



УТВЕРЖДАЮ

Генеральный директор
ООО «ЭЙЧ-КЛИНИК»

А.А. Злобин

20 18 г.

Политика в области обработки и защиты персональных данных ООО «ЭЙЧ-КЛИНИК»

1. Общие положения

1.1. Настоящий документ определяет политику ООО «ЭЙЧ-КЛИНИК» (далее – Клиника) в области обработки и обеспечения безопасности персональных данных (далее – Политика).

1.2. Настоящая Политика разработана в целях реализации требований законодательства в области обработки и обеспечения безопасности персональных данных и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в Клинике.

1.3. Положения настоящей Политики являются основой для организации всех процессов в Клинике, связанных с обработкой и защитой персональных данных и обязательны для исполнения всеми сотрудниками Клиники.

1.4. Настоящая Политика разработана в соответствии с федеральным законодательством Российской Федерации:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ,
- Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»;
- Федеральный закон от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности»;
- Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
- Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (утв. Постановлением Правительства Российской Федерации от 16.03.2009 № 228);
- Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. Постановлением Правительства Российской Федерации от 01.11.2012 № 1119);

- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. Постановлением Правительства Российской Федерации от 15.09.2008 № 687);
- Административный регламент Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных» (утв. приказом Министерства связи и массовых коммуникаций Российской Федерации от 21.12.2011 № 346);
- Административный регламент исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (утв. приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312);
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21);
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (утв. приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378),

а также в соответствии с иными действующими федеральными законами и подзаконными актами Российской Федерации, определяющими правила и особенности обработки персональных данных и обеспечения безопасности и конфиденциальности такой обработки.

1.5. Настоящая Политика устанавливает:

- цели обработки персональных данных;
- общие принципы и правила обработки персональных данных;
- классификацию персональных данных и субъектов персональных данных;
- права и обязанности субъектов персональных данных и Клиники по их обработке;
- порядок организации обработки персональных данных.

1.6. Настоящая Политика в соответствии с требованиями п. 2 ст. 18.1 Федерального закона «О персональных данных» подлежит опубликованию на официальном сайте www.h-clinic.ru, на бумажном носителе хранится по адресу: 127083, г. Москва, ул. 8 марта, д. 6А, стр. 1

1.7. Настоящая Политика вступает в силу с момента ее утверждения, подлежит пересмотру в связи с изменением законодательства Российской Федерации в области обработки и защиты персональных данных, по результатам оценки актуальности, достаточности и эффективности принимаемых мер обеспечения безопасности обработки персональных данных в Клинике.

1.8. Действие настоящей Политики распространяется на действия (операции) 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, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2. Основные термины и определения

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

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

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных - обязательное для соблюдения Клиникой или иным получившим доступ к персональным данным лицом требование не допускать их раскрытие и распространение без согласия субъекта персональных данных или наличия иного законного основания.

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.

Общедоступные персональные данные - персональные данные, 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.

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

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

Специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Субъект персональных данных - физическое лицо, которое прямо или косвенно определено или определяемо с помощью данных.

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

3. Цели обработки персональных данных

3.1. Клиника осуществляет обработку персональных данных в целях:

- оказания медицинских услуг в соответствии с Федеральным законом Федеральным Законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», действующим законодательством Российской Федерации и выданными Клинике лицензиями;
- осуществления дистанционного взаимодействия с пациентами и иными заинтересованными лицами в рамках сервисно-информационного обслуживания путем использования телефонной связи, электронной почты, посредством сайта Клиники в сети «Интернет»;
- организации и проведения мероприятий, направленных на повышение узнаваемости и лояльности в отношении Клиники, а также продвижение услуг Клиники;
- заключения с субъектом персональных данных любых договоров и соглашений и их дальнейшего исполнения;
- предоставления субъекту персональных данных информации об оказываемых услугах, новых продуктах и услугах, об услугах партнеров Клиники; информирования о расписании работы Клиники, изменениях расписания;
- ведения договорной работы, не связанной с основной деятельностью Клиники, в рамках возникновения, изменения и прекращения правоотношений между Клиникой и третьими лицами, а также оформление доверенностей на представление интересов Клиники;
- участия Клиники в гражданском, арбитражном, уголовном, административном процессах и исполнения судебных актов;
- формирования статистической отчетности, в том числе для предоставления контролирующим органам государственной власти Российской Федерации;
- замещения вакантных должностей в Клинике соискателями;
- соблюдения Клиникой требований трудового законодательства, законодательства по учету труда и его оплаты;
- сохранения жизни и здоровья сотрудников Клиники в процессе трудовой деятельности и выявления нарушений состояния здоровья и медицинских противопоказаний к работе у сотрудников Клиники (включая освидетельствование на наличие медицинских противопоказаний к занимаемой должности), а также выполнение требований действующего законодательства по расследованию и учету несчастных случаев, происшедших с сотрудниками Клиники;
- реализации Клиникой как работодателя обязанностей, предусмотренных Трудовым кодексом Российской Федерации, по выплате сотрудникам причитающейся заработной платы,

