

«УТВЕРЖДЕНО»

ООО «Дентком»

Директор Добрычева  
Екатерина  
Владимировна

М.П.

Дата

## ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ в ООО «Дентком» для Пациентов

### I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящим положением определяется порядок сбора, систематизации, накопления, уточнения, использования, хранения, распространения и защиты персональных данных работников и клиентов ООО «Дентком».

1.2. Настоящее положение разработано в строгом соответствии с требованиями:

- Конституции РФ;
- гл. 14 Трудового кодекса РФ;
- Перечнем сведений конфиденциального характера, утв. Указом Президента РФ от 06.03.1997г., № 188;
- Федерального закона «О персональных данных» от 27.07.2006г., №152-ФЗ;
- ФЗ № 242 от 21.07.2014 года «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»;
- ФЗ № 323 от 21.11.2011 года «Об основах охраны здоровья граждан в РФ»;
- Постановлением Правительства РФ № 1119 от 01.11.2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства РФ № 687 от 15.09.2008 года «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказа ФСТЭК России № 21 от 18.02.2013 года «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Настоящее Положение разработано с учетом понимания законодательства о персональных данных, изложенного в Научно-практическом комментарии к ФЗ «О персональных данных» под ред. Зам.руководителя Федеральной службы Роскомнадзора Приезжевой А.А.

1.4. В настоящем Положении используются следующие термины и понятия:

**Работник** – физическое лицо, состоящее в трудовых отношениях с работодателем.

**Персональные данные работника** – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (сведения о фактах, обстоятельствах и событиях частной жизни).

**Клиент (пациент)** – физическое лицо, выступающее стороной в гражданско-правовом договоре на оказание медицинских услуг.

**Обработка персональных** – 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.

**Защита персональных данных** – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном работнике, клиенте.

**Конфиденциальная информация** – это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

**Предприятие, работодатель, клиника** – ООО «Дентком».

## **II. ПЕРСОНАЛЬНЫЕ ДАННЫЕ КЛИЕНТОВ (ПАЦИЕНТОВ)**

### **Раздел 1. Состав сведений (персональных данных) о клиентах и цели их обработки.**

**2.1. Персональные данные пациентов (лиц, являющихся стороной договора на оказание медицинских услуг), обрабатываемые на предприятии:**

- паспортные данные;
- номера телефонов для связи с пациентом (контактная информация);
- информация о состоянии здоровья пациента, поставленных диагнозах, проведенном или планируемом к проведению медицинском вмешательстве.

2.2. Персональные данные пациентов, полученные при заключении договора на медицинские услуги, обрабатываются только в целях предоставления качественной медицинской помощи, проведения оценки качества оказываемых услуг, в целях обеспечения оплаты лечения пациентов посредством страховых компаний.

2.3. Предприятие обеспечивает конфиденциальность персональных данных клиентов и обязано не допускать их распространения без согласия клиентов, либо наличия иного законного основания.

2.4. Все меры конфиденциальности при сборе, обработке и хранении персональных данных клиентов распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

### **Раздел 2. Порядок обработки персональных данных клиентов.**

2.5. Предприятие получает персональные данные непосредственно от субъекта персональных данных – Клиента, на основании заключения с Клиентом письменного договора на медицинские услуги.

2.6. В силу пп.5, ч.1 ст.6, пп.4.ч.2 ст. 10 ФЗ № 152 «О персональных данных» письменного согласия на обработку персональных данных о здоровье пациента не требуется.

По смыслу ч.1 ст. 11 ФЗ № 152 «О персональных данных» рентгеновские снимки, слепки зубов, фотографии пациентов не являются биометрическими данными, поскольку не используются оператором для установления личности субъекта персональных данных.

Согласие на обработку персональных данных пациентов берется Клиникой с целью демонстрации пациентам серьезности намерений соблюдения конфиденциальности, а также предупреждения о тех случаях, когда информация о здоровье пациента может быть передана третьим лицам без его согласия

2.7. Обработка персональных данных Клиента осуществляется Предприятием исключительно для достижения целей, определенных письменным договором между Клиентом и Предприятием, в частности для оказания медицинских услуг Клиенту.

2.8. Обработка персональных данных Клиентов ведется методом смешанной (в том числе автоматизированной) обработки.

2.9. К обработке персональных данных Клиента могут иметь доступ только сотрудники Предприятия, допущенные к работе с персональными данными Клиента.

