

«УТВЕРЖДАЮ»

Директор
ООО «Стоматологическая клиника «Престиж»



Маврицкий Е.Ю.

01 июля 2017 года

**Порядок, условия обработки персональных
данных и реализация требований по
защите персональных данных в ООО
«Стоматологическая клиника «Престиж»**

г. Екатеринбург
2017

1. Общие положения

1. Политика ООО «Стоматологическая клиника «Престиж» в отношении обработки персональных данных (далее – Политика) определяет порядок, условия обработки персональных данных и реализацию требований по защите персональных данных в ООО «Стоматологическая клиника «Престиж»
2. Политика в отношении обработки персональных данных ООО «Стоматологическая клиника «Престиж» , ОГРН 1146671011442 ИНН 6671450746, адрес: г. Екатеринбург, ул. Гоголя д.36, оф.1203 (далее – Оператор) разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», иными федеральными законами и нормативно правовыми актами.
3. В настоящей Политике используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».
4. Политика разработана с целью обеспечения защиты прав и свобод субъекта персональных данных (ПДн) при обработке его ПДн. ПДн являются конфиденциальной информацией. Обеспечение необходимого и достаточного уровня безопасности ПДн и другой конфиденциальной информации является важнейшим условием деятельности ООО «Стоматологическая клиника «Престиж» .
5. Настоящая Политика действует в отношении всех информационных данных, которые сайт Оператора (ООО «Стоматологическая клиника «Престиж»), расположенный на доменном имени www.стоматология-престиж.рф(далее – Сайт) может получить от Пользователя во время использования им сайта.

2. Принципы обработки персональных данных

1. Обработка ПДн осуществляется Оператором на законной и справедливой основе.
2. При обработке ПДн Оператором соблюдаются следующие принципы:
 - обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей; не допускается обработка ПДн, несовместимая с целями сбора ПДн;
 - не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
 - обработке подлежат только ПДн, которые отвечают целям их обработки;
 - содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки; не допускается избыточность обрабатываемых ПДн по отношению к заявленным целям их обработки;
 - получение персональных данных может осуществляться как путем представления их самими субъектами персональных данных, так и путем получения их из иных источников.
 - ПДн следует получать у самого субъекта персональных данных. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен

сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

- при обработке ПДн обеспечивается точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн; принимаются необходимые меры по удалению или уточнению неполных или неточных данных;
- хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3. Сроки хранения документов, в том числе электронных документов, содержащих ПДн, определены приказом Оператора. Порядок уничтожения документов, содержащих ПДн, установлен Инструкцией по делопроизводству.

3. Цели обработки персональных данных

1. ПДн обрабатываются Оператором в следующих целях:
 1. Обработка ПДн необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей, в частности:
 - выполнение требований законодательства в сфере труда и налогообложения;
 - ведение текущего бухгалтерского и налогового учёта, формированию, изготовлению и своевременной подаче бухгалтерской, налоговой и статистической отчётности.
 2. Обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством, в частности:
 - индивидуального (персонифицированного) учёта в системе обязательного пенсионного страхования;
 - обязательного медицинского страхования.
 3. 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 или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем.
 4. Обработка ПДн необходима для информационного обеспечения Общества и клиентов.
 5. Обработка ПДн осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка ПДн осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

6. Обработка ПДн необходима для защиты жизни, здоровья, или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно.
7. Обработка ПДн осуществляется в статистических целях при условии обязательного обезличивания ПДн.
8. Обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе (далее – ПДн, сделанные общедоступными субъектом ПДн), включая размещение на корпоративном сайте Общества.
9. Обработка ПДн осуществляется с целью установления обратной связи с субъектом ПДн и обработкой его заявок и запросов;
10. Обработка ПДн осуществляется с целью уведомления субъектом ПДн о статусе обработки его заявок и запросов;
11. Обработка ПДн осуществляется с целью предоставления субъекту ПДн персональной технической поддержки в случае возникновения вопросов, связанных с использованием сайта Оператора.
12. Обработка ПДн осуществляется в целях информирования Пользователя о специальных предложениях, акциях, скидках и новостях от имени Оператора.

