

## ПОЛИТИКА обработки персональных данных

### 1. Общие положения

**1.1.** Настоящая политика в отношении обработки персональных данных (далее по тексту – «Политика») разработана **ООО "Центр современной офтальмологии"** (далее по тексту – «Оператор») в целях исполнения требований Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных». Политика определяет общий порядок, принципы и условия обработки персональных данных Оператором и обеспечивает защиту прав субъектов персональных данных при обработке их персональных данных.

**1.2.** Основные понятия, используемые в Политике:

- персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);
- оператор персональных данных (оператор) – организация, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;
- автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;
- 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;
- блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных 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;
- обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
- субъект персональных данных – физическое лицо, данные которого обрабатываются;
- конфиденциальность персональных данных – обязательное для оператора и иных лиц, получивших доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

### 2. Основные права и обязанности Оператора персональных данных

**2.1.** Оператор при сборе персональных данных обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных.

**2.2.** Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

**2.3.** При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети интернет, Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных Федеральном законе «О персональных данных».

**2.4.** Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

**2.5.** Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике, к сведениям о реализуемых требованиях к защите персональных данных. Оператор в случае осуществления сбора персональных данных с использованием информационно-телекоммуникационных сетей обязан опубликовать в соответствующей информационно-телекоммуникационной сети Политику и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием соответствующей информационно-телекоммуникационной сети.

**2.6.** Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.

**2.7.** Оператор 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. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

### **3. Основные права и обязанности субъекта персональных данных**

**3.1.** Субъект персональных данных вправе требовать от Оператора 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, а также принимать предусмотренные законом меры по защите своих прав.

**3.2.** Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных.

**3.3.** Принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы разрешается только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

**3.4.** Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

**3.5.** 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.

### **4. Цели сбора персональных данных**

**4.1.** Оператор обрабатывает персональные данные в целях:

- ✓ оказания медицинских услуг, в том числе идентификации пациентов (заказчиков), отражения информации в медицинской документации, предоставления сведений страховым компаниям (в случае оплаты ими оказываемых услуг), предоставления установленной законодательством отчетности в отношении оказанных медицинских услуг;
- ✓ выполнения требований действующего законодательства;
- ✓ в иных случаях, установленных в законе, Уставе Оператора.

**4.2.** Обработка персональных данных должна осуществляться на законной и справедливой основе.

**4.3.** Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

**4.4.** Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

**4.5.** Обработке подлежат только персональные данные, которые отвечают целям их обработки.

**4.6.** Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

## **5. Правовые основания обработки персональных данных**

**5.1.** Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных.

**5.2.** Оператор обрабатывает персональные данные на основании:

- Конституция РФ;
- Гражданский кодекс РФ;
- Налоговый кодекс РФ;
- Федеральный закон №323-ФЗ от 21.11.2011 г. «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон №152-ФЗ от 27.07.2006 г. «О персональных данных»;
- Федеральный закон №149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон №402-ФЗ от 06.12.2011 г. «О бухгалтерском учете»;
- Федеральный закон №125-ФЗ от 22.10.2004 г. «Об архивном деле в Российской Федерации»;
- Устав и иные локальные нормативные акты Оператора;
- иные нормативные правовые акты РФ и нормативные документы уполномоченных органов государственной власти;
- договоры, заключаемые между Оператором и субъектами персональных данных;
- согласие субъектов персональных данных на обработку их персональных данных.

## **6. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных**

**6.1.** Категории субъектов персональных данных, чьи данные обрабатываются.

**6.1.1.** Пациенты, законные представители пациентов.

**6.1.2.** Законные представители или представители пациентов по доверенности.

**6.2.** В отношении пациентов обрабатываются:

- ✓ фамилия, имя, отчество;
- ✓ пол;
- ✓ возраст;
- ✓ дата и место рождения;
- ✓ адреса места жительства и регистрации;
- ✓ серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- ✓ данные страхового свидетельства государственного пенсионного страхования;
- ✓ гражданство;
- ✓ данные о состоянии здоровья, в том числе биометрические персональные данные;
- ✓ семейное и социальное положение;
- ✓ контактный телефон;
- ✓ адрес электронной почты;
- ✓ реквизиты полиса обязательного медицинского страхования;
- ✓ реквизиты полиса (договора) добровольного медицинского страхования;
- ✓ тип занятости;
- ✓ место работы;
- ✓ должность.
- ✓ контактный телефон;
- ✓ адрес электронной почты;
- ✓ серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе.