2.10. Отзыв пациентом согласия на обработку персональных данных о здоровье не влечет прекращения обработки персональных данных в силу ч. 2 ст. 9 ФЗ № 152 «О персональных данных».

2.11. Предприятие уничтожает персональные данные Клиента, за исключением данных, содержащихся в медицинской карте и иной медицинской документации, в следующие сроки: хранящиеся на электронных носителях в течение трех рабочих дней с момента расторжения договора или отзыва согласия на обработку.

2.12. Передача персональных данных Клиента осуществляется Предприятием исключительно для достижения целей, определенных письменными договорами между Клиентом – Предприятием, в

частности для оплаты медицинских услуг, оказываемых на основании договоров добровольного медицинского страхования.

Передача копии медицинской карты для экспертизы страховой компании осуществляется в бумажном виде - копии, заверенной надлежащим образом, по запросу страховой компании на имя директора клиники и в силу пп.8 ч. 2 ст. 10 ФЗ № 152 «О персональных данных» не требует письменного согласия пациента.

2.13. Без согласия клиента персональные данные о состоянии его здоровья могут быть переданы в случаях, прямо предусмотренных ст. 13 ФЗ «Об основах охраны здоровья граждан в РФ» **в случае возникновения угрозы распространения инфекционных заболеваний** (гепатиты, ВИЧ, сифилис, ОРИ, туберкулез), о чем клиент уведомляется в согласии на обработку его персональных данных.

2.14. Персональные данные Клиентов могут храниться, как на бумажных носителях, так и в электронном виде.

2.15. Персональные данные Клиентов содержатся в следующих группах документов:

- договор на оказание медицинских услуг и все приложения к нему;
- согласие родителей на подписание договора несовершеннолетним;
- Анкета о здоровье;
- медицинская карта;
- информированные согласия на различные виды медицинских манипуляций;
- протоколы фиксации претензий пациентов.

2.16. Персональные данные Клиентов на бумажных носителях, если с них не снят на законном основании режим конфиденциальности, хранятся в специально отведенных железных шкафах.

2.17. Ключи от железных шкафов хранятся лично у старшей медицинской сестры, допущенной к обработке персональных данных Клиентов.

2.18. Персональные данные Клиентов также хранятся в электронном виде: в локальной компьютерной сети Предприятия, в базах данных, каталогах и файлах, размещенных на серверах предприятия, доступ к которым разрешен сотрудникам, допущенным к обработке персональных данных Клиентов.

2.19. При передаче персональных данных Клиента Предприятие должно соблюдать следующие требования:

- не сообщать персональные данные Клиента третьей стороне без письменного согласия Клиента, за исключением случаев, установленных федеральным законом;
- не сообщать персональные данные Клиента в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные Клиента 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 Клиентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные Клиентов, которые необходимы для выполнения конкретных функций.

### **Раздел 3. Права и обязанности предприятия при обработке персональных данных клиента (пациента).**

2.20. В целях обеспечения прав и свобод человека и гражданина **Предприятие и его сотрудники при обработке персональных данных Клиента обязаны соблюдать следующие общие требования:**

2.20.1. При определении объема и содержания персональных данных Клиента, подлежащих обработке, Предприятие должно руководствоваться Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных», ФЗ № 323 от 21.11.2011 года, договорными обязательствами, взятыми на себя сторонами по договору между Клиентом и Предприятием. Предприятие получает персональные данные Клиентов только в объеме, необходимом для достижения целей, указанных в договоре с Клиентом.

2.20.2. Предприятие не имеет права получать и обрабатывать персональные данные Клиента о его судимости, политических, религиозных и иных убеждениях и частной жизни.

2.21. Предприятие должно обеспечить защиту персональных данных Клиента от неправомерного их использования или утраты за собственный счет в порядке, установленном федеральным законодательством.

2.22. Предприятие обязано сообщить Клиенту информацию о наличии персональных данных о нем, а также предоставить возможность ознакомления с ними в течение:

- 3 рабочих дней с момента обращения (подачи запроса) – если речь идет о предоставлении медицинской справки или медицинского заключения,

- 5 рабочих дней с момента обращения (подачи запроса)– если речь идет о предоставлении информации в виде копии медицинской карты.

2.23. Все сотрудники, связанные с получением, обработкой и защитой персональных данных Клиентов, обязаны подписать уведомление-обязательство о неразглашении персональных данных Клиентов (Приложение 2).