- компенсаций и премий, по осуществлению пенсионных и налоговых отчислений, а также расчет с контрагентами и пациентами;
- организации обучения, повышения квалификации и проверки знаний для сотрудников Клиники, осуществления оценки деловых, личностных качеств сотрудников и результатов их труда, а также осуществление оценки удовлетворенности сотрудников своим трудом;
 - оформления командировочных документов для сотрудников Клиники, а также бронирования и приобретения гостиничных мест и транспортных билетов в интересах сотрудников, направляемых в командировки;
 - облегчения коммуникаций между сотрудниками Клиники посредством ведения справочника контактных данных сотрудников;
 - обеспечения личной безопасности сотрудников Клиники, иных лиц, посещающих объекты недвижимости (помещения, здания, территорию) Клиники, а также обеспечение сохранности материальных и иных ценностей, находящихся в ведении Клиники;
 - выделения/подключения вычислительных средств, создание новых пользователей в информационных системах Клиники, предоставления доступа к ресурсам информационных систем Клиники, а также решения проблем, возникающих у пользователей в процессе работы с компьютерами (аппаратным и программным обеспечением) и оргтехникой;
 - учёта информации об использовании услуг корпоративной стационарной и мобильной связи сотрудниками Клиники;
 - проведения независимой проверки бухгалтерской (финансовой) отчетности Клиники;
 - организации и осуществления в Клинике внутреннего контроля качества и безопасности медицинской помощи и внутренних производственных процессов.

4. Классификация персональных данных и категории субъектов

4.1. К персональным данным относится любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), обрабатываемая Клиникой для достижения указанных целей.

4.2. Клиника не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, судимости физических лиц, если иное не установлено законодательством Российской Федерации.

4.3. Клиника осуществляет обработку персональных данных следующих категорий субъектов персональных данных:

- действительные пациенты Клиники;
- потенциальные пациенты Клиники;
- члены семей и иные родственники действительных и потенциальных пациентов Клиники;
- представители (в силу закона и по доверенности) действительных и потенциальных пациентов Клиники;
- сотрудники и представители сторонних медицинских организаций;
- сотрудники и представители действующих контрагентов Клиники (юридических лиц), включая страховые и ассистансные компании;
- лица, являющиеся соискателями на замещение вакантных должностей Клиники;
- действующие и потенциальные контрагенты Клиники (физические лица);

- сотрудники и представители действующих и потенциальных контрагентов Клиники (юридических лиц);
- посетители частных и публичных мероприятий, организованных Клиники;
- сотрудники (представители, контактные лица) Клиники;
- члены семей сотрудников Клиники;
- получатели алиментов от сотрудников Клиники;
- сотрудники юридических лиц и физические лица, представляющие интересы Клиники;
- лица, участвующие в гражданском, арбитражном, уголовном, административном процессах и исполнительном производстве (участником которых является Клиника);
- посетители помещений, зданий и территории Клиники.

5. Основные принципы обработки персональных данных

5.1. Обработка персональных данных в Клинике осуществляется на основе следующих принципов:

- законности целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
- соответствия состава и объема обрабатываемых персональных, а также способов обработки персональных данных заявленным целям обработки;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости обработки персональных данных, несовместимых с целями сбора персональных данных;
- недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместных между собой;
- обеспечения хранения персональных данных не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является субъект персональных данных;
- уничтожения или обезличивания персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации, договором, стороной которого является субъект персональных данных;
- обеспечения конфиденциальности и безопасности обрабатываемых персональных данных.

6. Организация обработки персональных данных

6.1. Обработка персональных данных осуществляется с соблюдением принципов и правил, установленных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

6.2. Обработка персональных данных в Клинике включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

В Клинике осуществляется обработка персональных данных с использованием средств автоматизации и без использования средств автоматизации.

6.3. Клиника может включать персональные данные субъектов в общедоступные источники персональных данных, при этом Клиника берет письменное согласие субъекта на обработку его персональных данных.

6.4. В Клинике осуществляется обработка биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, в т.ч. фото) с письменного согласия субъектов персональных данных (сотрудников и пациентов).

В Клинике осуществляется обработка специальных категорий персональных данных о состоянии здоровья в соответствии с требованиями законодательства, а также с письменного согласия субъектов персональных данных (сотрудников и пациентов).

