УТВЕРЖДЕНО:
Главный врач ООО «АЛЬТЕР-Д»
Бугаева О.Е.
/_____/

ПОЛИТИКА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

ООО «Альтер-Д»

СОДЕРЖАНИЕ:

ОБЩИЕ ПОЛОЖЕНИЯ

В процессе осуществления своей деятельности Организация обрабатывает персональные данные. Важнейшими задачами при осуществлении обработки персональных данных (далее – ПДн) Организация считает соблюдение принципов законности, справедливости и конфиденциальности. Руководство Организации несет ответственность за соблюдение конфиденциальности и безопасности обрабатываемых персональных данных.

Настоящая Политика по защите персональных данных в Организации (далее – Политика) обеспечивает реализацию требований законодательства Российской Федерации в области обработки персональных данных. В Политике раскрываются основные категории персональных данных, цели, способы и принципы обработки персональных данных, права и обязанности при обработке персональных данных, права субъектов персональных данных, а также меры, применяемые в целях обеспечения безопасности персональных данных при их обработке.

Настоящая Политика распространяется на все случаи обработки персональных данных в Организации, вне зависимости от того, является обработка персональных данных автоматизированной или неавтоматизированной, производится она вручную либо автоматически.

Настоящая Политика является внутренним локальным нормативным актом и является обязательной для исполнения всеми сотрудниками Организации.

Каждый сотрудник, вновь принимаемый на работу в Организацию, во время первого вводного инструктажа должен быть ознакомлен с настоящей Политикой.

Настоящая Политика утверждается Руководителем Организации, который осуществляет контроль соблюдения Политики в Организации.

Политика может быть пересмотрена по решению руководителя Организации.

Политика подлежит обязательному пересмотру при изменении законодательства Российской Федерации в области защиты персональных данных.

Ответственность за актуализацию настоящей Политики и текущий контроль над выполнением норм Политики возлагается на назначаемого приказом Руководителя уполномоченного сотрудника, ответственного за организацию обработки и защиты ПДн.

Организация на основании требований настоящей Политики разрабатывает все внутренние локальные акты и иные документы, связанные с обработкой ПДн.

Настоящая Политика является общедоступным документом. Для обеспечения неограниченного доступа к документу, текст настоящей Политики размещен в уголке потребителя общедоступном неопределенному кругу лиц, а так же на сайте Организации.

ОСНОВНЫЕ ПОНЯТИЯ

«Политика по защите персональных данных в Организации – внутренний локальный нормативный акт, утвержденный Руководителем Организации.

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

Обработка персональных данных - любое действие с персональными данными, совершаемое с использованием средств автоматизации или без использования таких средств.

Субъект персональных данных - идентифицированное или не идентифицированное физическое лицо, в отношении которого проводится обработка персональных данных.

Сотрудник - физическое лицо (субъект персональных данных), заключившее с Организацией трудовой договор.

Соискатель - физическое лицо (субъект персональных данных), представившее в Организацию свои персональные данные с предложением заключения трудового договора.

Партнер – юридическое лицо или индивидуальный предприниматель, оператор персональных данных, с которым у Организации имеются договорные отношения, во исполнение обязательств по которым Партнер поручает Организации в качестве третьего лица обработку ПДн Пациентов или же по которым Организация поручает Партнеру в качестве третьего лица обработку ПДн Пациентов.

Пациент - физическое лицо - заказчик услуг (субъект персональных данных), заключивший с Организацией или Партнером договор на оказание услуг, согласно договору.

Иное физическое лицо – физическое лицо (субъект персональных данных), заключившее с Организацией договор на оказание определенного вида услуг или работ, либо сотрудник Партнера.

Посетитель – физическое лицо (субъект персональных данных), не являющееся Сотрудником и получившее на законных основаниях допуск в помещения Организации.