4. **Правовое основание обработки персональных данных**

Обработка ПДн осуществляется на основе следующих федеральных законов и нормативно-правовых актов:

- Гражданский Кодекс РФ;
- Трудовой Кодекс РФ от 30.12.2001 №197-ФЗ (ст. 65, ст. 85-90);
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Государственного комитета Российской Федерации по статистике от 05.01.2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;
- Приказ ФНС России от 17.10.2010 № ММВ-7-3/611 «Об утверждении формы сведений о доходах физических лиц и рекомендации по ее заполнению, формата сведений о доходах физических лиц в электронном виде, справочников»;
- Федеральный закон РФ от 24.07.2009 №212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования»;
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования».
- Постановление Правления ПФР РФ от 31.07.2006 № 192п «О формах документов индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования и инструкции по их заполнению»;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Постановление Правительства РФ от 04.10.2012 № 1006 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг»;

- Приказ Минздравсоцразвития России от 22.11.2004 No 255 «О порядке оказания первичной медико-санитарной помощи гражданам, имеющим право на получение набора социальных услуг»;
- Приказ ФМБА РФ от 30.03.2007 No 88 «О добровольном информированном согласии на медицинское вмешательство»;
- Федеральный закон от 29.11.2010 No 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Приказ Минздравсоцразвития России от 28.02.2011 No 158Н «Об утверждении Правил обязательного медицинского страхования»;
- Приказ Федерального фонда обязательного медицинского страхования от 01.12.10 No 230 «Об утверждении Порядка организации и проведения контроля объемов, сроков, качества и условий предоставления медицинской помощи по обязательному медицинскому страхованию»;
- Приказ Минздравсоцразвития России от 02.05.2012 No 441н «Об утверждении Порядка выдачи медицинскими организациями справок и медицинских заключений»;
- Постановление Правительства Омской области от 12.12.2012 No 262-п «О Территориальной программе государственных гарантий бесплатного оказания гражданам медицинской помощи в Омской области на 2013 год и на плановый период 2014 и 2015 годов».
- Закон РФ от 27.11.1992 No 4015-1 «Об организации страхового дела в Российской Федерации»;
- Федеральный закон от 02.05.2006 No 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Закон РФ от 07.02.1992 No 2300-1 «О защите прав потребителей»;
- Письмо Банка России от 02.10.2009 No 120-Т «О памятке «О мерах безопасного использования банковских карт».

5. **Перечень действий с персональными данными**

При обработке ПДн оператор будет осуществлять следующие действия с ПДн: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

6. **Состав обрабатываемых персональных данных**

Обработке Оператором подлежат ПДн следующих субъектов ПДн:

ПДн работников в составе:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- знание иностранного языка;
- сведения об образовании (включая название образовательного учреждения, специальность, квалификацию);
- семейное положение,
- сведения о составе семьи;
- паспортные данные (вид документа, серия и номер документа, наименование органа, выдавшего документ, дата выдачи документа);

- адрес регистрации и фактического места жительства;
- банковские реквизиты;
- сведения о трудовой деятельности;
- сведения воинского учета;
- ученая степень;
- ученое звание;
- почетное звание;
- сведения о дате защиты и теме диссертации, диплома;
- сведения о прохождении за последние пять лет повышения квалификации или профессиональной переподготовки или стажировки, способствующие подготовке к решению задач, стоящих перед руководством;
- сведения о наградах/поощрениях;
- сведения о привлечении к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности;
- биографические данные;
- сведения о государственном пенсионном страховании;
- идентификационный номер налогоплательщика;
- сведения об отчислениях в Федеральную налоговую службу;
- сведения об отчислениях в Пенсионный фонд России;
- сведения о начислениях и удержаниях;
- подразделение;
- должность;
- табельный номер;
- сведения трудового договора (номер, дата, испытательный срок), график работы;
- инвалидность;
- сведения о налоговых вычетах;
- сведения о наградах;
- сведения об отпуске;
- социальные льготы;
- данные больничного листа;
- сведения о дополнительных навыках;
- контактный телефон;
- адрес электронной почты (email);
- ссылки на персональный сайт, профили в социальных сетях;
- данные об изображении лица.