**Процедура оформления доступа к персональным данным Клиента включает в себя:**

- Ознакомление сотрудника под роспись с настоящим Положением. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных Клиента, с данными актами также производится ознакомление под роспись.

- Уведомление сотрудника о факте обработки персональных данных;

- Истребование с сотрудника (за исключением директора) письменного обязательства о соблюдении конфиденциальности персональных данных Клиентов и соблюдении правил их обработки, подготовленного по установленной форме (Приложение 2).

2.24. Сотрудник Предприятия, имеющий доступ к персональным данным Клиентов в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные Клиента, исключаящее доступ к ним третьих лиц;

- в отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные Клиентов;

- при уходе в отпуск, во время служебной командировке и иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные Клиентов директору Предприятия.

2.25. Допуск к персональным данным Клиента других сотрудников Предприятия (санитарок, охранников, бухгалтеров), не имеющих надлежащим образом оформленного доступа, запрещается.

#### **Раздел 4. Права и обязанности Клиента (пациента).**

2.26. Клиент обязан передавать Предприятию или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен настоящим Положением и договорными обязательствами, взятыми на себя сторонами по договору между Клиентом - Предприятием.

2.27. Клиент должен без неоправданной задержки сообщать Предприятию об изменении своих персональных данных.

2.28. Клиент имеет право на получение сведений о Предприятии, о месте его нахождения, о наличии у Предприятия персональных данных, относящихся к Клиенту, а также на ознакомление с такими персональными данными.

Клиент вправе требовать от Предприятия 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, а также принимать предусмотренные законом меры по защите своих прав.

2.29. Доступ Клиента к своим персональным данным предоставляется на основании письменного запроса пациента на имя главного врача клиники. Запрос должен содержать номер основного документа, удостоверяющего личность Клиента или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись Клиента или его законного представителя.

2.30. Сведения о наличии персональных данных должны быть предоставлены Клиенту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

2.31. Клиент имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных Предприятием, а также цель такой обработки;

2) способы обработки персональных данных, применяемые Предприятием;

3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

4) перечень обрабатываемых персональных данных и источник их получения;

5) сроки обработки персональных данных, в том числе сроки их хранения;

6) сведения о том, какие юридические последствия для Клиента может повлечь за собой обработка его персональных данных.

2.32. Клиент имеет право отозвать согласие на обработку персональных данных, ограничить способы и формы обработки персональных данных, запретить распространение персональных данных без его согласия. Отзыв пациентом согласия на обработку персональных данных о здоровье не влечет прекращения обработки персональных данных в силу ч. 2 ст. 9 ФЗ № 152 «О персональных данных».

2.33. Клиент вправе обжаловать действия или бездействие Предприятия в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2.34. Клиент имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда в судебном порядке.

### **III. СИСТЕМА МЕР ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

3.1. Общую организацию защиты персональных данных Клиентов осуществляет директор Предприятия.

3.2. Защита персональных данных Клиентов, хранящихся в электронных базах данных Предприятия, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается специалистом ИТ, находящимся в штате предприятия либо оказывающим услуги на основании договора подряда.

**3.3. Система мер защиты персональных данных в зависимости от типа угроз включает в себя:**

- Охрана клиники
- Сигнализация
- Защита сервера
- Логины-пароли для каждого сотрудника при входе в информационную систему клиники.

### **IV. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

4.1. Предприятие несет ответственность за разработку, введение и действенность соответствующих требованиям законодательства норм, регламентирующих получение, обработку и защиту персональных данных Клиента и сотрудников. Предприятие закрепляет персональную ответственность сотрудников за соблюдением установленного в организации режима конфиденциальности.

4.2. Руководитель, разрешающий доступ сотрудника к документам, содержащим персональные данные Клиента, несет персональную ответственность за данное разрешение.

4.3. Каждый сотрудник Предприятия, получающий для работы документ, содержащий персональные данные Клиента, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

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

Ст. 150, 151 ГК РФ - гражданско-правовая ответственность;

Ст. 13.14 КоАП РФ – административная ответственность;

Ст. 137 УК РФ - уголовная ответственность.

4.5. За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка обработки персональных данных Клиентов Предприятие вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания, в том числе, увольнение на основании пп. «в» п. 6 статьи 81 Трудового кодекса РФ за разглашение персональных данных другого работника.

### **V. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

Настоящее положение вступает в силу с момента издания Приказа директора организации о введении Положения в силу, и обязательно для ознакомления, соблюдения и исполнения всеми сотрудниками организации.