Уполномоченный сотрудник – Сотрудник, назначенный приказом Руководителя ответственным за обеспечение информационной безопасности и защиту персональных данных.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

ОСНОВНЫЕ ПОЛОЖЕНИЯ

1. Цели обработки ПДн

Организация проводит обработку персональных данных исключительно в целях:

а) осуществления уставной деятельности в соответствии с законодательством РФ;

б) организации учета Сотрудников в соответствии с требованиями законов и иных нормативно-правовых актов, содействия им в карьерном росте и трудоустройстве, в обучении, для осуществления медицинского страхования и для предоставления им иных льгот и компенсаций;

в) принятия решения о заключении с Соискателем трудового договора;

г) исполнения обязательств и осуществление прав по заключенным с Пациентами договорам оказания услуг в соответствии с нормами законодательства.

д) исполнения обязательств и осуществление прав по заключенным с иными физическими лицами или юридическими лицами договорам в соответствии с нормами Гражданского кодекса Российской Федерации;

е) для исполнения обязательств и осуществления прав в процессе судопроизводства по искам к Организации Сотрудников, Пациентов или Партнеров, или исков к Сотрудникам, Пациентам или Партнерам в рамках Гражданского процессуального кодекса Российской Федерации, Арбитражного процессуального кодекса Российской Федерации, Кодекса Российской Федерации об административных правонарушениях;

ж) обработки персональных данных, доступ неограниченного круга лиц к которым предоставлен Сотрудником или Пациентом либо по их просьбе;

з) выполнения маркетинговых и рекламных действий в целях установления и дальнейшего развития отношений с Пациентами и Партнерами;

и) осуществления пропускного и внутриобъектового режима в помещениях Организации.

В Организации обработке подлежат только те персональные данные, которые отвечают указанным выше целям их обработки. Персональные данные не подлежат обработке в случае несоответствия их характера и объема поставленным целям.

Организация не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

В том случае если для достижения указанных выше целей обработки персональных данных, Организации необходимо осуществить обработку биометрических персональных данных, либо касающихся состояния здоровья, то такая обработка осуществляется только на основании согласия субъекта персональных данных.

2. Допуск Сотрудников к обработке ПДн

Персональные данные в Организации могут обрабатываться только уполномоченными в установленном порядке Сотрудниками.

Сотрудники допускаются в Организации к обработке персональных данных только на основании приказа Руководителя.

Сотрудники, допущенные к обработке персональных данных, имеют право приступать к работе с персональными данными только после ознакомления под личную подпись с локальными нормативными актами, регламентирующими в Организации обработку ПДн.

Сотрудники, осуществляющие обработку персональных данных, должны действовать в соответствии с должностными инструкциями, регламентами и другими распорядительными документами Организации, и соблюдать требования по соблюдению режима конфиденциальности.

3. Получение ПДн, их категории, сроки хранения

Организация получает персональные данные только на основании того, что субъект персональных данных принимает решение о предоставлении Организации своих персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой форме, позволяющей подтвердить факт его получения. Как правило, такое согласие дается при заключении письменных договоров с Организацией или Партнерами Организации.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

В Организации обрабатываются следующие категории персональных данных:

а) Персональные данные Сотрудников и Руководителя. Источники получения: от субъектов персональных данных, на основании заключенных трудовых договоров.

б) Персональные данные Пациентов. Источники получения: от субъектов персональных данных или Партнеров, на основании заключенных договоров.

в) Персональные данные Партнеров и их представителей. Источники получения: от субъектов персональных данных или Партнеров, на основании заключенных договоров.

г) Персональные данные Посетителей. Источники получения: от субъектов персональных данных.

д) Персональные данные Соискателей. Источники получения: от субъектов персональных данных.

Сроки обработки и хранения персональных данных определяются в соответствии со сроком действия договора с субъектом персональных данных, сроком исковой давности, сроками хранения документов, в том числе медицинских, иными требованиями законодательства и нормативными документами, а также сроком предоставленного субъектом согласия на обработку персональных, в случаях, когда такое согласие должно быть предоставлено в соответствии с требованиями законодательства.

4. Передача ПДн третьим лицам

Передача персональных данных осуществляется Организацией исключительно для достижения целей, заявленных выше целей.