1. ПДн клиентов в составе:

- фамилия, имя, отчество;
- дата рождения;
- возраст;
- пол;
- СНИЛС;
- номер телефона;
- данные, документа удостоверяющий личность (тип документа, серия, номер дата выдачи, наименование органа, выдавшего документ);
- гражданство;
- социальный статус;

- место работы;
 - место учебы;
 - должность;
 - адрес прописки;
 - адрес проживания;
 - полис ОМС (серия и номер, дата действия);
 - номер договора;
 - ЛПУ прописки;
 - полис ДМС (серия и номер, дата действия);
 - сведения об оплате;
 - медицинские сведения;
 - контактный телефон;
 - адрес электронной почты (email);
 - данные cookie;
 - данные IP-адреса;
 - ссылки на персональный сайт, профили социальных сетей;
 - данные об изображении лица.
2. ПДн контрагентов в составе:
- фамилия, имя, отчество;
 - идентификационный номер налогоплательщика;
 - адрес;
 - контактный телефон;
 - банковские реквизиты;
 - сведения о договоре.
3. Основанием для обработки ПДн субъекта, не являющегося работником Оператора или лицом, заключившим с Оператором договор, является согласие субъекта ПДн на обработку его ПДн в письменной форме.
4. Использование субъектом ПДн сайта Оператора, расположенному в сети Интернет по адресу www.стоматология-престиж.рф, означает согласие с настоящей Политикой в отношении обработки персональных данных. В случае несогласия с условиями Политики конфиденциальности Субъект ПДн должен прекратить использование сайта.
5. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе.
6. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям обработки.
7. **Обработка ПДн**
1. ПДн клиентов и контрагентов обрабатываются Оператором с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, и без использования таких средств, с фиксацией ПДн на материальном носителе (бумажные документы).
2. ПДн работников обрабатываются Оператором с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, и без использования таких средств, с фиксацией ПДн на материальном носителе (бумажные документы).

8. Обеспечение защиты персональных данных при их обработке

Оператором

1. Оператор принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152 «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152 «О персональных данных», Постановлением Правительства от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Приказом ФСТЭК от 18.02.2013 №21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами, если иное не предусмотрено федеральными законами. К таким мерам могут, в частности, относиться:

- назначение Оператором ответственного за организацию обработки ПДн;
- издание Оператором документов, определяющих политику оператора в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности ПДн;
- осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике Оператора в отношении обработки ПДн, локальным актам оператора;
- оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
- ознакомление работников Оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику Оператора в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников.

2. Оператор при обработке ПДн принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

3. С целью обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных

данных» и принятыми в соответствии с ним нормативными правовыми актами Оператором приняты следующие меры:

- приняты правовые, организационные и технические меры, установленные законодательством Российской Федерации в области ПДн, по обеспечению безопасности обрабатываемых ПДн;
- назначено лицо, ответственное за организацию обработки ПДн;
- приказом директора ООО «Стоматологическая клиника «Престиж» утверждены следующие документы: правила обработки ПДн; правила рассмотрения запросов субъектов ПДн или их представителей; правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Оператора; правила работы Оператора с обезличенными ПДн; перечень информационных систем ПДн Оператора; перечень ПДн, обрабатываемых Оператором в связи с реализацией трудовых отношений, а также в связи с оказанием медицинских услуг и осуществлением текущей хозяйственной деятельности; перечень должностей Оператора, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн; перечень должностей Оператора, замещение которых предусматривает осуществление обработки ПДн, либо осуществление доступа к ПДн; должностная инструкция лица ответственного, за организацию Оператором обработки ПДн; типовое обязательство работника Оператора, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним трудового договора прекратить обработку ПДн, ставших известными ему в связи с исполнением должностных обязанностей; типовая форма согласия на обработку ПДн работников Оператора, иных субъектов ПДн; порядок доступа работников Оператора в помещения, в которых ведется обработка ПДн; список работников Оператора, ответственных за обеспечение безопасности ПДн и сохранность носителей ПДн в служебных помещениях; список работников Оператора, допущенных к обработке ПДн; инструкции администратору безопасности информации и пользователям;
- выполнены требования по обработке ПДн, осуществляемой без использования средств автоматизации;
- с целью осуществления внутреннего контроля за соответствием обработки ПДн обязательным требованиям Оператором организовано проведение периодических проверок условий обработки ПДн работниками Оператора, допущенных к обработке ПДн;
- работники Оператора, непосредственно осуществляющие обработку ПДн, ознакомлены с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), локальными актами по вопросам обработки ПДн.

