

Утверждено
Приказом № 041(10) от «08» июля 2020 г.

ПОЛИТИКА
обработки и защиты персональных данных в
Обществе с ограниченной ответственностью «ЕС-клиника»

Москва 2020

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Общество — Общество с ограниченной ответственностью «ЕС-клиника», ООО «ЕС-клиника».

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

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.

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

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

Носитель персональных данных — физическое лицо или материальный объект, в том числе физическое поле, в котором персональные данные находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Ответственный за организацию обработки персональных данных — лицо, осуществляющее внутренний контроль за соблюдением Обществом и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных.

Ответственный за обеспечение безопасности персональных данных — лицо, ответственное за обеспечение безопасности персональных данных, за реализацию и непрерывность соблюдения установленных мер защиты и осуществляющих поддержку функционирования средств защиты информации, применяемых в информационной системе персональных данных Общества.

Пользователь — работник Общества, которому разрешено выполнять некоторые действия (операции) по обработке персональных данных в информационной системе персональных данных или использующее результаты ее функционирования.

Безопасность персональных данных — состояние защищенности персональных данных, при котором обеспечены их конфиденциальность, доступность и целостность.

Конфиденциальность персональных данных — обязательное для выполнения лицом, получившим доступ к персональным данным, требование не передавать такие персональные данные третьим лицам без согласия ее обладателя.

Доступность персональных данных — состояние персональных данных, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Целостность персональных данных — состояние персональных данных, при котором их изменение осуществляется только преднамеренно субъектами, имеющими на него право.

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

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

Несанкционированный доступ (несанкционированные действия) — доступ к персональным данным или действия с персональными данными, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Политика обработки и защиты персональных данных в Обществе с ограниченной ответственностью «ЕС-клиника» (далее — Политика) разработана в соответствии с п.2 ч.1 ст.18.1 Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных» и определяет основные принципы, цели и условия обработки персональных данных (далее — ПДн), а также стратегию их защиты в Обществе с ограниченной ответственностью «ЕС-клиника» (далее — Общество).

Настоящая Политика является основным руководящим внутренним документом Общества, определяющим требования, предъявляемые в отношении обработки и обеспечения безопасности ПДн.

Внутренние документы Общества, регламентирующие вопросы, рассматриваемые в настоящей Политике, должны разрабатываться с учетом положений настоящей Политики и не противоречить им.

Настоящая Политика разработана в целях реализации положений законодательства Российской Федерации в отношении обработки ПДн, а также требований нормативных и методических документов по защите ПДн.

В отношении медицинской клиники ООО «ЕС-клиника» могут утверждаться отдельные регламенты и положения, уточняющие и/или дополняющие положения настоящего документа.

3. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЩЕСТВА

Обработка ПДн Обществом осуществляется на основе принципов:

- законности и справедливости целей и способов обработки ПДн;
- соответствия целей обработки ПДн законным целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Общества;
- соответствия объема и содержания обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- точности ПДн, их достаточности и актуальности по отношению к целям обработки ПДн;
- 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 в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, или устанавливаемый срок хранения федеральный закон, договор, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн;
- уничтожения ПДн по достижении целей их обработки, в случае утраты необходимости в достижении целей обработки или по окончании срока хранения ПДн, установленного федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.

Обработка ПДн Общества осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн.

Общество в своей деятельности исходит из того, что субъект ПДн предоставляет точную и достоверную информацию во время взаимодействия с Обществом, извещает представителей Общества об изменении своих ПДн.

4. ЦЕЛИ И ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общество осуществляет сбор и дальнейшую обработку персональных данных в следующих целях:

- принятие решения о трудоустройстве;
- обеспечение соблюдения законов и иных нормативных правовых актов, содействие работникам в трудоустройстве, получении образования и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы и обеспечения сохранности имущества;
- принятие решения о заключении договоров оказания услуг, заключение договоров оказания услуг, исполнение обязательств по договорам оказания услуг перед физическими или юридическими лицами (а также индивидуальными предпринимателями и партнерами Общества);
- обеспечение исполнения обязательств по договорам (но не ограничиваясь) с физическими или юридическими лицами (в том числе с индивидуальными предпринимателями), не являющимися клиентами Общества;
- улучшение качества обслуживания, проведение маркетинговых программ и продвижение услуг на рынке.