Передача персональных данных третьим лицам осуществляется либо с письменного согласия субъекта персональных данных, которое оформляется по установленной форме, либо для исполнения договора, стороной которого или выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем, либо в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных; либо в иных случаях, установленных федеральным законодательством.

Передача персональных данных третьим лицам осуществляется Организацией только на основании соответствующего договора с третьим лицом, существенным условием которого является обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Организация не осуществляет трансграничную передачу персональных данных.

В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Организация в ходе своей деятельности предоставляет персональные данные ниже следующим третьим лицам.

а) Персональные данные Сотрудников и Руководителя на основании трудового договора и/или письменного согласия передаются в ниже следующие организации:

- Банку – для оформления безналичного счета, на который будет перечисляться заработная плата и иные доходы Сотрудника и Руководителя, при условии, что Организация заранее сообщит Сотруднику и Руководителю наименование и адрес данного банка.

- Кредитным организациям, в которые Сотрудник обращался для оформления кредитов, ссуд либо получения иных услуг, при условии, что Сотрудник заранее сообщит Работодателю наименования указанных кредитных организаций.

- Страховой компании – для оформления полиса добровольного медицинского страхования, при условии, что Организация заранее сообщит Сотруднику наименование и адрес данной страховой компании.

- Полиграфической организации или типографии - для изготовления визитных карточек Сотрудника и Руководителя при условии, что Организация заранее сообщит им наименование и адрес данного полиграфического предприятия.

- Партнерам Организации - для исполнения обязательств, возложенных на Организацию договорами и иными законными сделками, исполнение которых предусмотрено должностными обязанностями Сотрудника, при условии, что Организация заранее сообщит Сотруднику наименования и адреса данных организаций.

- Налоговым органам, подразделениям Пенсионного фонда Российской Федерации, подразделениям Федеральной миграционной службы России - для исполнения обязательств, возложенных на Организацию законодательными и нормативными актами, а также исполнения законных официальных запросов, касающихся Сотрудника.

б) Персональные данные Пациентов в соответствии с заключенным с ними Организацией или Партнерами письменным договором, и/или с письменного согласия субъекта персональных Организации на основании договоров передает ниже следующим третьим лицам:

- Банкам – для безналичного перечисления денежных средств в счет оплаты услуг, заказанных Пациентом.

- Налоговым и правоохранительным органам - для исполнения обязательств, возложенных на Организацию законодательными и нормативными актами, а также исполнения законных официальных запросов, касающихся Пациента.

5. Получение Организацией в качестве третьего лица персональных данных от Партнеров

Получение персональных данных Пациентов от Партнеров – операторов персональных данных, осуществляется Организацией исключительно для достижения целей, заявленных для обработки персональных данных, и на основании заключенных с Партнерами письменных договоров.

В тексте договоров с Партнерами обязательно определяются цели обработки ПДн, перечень операций с ними, и устанавливается обязанность Организации соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указываются требования к защите обрабатываемых персональных данных.

6. Меры по обеспечению безопасности ПДн при их обработке

До начала обработки персональных данных Организацией предприняты правовые, технические и организационные меры к защите персональных данных от неправомерного

или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

Вводом в Организации режима конфиденциальности персональных данных, когда все документы и сведения, содержащие информацию о персональных данных, являются в Организации конфиденциальными.

Организацией режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

Утверждением полного перечня персональных данных и иных объектов, подлежащих защите в Организации.

Обеспечением нераспространения документов и сведений, содержащих информацию о персональных данных, без согласия субъекта персональных данных, либо наличия иного законного основания.

Назначением уполномоченного сотрудника, ответственного за организацию обработки персональных данных.

Введением персональной ответственности руководителя Организации и его сотрудников за обеспечение режима безопасности персональных данных при их обработке.

Утверждением перечня лиц, осуществляющих в Организации обработку персональных данных либо имеющих к ним доступ.

Определением типа угроз безопасности персональных данных, актуальных для информационных систем Организации с учетом оценки возможного вреда, который может быть причинен субъектам персональных данных.