6.5. Клиника не осуществляет трансграничную передачу персональных данных.

6.6. В Клинике не принимаются решения, порождающие юридические последствия в отношении субъектов персональных данных или иным образом затрагивающие их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

6.7. Клиника 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 (далее – поручение оператора). При этом Клиника в договоре обязывает лицо, осуществляющее обработку персональных данных по поручению Клиники, соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом.

6.8. Предоставление доступа органам государственной власти (в том числе, контролирующим, надзорным, правоохранительным и иным органам) к персональным данным, обрабатываемым Клиникой осуществляется в объеме и порядке, установленном соответствующим законодательством Российской Федерации.

7. Права субъекта персональных данных

7.1. Субъект персональных данных имеет право:

- получать информацию, касающуюся обработки его персональных данных, в порядке, форме и сроки, установленные законодательством о персональных данных;
- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными, не являются необходимыми для заявленной цели обработки или используются в целях, не заявленных ранее при предоставлении субъектом персональных данных согласия на обработку персональных данных;
- принимать предусмотренные законом меры по защите своих прав;
- отозвать свое согласие на обработку персональных данных.

7.2. Субъект персональных данных обязан предоставить полные, точные и достоверные сведения о своих персональных данных.

7.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

7.3.1. Для реализации и защиты своих прав и законных интересов субъект персональных данных имеет право обратиться в Клинику.

Клиника (оператор) рассматривает обращения и запросы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций.

7.3.2. Субъект персональных данных вправе обжаловать действия или бездействие Клиники путем обращения в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

8. Права и обязанности Клиники при обработке персональных данных

8.1. Клиника имеет право:

- обрабатывать персональные данные субъекта персональных данных в соответствии с заявленной целью;
- требовать от субъекта персональных данных предоставления достоверных персональных данных, необходимых для исполнения договора, оказания услуги, идентификации субъекта персональных данных, а также в иных случаях, предусмотренных законодательством о персональных данных;
- ограничить доступ субъекта персональных данных к его персональным данным в случае, если таковой нарушает права и законные интересы третьих лиц, а также в иных случаях, предусмотренных законодательством Российской Федерации;
- обрабатывать общедоступные персональные данные физических лиц;
- осуществлять обработку персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации;
- уточнять обрабатываемые персональные данные, блокировать или удалять, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- вести учет обращений субъектов персональных данных;
- поручить обработку персональных данных другому лицу с согласия субъекта персональных данных.

8.2. В соответствии с требованиями Федерального закона «О персональных данных» Клиника обязана:

- предоставлять субъекту персональных данных по его запросу информацию, касающуюся обработки его персональных данных, либо на законных основаниях предоставить отказ;
- по требованию субъекта персональных данных уточнять обрабатываемые персональные данные, блокировать или удалять, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- вести учет обращений субъектов персональных данных;
- уведомлять субъекта персональных данных об обработке персональных данных в том случае, если персональные данные были получены не от субъекта персональных данных за исключением предусмотренных законом Российской Федерации случаев;
- в случае достижения цели обработки персональных данных незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между Клиникой и субъектом персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекратить обработку персональных данных и уничтожить персональные данные в срок, установленный законодательством Российской Федерации, об уничтожении персональных данных Клиника обязано уведомить субъекта персональных данных;
- Клиника обязуется и обязывает иные лица, получившие доступ к персональным данным, не раскрывать их третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;
- назначить лицо (лиц), ответственных за организацию обработки персональных данных.

9. Меры по обеспечению безопасности персональных данных при их обработке

9.1. При обработке персональных данных Клиника принимает необходимые правовые, организационные и технические меры 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.

9.2. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

- назначением ответственного лица за организацию обработки персональных данных, права и обязанности которого определяются локальными актами Клиники;
- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- обучением персонала Клиники, участвующего в обработке персональных данных, вопросам обеспечения безопасности персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

9.3. Обязанности сотрудников Клиники, непосредственно осуществляющих обработку персональных данных, а также их ответственность определяются в локальных актах Клиники.

10. Ответственность Клиники

10.1. Контроль за выполнением требований настоящей Политики, правил и требований, применяемых при обработке персональных данных в Клинике осуществляют лица, назначенные приказом генерального директора Клиники.

10.2. Клиника, а также его должностные лица и сотрудники несут уголовную, гражданско-правовую, административную и дисциплинарную ответственность за несоблюдение принципов и условий обработки персональных данных, а также за разглашение или незаконное использование персональных данных в соответствии с законодательством Российской Федерации.

Контакты для обращения субъектов по вопросам обработки персональных данных:

127083, г. Москва, ул. 8 марта, д.6А, стр. 1

E-mail: info@h-clinic.ru