**6.3.** В отношении законных представителей или представителей пациентов по доверенности указанных лиц обрабатываются:

- ✓ фамилия, имя, отчество;
- ✓ пол;
- ✓ возраст;
- ✓ дата и место рождения;
- ✓ адреса места жительства и регистрации;
- ✓ контрактный телефон;
- ✓ адрес электронной почты;
- ✓ серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- ✓ сведения о документе, который подтверждает полномочия представителя.

## **7. Порядок и условия обработки персональных данных**

**7.1.** Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных.

**7.2.** Оператор не вправе обрабатывать персональные данные субъекта персональных данных без его письменного согласия, за исключением случаев, предусмотренных статьей 6 Федерального закона «О персональных данных».

**7.3.** равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

**7.4.** Письменное согласие субъекта персональных данных должно включать:

- ✓ фамилию, имя, отчество;
- ✓ адрес субъекта персональных данных;
- ✓ номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- ✓ наименование и адрес Оператора;
- ✓ цель обработки персональных данных;
- ✓ перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- ✓ перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;
- ✓ срок, в течение которого действует согласие;
- ✓ способ его отзыва;
- ✓ подпись субъекта персональных данных.

**7.5.** Обработка персональных данных осуществляется Оператором следующими способами:

- ✓ неавтоматизированная обработка персональных данных;
- ✓ автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- ✓ смешанная обработка персональных данных.

**7.6.** Оператор организует обработку персональных данных в следующем порядке:

- 1) назначает ответственного за организацию обработки персональных данных, устанавливает перечень лиц, имеющих доступ к персональным данным;
- 2) издает настоящую Политику, локальные акты по вопросам обработки персональных данных;
- 3) применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных;
- 4) осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Оператора;
- 5) осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяет соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом;
- 6) знакомит работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политики, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

**7.7.** Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры, в том числе:

- 1) определяет угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

- 2) применяет организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
  - 3) применяет прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;
  - 4) оценивает эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
  - 5) учитывает машинные носители персональных данных;
  - 6) обнаруживает факты несанкционированного доступа к персональным данным и принимает меры;
  - 7) восстанавливает персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
  - 8) устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных.
- 7.8.** При обработке персональных данных Оператор выполняет, в частности, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
- 7.9.** В целях обеспечения сохранности и конфиденциальности персональных данных все операции с персональными данными должны выполняться только работниками Оператора, осуществляющими данную работу в соответствии с трудовыми обязанностями.
- 7.10.** Оператор получает персональные данные непосредственно от субъектов персональных данных или их представителей, наделенных соответствующими полномочиями. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном виде при заключении договора с Оператором, а также в случаях, установленных федеральным законом.
- 7.11.** Запрещается хранение документов с персональными данными и их копий на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода работника из рабочего помещения.
- 7.12.** В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специально отведенных для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.
- 7.13.** При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

## **8. Порядок обработки персональных данных в информационных системах**

- 8.1.** Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.
- 8.2.** Обеспечение безопасности при обработке персональных данных, содержащихся в информационных системах органов и подведомственных организаций, осуществляется в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных Приказом ФСТЭК России от 18.02.2013 № 21.
- 8.3.** Уполномоченному работнику, имеющему право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными обязанностями работника.
- 8.4.** Информация может вноситься как в автоматическом режиме при получении персональных данных с официального сайта в сети интернет, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.
- 8.5.** Обеспечение безопасности персональных данных, обрабатываемых в информационных системах органов, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.
- 8.6.** В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.
- 8.7.** В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:
- ✓ идентификация и аутентификация субъектов доступа и объектов доступа;
  - ✓ управление доступом субъектов доступа к объектам доступа;

- ✓ ограничение программной среды;
- ✓ защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- ✓ регистрация событий безопасности;
- ✓ антивирусная защита;
- ✓ обнаружение (предотвращение) вторжений;
- ✓ контроль (анализ) защищенности персональных данных;
- ✓ обеспечение целостности информационной системы и персональных данных;
- ✓ обеспечение доступности персональных данных;
- ✓ защита среды виртуализации и технических средств;
- ✓ защита информационной системы, ее средств, систем связи и передачи данных;
- ✓ выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
- ✓ управление конфигурацией информационной системы и системы защиты персональных данных.

**8.8.** Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

## **9. Заключительные положения**

**9.1.** Политика является общедоступным документом. Политика размещается на официальном веб-сайте Оператора в информационно-телекоммуникационной сети Интернет по адресу: 191040, Санкт-Петербург г, Лиговский пр-кт, дом № 52, литер К, помещение.1Н, оф. 44, а также на информационном стенде (стойке) и в регистратуре Оператора.

**9.2.** Ответственность лиц, имеющих доступ к персональным данным, определяется действующим законодательством Российской Федерации.