4. Оператором разработана частная модель угроз безопасности ПДн, на основании которой выполнено построение системы защиты ПДн. При этом, использовались следующие основные принципы построения системы безопасности ПДн:

- законность;
- системность,
- комплексный подход;

- непрерывность защиты;
 - своевременность;
 - преемственность и совершенствование;
 - разумная достаточность (экономическая целесообразность);
 - минимизация полномочий;
 - персональная ответственность;
 - гибкость системы защиты;
 - применение только сертифицированных средств защиты информации;
 - обоснованность и реализуемость;
 - специализация и профессионализм обслуживающего персонала;
 - обязательность контроля.
5. Объектами защиты являются:
- ПДн, обрабатываемые и хранящиеся на серверах, на автоматизированных рабочих местах пользователей (далее — АРМ), на отчуждаемых (съемных) носителях информации, на выносных терминалах, мониторах, в средствах звукозаписи, звуковоспроизведения;
 - ПДн, передаваемые по каналам и линиям связи;
 - ПДн, хранящиеся в документированном виде на бумажных носителях;
 - прикладное и системное программное обеспечение серверов, АРМ, используемых для обработки ПДн;
 - аппаратные средства программно-технических комплексов, оборудование серверов, АРМ, коммуникационное оборудование;
 - средства защиты информации информационных систем ПДн;
 - съемные (отчуждаемые) машинные носители информации — накопители на гибких и жестких магнитных дисках, Flash-накопители, оптические диски (CD-R, CD-RW, DVD-R, DVD-RW), аудио-, видеокассеты, магнитные ленты и т.д.
6. Рабочие и служебные помещения Оператора находятся под охраной. Доступ посетителей в служебные помещения Оператора, в которых ведется обработка ПДн, разрешен только после регистрации в книге учета посетителей, находящейся у администратора.
7. Компоненты информационных систем ПДн Оператора размещаются в помещениях, находящихся под охраной и наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.д.). По окончании рабочего дня служебные помещения сдаются под охрану в соответствии с приказом директора ООО «Стоматологическая клиника «Престиж»
9. **Право субъекта персональных данных на доступ к его персональным данным**
0. Субъект ПДн вправе требовать от Оператора 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.
1. Сведения предоставляются субъекту ПДн или его представителю оператором при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о

дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Оператором, подпись субъекта ПДн или его представителя. Запрос может быть направлен на электронную почту Оператора prestigest@mail.ru в форме электронного документа.

2. Оператор вправе отказать субъекту ПДн в выполнении повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

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

- подтверждение факта обработки ПДн Оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые Оператором способы обработки ПДн;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором 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 Федеральным законом «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 Оператора, если обработка поручена или будет поручена такому лицу.

4. В случае, если субъект ПДн считает, что оператор осуществляет обработку его ПДн с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

5. 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.

10. **Заключительные положения**

0. Настоящая Политика является общедоступным документом и подлежит размещению на Сайте Оператора.

1. Настоящая Политика подлежит пересмотру в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

2. Контроль за исполнением требований настоящей Политики осуществляется ответственными лицами компании Оператора, назначаемыми в установленном порядке локальным актом.

3. Ответственность должностных лиц компании – Оператора, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и

защиту персональных данных, определяется в соответствии с действующим законодательством Российской Федерации в области персональных данных и локальными актами Компании.

4. Иные права и обязанности компании – Оператора определяются законодательством Российской Федерации в области персональных данных