Правовыми основаниями для обработки ПДн субъектов ПДн Обществом являются:

- Федеральный закон Российской Федерации от 30 ноября 1994 г. № 51-ФЗ «Гражданский кодекс Российской Федерации (часть первая)»;
- Федеральный закон Российской Федерации от 26 января 1996 г. № 14-ФЗ «Гражданский кодекс Российской Федерации (часть вторая)»;

- Федеральный закон Российской Федерации от 31 июля 1998 года № 146-ФЗ «Налоговый кодекс Российской Федерации»;
- Федеральный закон Российской Федерации от 30 декабря 2001 г. № 197-ФЗ «Трудовой кодекс Российской Федерации»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»);
- Федеральный закон от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее — № 1119-ПП);
- Устав Общества;
- Иные нормативные правовые акты.

Общество обрабатывает ПДн, ставшие известными Обществу в связи с реализацией уставных задач и целей деятельности Общества, а также в результате, но не ограничиваясь:

- заключения гражданско-правовых договоров;
- заключения соглашений о сотрудничестве;
- оформления и/или получения доверенностей (в том числе от имени Общества);
- получения любых иных документов от клиентов, контрагентов Общества, необходимых для заключения Обществом договоров с такими лицами;
- поступления в Общество письменных, в том числе электронных обращений, запросов, заявлений, жалоб, ходатайств;
- переписки по электронной почте;
- осуществления иных действий, предусмотренных действующим законодательством Российской Федерации или внутренними политиками Общества.

5. ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Общество обрабатывает ПДн следующих категорий субъектов ПДн:

- соискатель вакансии Общества;
- работник Общества;
- контрагент Общества;
- клиент Общества
- законный представитель клиента.

Общество осуществляет обработку персональных данных с использованием средств автоматизации и без использования средств автоматизации.

В соответствии с положениями № 1119-ПП в Обществе обрабатываются следующие категории ПДн:

- иные категории персональных данных — персональные данные, не отнесенные к категориям: специальные, биометрические и общедоступные персональные данные;
- специальные категории персональных данных — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

В Обществе обрабатываются следующие категории ПДн без использования средств автоматизации:

- иные категории персональных данных — персональные данные, не отнесенные к категориям: специальные, биометрические и общедоступные персональные данные;
- специальные категории персональных данных — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Общество обрабатывает cookie-данные для статистического анализа использования сервисов и обеспечения их работоспособности, как в целом, так и их отдельных функций.

Полный перечень ПДн и категории субъектов ПДн утверждается «Перечнем обрабатываемых персональных данных».

6. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка ПДн Общества допускается в следующих случаях:

- обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;
- обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации;
- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн;
- обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн;
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Общество вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этой стороной договора (поручения на обработку ПДн). Лицо, осуществляющее обработку ПДн по поручению Общества, обязано соблюдать принципы и правила обработки ПДн, предусмотренные ФЗ «О персональных данных».

В поручении третьему лицу указываются цели обработки и перечень действий (операций) с ПДн, которые могут быть совершены данным лицом, устанавливаются его обязанности по обеспечению конфиденциальности и безопасности ПДн при их обработке, а также требования к защите обрабатываемых ПДн в соответствии с ФЗ «О персональных данных».

Общество осуществляет трансграничную (на территорию иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу ПДн.

Обществом не создаются общедоступные источники ПДн (справочники, адресные книги).

Обществом 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.

Общество прекращает обработку ПДн в следующих случаях:

- при выявлении неправомерных действий с ПДн в срок, не превышающий трех рабочих дней с даты такого выявления, Общество устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений Общество в срок, не превышающий десяти рабочих дней с даты выявления неправомерности действий с ПДн, уничтожает ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Общество уведомляет субъекта ПДн или его законного представителя, а в случае, если обращение или запрос были направлены в уполномоченный орган по защите прав субъектов ПДн, также этот орган;
- при достижении цели обработки ПДн Общество незамедлительно прекращает обработку ПДн и уничтожает соответствующие ПДн в срок, не превышающий тридцати рабочих дней с даты достижения цели обработки ПДн;
- при отзыве субъектом ПДн согласия на обработку своих ПДн Общество прекращает обработку ПДн и уничтожает (за исключением ПДн, которые хранятся в соответствии с действующим законодательством) ПДн в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва. Об уничтожении ПДн Общество уведомляет субъекта ПДн.

7. СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Получение и обработка ПДн в случаях, предусмотренных ФЗ «О персональных данных», осуществляется Обществом с согласия субъекта ПДн, в том числе в письменной форме.

Письменное согласие субъекта ПДн должно включать:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Общества;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Общества, если обработка будет поручена такому лицу;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Обществом способов обработки ПДн;
- срок, в течение которого действует согласие, а также способ его отзыва;
- подпись субъекта ПДн.

