

УТВЕРЖДЕНО

приказом ООО «Курский центр  
здоровья зубов» от 05.10.2022 №

**Политика обработки и защиты персональных данных  
общества с ограниченной ответственностью «Курский центр здоровья зубов»**

**1. Общие положения**

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с пунктом 2 статьи 18.1 Закона от 27.07.2006 № 152-ФЗ «О персональных данных» и является основополагающим внутренним регулятивным документом общества с ограниченной ответственностью «Курский центр здоровья зубов» (далее – Клиника), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПД), оператором которых является Клиника.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПД и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПД в Клинике, в том числе защиты прав на неприкосновенность частной жизни, личную, семейную и врачебную тайну.

1.3. Положения Политики распространяются на отношения по обработке и защите ПД, полученных Клиникой как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПД, полученных до ее утверждения.

1.4. Обработка ПД в Клинике осуществляется в связи с выполнением Клиникой функций, предусмотренных ее учредительными документами и определяемых:

- Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановлением Правительства от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановлением Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПД в Клинике осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Клиника выступает в качестве работодателя (гл. 14 ТК), в связи с реализацией Клиникой своих прав и обязанностей юридического лица.

1.5. Клиника имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента утверждения ее приказом.

1.6. Действующая редакция хранится в месте нахождения Клиники по адресу: г. Курск, проспект Дружбы, д. 22, электронная версия Политики – на сайте по адресу: [stomcentr46.pro](http://stomcentr46.pro).

1.7. Персональные данные обрабатываются с использованием средств автоматизации или без них.

1.8. Клиника до начала обработки персональных данных обязана уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять

обработку персональных данных согласно частям 1 и 3 статьи 22 Федерального закона 27.07.2006 № 152-ФЗ «О персональных данных».

1.9. Приказом директора Клиники назначается ответственное лицо за организацию обработки персональных данных.

## **2. Термины и принятые сокращения**

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

2.2. 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.

2.3. 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.

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

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

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

2.7. 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.

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

2.9. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.10. Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.11. Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

2.12. Медицинская деятельность – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

2.13. Лечащий врач – врач, на которого возложены функции по организации и непосредственно оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

### **3. Принципы обеспечения безопасности персональных данных**

3.1. Основной задачей обеспечения безопасности ПД при их обработке в Клинике является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПД, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПД Клиника руководствуется следующими принципами:

- законность: защита ПД основывается на положениях нормативных правовых актов методических документов уполномоченных государственных органов в области обработки защиты ПД;
- системность: обработка ПД в Клинике осуществляется с учетом всех взаимосвязанных взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПД;
- комплексность: защита ПД строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Клиники и других имеющихся в Клинике систем и средств защиты;
- непрерывность: защита ПД обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПД, в том числе при проведении ремонтных регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПД, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер средств защиты ПД осуществляется на основании результатов анализа практики обработки ПД в Клинике с учетом выявления новых способов и средств реализации угроз безопасности ПД, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПД возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПД;
- минимизация прав доступа: доступ к ПД предоставляется Работникам только в объеме необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты ПД при изменении характеристик функционирования информационных систем персональных данных Клиники, а также объема и состава обрабатываемых ПД;
- специализация и профессионализм: реализация мер по обеспечению безопасности ПД осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Клиники предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить и минимизировать возможность нарушения ими безопасности ПД;
- наблюдаемость и прозрачность: меры по обеспечению безопасности ПД должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны), могли быть оценены лицами, осуществляющими контроль;

– непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПД, а результаты контроля регулярно анализируются.

3.3. В Клинике не производится обработка ПД, несовместимая с целями их сбора. Если иное предусмотрено федеральным законом, по окончании обработки ПД в Клинике, в том числе по достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Клинике ПД уничтожаются или обезличиваются.

3.4. При обработке ПД обеспечиваются их точность, достаточность, а при необходимости – актуальность по отношению к целям обработки. Клиника принимает необходимые меры удалению или уточнению неполных или неточных ПД.

## **4. Обработка персональных данных**

### **4.1. Получение ПД**

4.1.1. Все ПД следует получать от самого субъекта. Если ПД субъекта можно получить только третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

4.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способ получения ПД, характере подлежащих получению ПД, перечне действий с ПД, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.1.3. Документы, содержащие ПД, создаются путем:

- а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и т. д.);
- б) внесения сведений в учетные формы;
- в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и т. д.).

Порядок доступа субъекта ПД к его ПД, обрабатываемым Клиникой, определяется соответствии с законодательством и определяется внутренними регулятивными документами Клиники.

### **4.2. Обработка ПД:**

4.2.1. Обработка персональных данных осуществляется:

- с согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, когда обработка персональных данных необходима для осуществления выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).

Доступ Работников к обрабатываемым ПД осуществляется в соответствии с должностными обязанностями и требованиями внутренних регулятивных документов Клиники.

Допущенные к обработке ПД Работники под подпись знакомятся с документами Клиники, устанавливающими порядок обработки ПД, включая документы, устанавливающие права и обязанности конкретных Работников.

Клиникой производится устранение выявленных нарушений законодательства об обработке и защите ПД.

