машинных носителях может осуществляться Обществом систематизировано с использованием информационных систем персональных данных, формируемых из различных персональных данных, а также в отдельных базах данных (технических решениях, ПО). − обработка, в том числе архивное хранение персональных данных уволенных работников, осуществляется в соответствии с законодательством Российской Федерации.

10. БЛОКИРОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Общество блокирует обрабатываемые персональные данные при выявлении недостоверности обрабатываемых персональных данных или неправомерных действий в отношении субъекта в следующих случаях:

- по требованию Субъекта персональных данных;
- по требованию уполномоченного органа по защите прав Субъектов персональных данных; − по результатам внутренних контрольных мероприятий.

10.2. Порядок блокирования определяется в зависимости от вида персональных данных, носителя, объема, применяемого ПО, а также иных фактических обстоятельств, лицом, ответственным за обеспечение безопасности персональных данных в Общества.

11. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Общество уничтожает персональные данные в случае:

- достижения целей обработки персональных данных или утраты необходимости в их достижении;
- выявления факта неправомерной обработки персональных данных;
- получения соответствующего запроса от Субъекта, при условии, что данный запрос не противоречит требованиям законодательства РФ;
- отзыва согласия Субъекта на обработку его персональных данных (если отзыв согласия влечет за собой уничтожение персональных данных);
- получения соответствующего предписания от уполномоченного органа по защите прав субъектов.

11.2. Способы уничтожения персональных данных определяются внутренними нормативными документами Общества по вопросам обработки и защиты персональных данных в зависимости от способов обработки персональных данных и материальных носителей персональных данных, на которых осуществляется запись и хранение персональных данных.

12. ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Компания вправе производить обезличивание персональных данных Субъектов в целях их защиты.

12.2. Результатом обезличивания персональных данных могут стать:

- обезличенные данные, по которым невозможно определить их принадлежность конкретному субъекту персональных данных без использования дополнительной информации, при этом у Организации есть доступ к такой дополнительной информации;
- обезличенные данные, по которым невозможно определить их принадлежность конкретному субъекту в связи с уничтожением информации, которая могла бы быть использована для определения такой принадлежности.

12.3. На обезличенные данные распространяется режим персональных данных, предусмотренный действующим законодательством и Политикой, при одновременном соблюдении следующих условий:

2.3.2. В отношении Обезличенных данных фактически возможно применить требования режима персональных данных.

13. МЕРЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕАЛИЗУЕМЫЕ В ОБЩЕСТВЕ

13.1. Обеспечение безопасности персональных данных при их обработке Обществом осуществляется в соответствии с законодательством Российской Федерации и требованиями уполномоченного органа государственной власти по защите прав субъектов персональных данных, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.
13.2. Общество предпринимает необходимые организационные и технические меры для защиты персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

13.3. Меры защиты, реализуемые Обществом при обработке персональных данных, включают (но не ограничиваются):

- назначение ответственного за организацию обработки персональных данных; − назначение работника, ответственного за обеспечение безопасности персональных данных в информационных системах Общества;
- принятие локальных нормативно-правовых актов по вопросам обработки персональных данных;
- осуществление внутреннего контроля и аудита соответствия обработки персональных данных требованиям законодательства, защиты персональных данных и политике ООО «ИДМК», а также локальным нормативно-правовым актам оператора;
- работники, непосредственно осуществляющие обработку персональных данных, ознакомлены с требованиями защиты персональных данных, документами, определяющими политику ООО «ИДМК» в отношении обработки персональных данных, локальными нормативно актами по вопросам обработки персональных данных;
- использование защищенных каналов связи;
- обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также с применением технических средств (используются антивирусные средства защиты информации, межсетевое экранирование, и иные технические средства защиты информации);
- осуществление идентификации и проверки подлинности пользователя при входе в информационные системы по паролям;
- разработка правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
- работники, непосредственно осуществляющие обработку персональных данных ознакомлены с положениями и требованиями законодательства Российской Федерации о персональных данных, с документами по вопросам обработки персональных данных (политика, положение, регламент, инструкции), проведено обучение указанной категории работников
- определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных
- установлены правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечены регистрация и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных − обеспечено наличие средств резервного копирования и восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

13.4. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Общество обязано с момента выявления такого инцидента Обществом, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:
1) в течение 24 (двадцати четырех) часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном на взаимодействие Обществом с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение 72 (семидесяти двух) часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

13.5. Контроль исполнения требований настоящей Политики осуществляется лицом, ответственным за организацию обработки ПДн.