Разработкой и утверждением локальных нормативных актов, регламентирующих в Организации обязанности должностных лиц, осуществляющих обработку и защиту ПДн, их ответственность за компрометацию персональных данных.

Осуществлением внутреннего контроля и аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам.

Запретом для Сотрудников, осуществляющих обработку персональных данных, проводить несанкционированное или нерегистрируемое копирование персональных данных, в том числе с использованием сменных носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующих различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото и видеосъемки.

Обеспечением сохранности носителей персональных данных.

Использованием средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных.

Ознакомлением Сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и обучением указанных сотрудников.

Выделением конкретных мест хранения персональных данных (материальных носителей), обработка которых осуществляется Организацией, режима обеспечения безопасности помещений и мест хранения материальных носителей ПДн.

Обеспечением раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется без использования средств автоматизации и в различных целях.

Осуществлением учета документов по обработке персональных данных без использования автоматизированных систем отдельным делопроизводством, хранением документов, содержащих персональные данные в надежно запираемых шкафах и сейфах, ключи от которых хранятся только у ответственных за данную деятельность Сотрудников.

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.

Учетом машинных носителей персональных данных.

Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих 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.

Обеспечением доступа к содержанию электронного журнала сообщений исключительно для Сотрудников Организации или уполномоченного сотрудника, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения трудовых обязанностей.

Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

7. Права и обязанности субъекта ПДн

Субъект персональных данных имеет право:

- на получение сведений от Организации: о месте ее нахождения, о наличии у Организации персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными;

- требовать от Организации уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- требовать прекращения обработки своих персональных данных;

- получать информацию, касающуюся обработки его персональных данных, в том числе содержащую: подтверждение факта обработки персональных данных Организацией, а также цель такой обработки; способы обработки персональных данных, применяемые Организацией; сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения; сроки обработки персональных данных, в том числе сроки их хранения; сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться в Организацию, которая рассматривает любые обращения и жалобы 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 в досудебном порядке.

Субъект персональных данных вправе обжаловать действия или бездействие Организации путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

Субъект персональных данных обязан предоставлять только достоверные и полные персональные данные, которые при необходимости должны быть документально подтверждены.

8. Порядок предоставления информации субъекту персональных данных

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю при обращении в Организацию либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Организация сообщает субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а так же о возможности ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает конституционные права и свободы других лиц.

Неправомерный отказ в предоставлении собранных в установленном порядке документов, содержащих персональные данные, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации может повлечь наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

9. Ответственность за обеспечение безопасности ПДн

Организация несет ответственность за разработку, введение и действенность соответствующих требованиям законодательства норм, регламентирующих получение, обработку и защиту персональных данных. Организация закрепляет персональную ответственность Сотрудников за соблюдением установленного в Организации режима конфиденциальности.

Руководитель подразделения несет персональную ответственность за соблюдение Сотрудниками его подразделения норм, регламентирующих получение, обработку и защиту персональных данных. Руководитель, разрешающий доступ сотрудника к документам и сведениям, содержащим персональные данные, несет персональную ответственность за данное разрешение.

Каждый Сотрудник, получающий для работы документ, содержащий персональные данные, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Сотрудники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Организация не несет ответственности за убытки и иные затраты, понесенные субъектами персональных данных в результате предоставления ими недостоверных и неполных персональных данных.

10. Список использованных источников правового обоснования.

Организация обязана осуществлять обработку персональных данных только на законной и справедливой основе.

- Политика Организации в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами РФ:
- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Налоговым кодексом Российской Федерации;
- Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Основами законодательства РФ "Об основах охраны здоровья граждан в Российской Федерации";
- Правилами предоставления платных медицинских услуг населению медицинскими учреждениями, утвержденными Постановлением Правительства РФ от 13.01.1996 г. №27;
- Федеральным законом № 2300-1 от 07.02.1992 года «О защите прав потребителей»;
- Постановлением Правительства Российской Федерации от 01 ноября 2012 года №1119 «Об утверждении требования к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».