Субъект ПДн дает Обществу согласие на обработку своих ПДн свободно, в своей воле и своем интересе. Согласие на обработку ПДн может быть отозвано субъектом ПДн путем направления в Общество письменного заявления в свободной форме. В этом случае Общество обязуется прекратить обработку, а также уничтожить все имеющиеся в Обществе ПДн в сроки, установленные ФЗ «О персональных данных».

Общество вправе обрабатывать ПДн без согласия субъекта ПДн (или при отзыве субъектом ПДн указанного согласия) при наличии оснований, указанных в пп. 2-11 ч. 1 ст. 6, ч. 2. ст. 10 и ч. 2 ст. 11 ФЗ «О персональных данных».

Передача ПДн третьим лицам осуществляется Обществом с согласия субъекта ПДн в соответствии с требованиями действующего законодательства.

8. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для обеспечения соблюдения установленных законодательством прав субъектов ПДн, в Обществе разработан и введен порядок работы с обращениями и запросами субъектов ПДн, а также порядок предоставления субъектам ПДн информации, установленной законодательством РФ в области ПДн.

Субъект ПДн имеет право на получение информации, касающейся обработки Обществом его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Обществом;
- правовые основания и цели обработки ПДн;
- цели и применяемые Обществом способы обработки ПДн;
- наименование и местонахождение Общества, сведения о лицах (за исключением работников Общества), 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 ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Общества, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами.

Общество предоставляет указанную информацию на основании соответствующего письменного запроса субъекта ПДн, содержащего: номер удостоверяющего личность документа, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения) и подпись субъекта ПДн.

Общество обязуется сообщить субъекту ПДн информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн в течение тридцати дней с даты получения Запроса субъекта ПДн.

Субъект ПДн вправе требовать от Общества уточнения его 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.

Для реализации и защиты своих прав и законных интересов субъект ПДн имеет право обратиться к Оператору. Оператор 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.

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.

Если субъект ПДн считает, что Общество осуществляет обработку его ПДн с нарушением требований ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Общества в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

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

9. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для обеспечения безопасности ПДн Общество принимает необходимые и достаточные организационные и технические меры для защиты ПДн субъектов ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий, включающие в том числе:

- назначение лица, ответственного за организацию обработки ПДн и лица, ответственного за обеспечение безопасности ПДн, а также определение их функций и полномочий;
- разработка и поддержание актуальности комплекта внутренних нормативных документов в отношении обработки и защиты ПДн;
- периодический внутренний контроль, а также внешний аудит соответствия обработки ПДн требованиям ФЗ «О персональных данных» и принятым в соответствии с ним нормативно-правовым актам;
- проведение оценки вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ «О персональных данных», а также соотношение указанного вреда с принимаемыми мерами по безопасности ПДн;
- ознакомление работников Общества, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации и внутренних нормативных документов Общества в отношении обработки и защиты ПДн, периодическое обучение вопросам обработки и защиты ПДн;
- определение угроз безопасности ПДн при их обработке в ИСПДн;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- учет работников, допущенных к обработке ПДн;
- учет материальных носителей ПДн;
- обнаружение фактов несанкционированного доступа к ПДн и принятием мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

Комплекс мероприятий и технических средств по обеспечению безопасности ПДн в Обществе формулируется с учетом результатов оценки возможного вреда субъекту ПДн, который может быть нанесен в случае нарушения безопасности его ПДн, актуальности угроз безопасности ПДн, а также установления уровня защищенности ПДн.

10. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ЗАКОНОДАТЕЛЬСТВА РФ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Контроль за соблюдением локальных нормативных актов Общества в области ПДн осуществляется с целью проверки соответствия процессов обработки и защиты ПДн требованиям законодательства РФ в области ПДн, а также выявления возможных каналов утечки и несанкционированного доступа к ПДн.

Внутренний контроль за соблюдением структурными подразделениями Общества требований законодательства РФ и локальных нормативных актов Общества в области ПДн осуществляется лицами, ответственными за обработку и защиту ПДн в Обществе.

Работники Общества, виновные в нарушении норм, регулирующих обработку и защиту ПДн, установленных в Обществе, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой, административной или уголовной ответственности в соответствии с законодательством РФ.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящая Политика является общедоступной и подлежит размещению на официальном сайте Общества.

Внесение изменений в настоящую Политику может вызвано изменениями в законодательстве Российской Федерации, внутренних документах Общества, информационных системах ПДн, системе защиты ПДн.

Все изменения и дополнения, внесенные в настоящую Политику, утверждаются генеральным директором Общества.

Все работники Общества подлежат обязательному ознакомлению с настоящей Политикой и несут предусмотренную законодательством Российской Федерации ответственность за нарушение её положений.

Генеральный директор ООО «ЕС-клиника»

Е.Н. Семёнова