4.2.2. Цели обработки ПД:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с законами от 21.11.2007 № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12.04.2008 № 61-ФЗ «Об обращении лекарственных средств» и от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правила предоставления медицинскими организациями платных медицинских услуг, утвержденные постановлением Правительства от 04.10.2012 № 1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

#### 4.2.3. Категории субъектов персональных данных

В Клинике обрабатываются ПД следующих субъектов:

- физические лица, состоящие с Клиникой в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников Клиники;
- физические лица, уволившиеся из Клиники;
- физические лица, являющиеся кандидатами на работу в Клинике;
- физические лица, состоящие с Клиникой в гражданско-правовых отношениях;
- физические лица, обратившиеся в Клинику за медицинской помощью.

#### 4.2.4. ПД, обрабатываемые Клиникой:

- полученные при осуществлении трудовых отношений;
- полученные для осуществления отбора кандидатов на работу в Клинику;
- полученные при осуществлении гражданско-правовых отношений;
- полученные при оказании медицинской помощи.

Полный список ПД представлен в перечне ПД, утвержденном директором Клиники.

#### 4.3. Обработка персональных данных ведется:

- с использованием средств автоматизации;
- без использования средств автоматизации.

#### 4.4. Хранение ПД

4.4.1. ПД субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.4.2. ПД, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа (например, регистратура).

4.4.3. ПД субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.4.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.4.5. Хранение ПД в форме, позволяющей определить субъекта ПД, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

#### 4.5. Уничтожение ПД

4.5.1. Уничтожение бумажных документов (носителей), содержащих ПД, производится путем сожжения.

4.5.2. ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.5.3. Уничтожение производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей, подписанным членами комиссии (не менее трех человек).

#### 4.6. Передача ПД

4.6.1. Клиника передает ПД третьим лицам, если субъект выразил свое согласие на такие действия или передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.6.2. Перечень третьих лиц, которым передаются ПД:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Фонд социального страхования (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- судебные и правоохранительные органы в случаях, установленных законодательством;
- бюро кредитных историй (с согласия субъекта);
- юридические компании, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта).

## **5. Защита персональных данных**

### **5.1. Подсистема защиты персональных данных**

5.1.1. В соответствии с требованиями нормативных документов Клиникой создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.1.2. Подсистема правовой защиты представляет собой комплекс правовых, организационных, распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.1.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами, сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.1.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПД.

5.2. Основными мерами защиты ПД, используемыми Клиникой, являются:

5.2.1. Назначение лица ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением Клиникой и ее работниками требований к защите ПД.

5.2.2. Определение актуальных угроз безопасности ПД при их обработке в ИСПД и разработка мер и мероприятий по защите ПД.

5.2.3. Разработка политики в отношении обработки персональных данных.

5.2.4. Установление правил доступа к ПД, обрабатываемым в ИСПД, а также обеспечение регистрации и учета всех действий, совершаемых с ПД в ИСПД.

5.2.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

5.2.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПД, обеспечение их сохранности.

5.2.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

5.2.8. Сертифицированное программное средство защиты информации от несанкционированного доступа.

5.2.9. Сертифицированные межсетевой экран и средство обнаружения вторжения.

5.2.10. Соблюдение условий, обеспечивающих сохранность ПД и исключаяющих несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПД.

5.2.11. Установление правил доступа к обрабатываемым ПД, обеспечение регистрации и учётных действий, совершаемых с ПД, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер.

5.2.12. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.2.13. Обучение работников Клиники, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Клиники в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

5.2.14. Осуществление внутреннего контроля и аудита.

5.2.15. Сотрудники Клиники, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены под подпись до начала работы с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политикой, локальными актами по вопросам обработки персональных данных, с данным Положением и изменениями к нему.

## **6. Основные права субъекта ПД и обязанности Клиники**

### **6.1. Основные права субъекта ПД**

6.1.1. Субъект ПД имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Законами № 152-ФЗ от 27.07.2006, № 266-ФЗ от 14.07.2022) или другими федеральными законами.

6.1.2. Субъект ПД вправе требовать от оператора уточнения его персональных данных, 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.

### **6.2. Обязанности Клиники:**

#### **6.2.1. Клиника обязана:**

- при сборе ПД предоставить информацию субъекту об обработке его ПД;

- в случаях, если ПД были получены не от субъекта ПД, уведомить субъекта;
- при отказе в предоставлении ПД субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документам, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;
- принимать необходимые правовые, организационные и технические меры и обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД, а также от иных неправомерных действий в отношении ПД;
- давать ответы на запросы и обращения субъектов ПД, их представителей и компетентных органов по защите прав субъектов ПД;
- не сообщать персональные данные субъекта ПД третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом или иными федеральными законами;
- не сообщать персональные данные субъекта ПД в коммерческих целях без письменного согласия;
- предупредить лиц, получающих персональные данные субъекта ПД, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;
- разрешать доступ к персональным данным субъекта ПД только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только персональные данные субъекта ПД, которые необходимы для выполнения конкретных функций.

## **7. Ответственность за нарушение норм, регулирующих обработку и защиту ПД**

7.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных субъектов ПД, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.