

УТВЕРЖДАЮ
Директор
ООО «Дентал Диагностика»

С.А.Карпов

01.02.2023

ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
общества с ограниченной ответственностью «Дентал Диагностика»
(ООО «Дентал Диагностика»)

Магнитогорск

01.02.2023

1. Общие положения

1.1. Настоящая Политика общества с ограниченной ответственностью «Дентал Диагностика» в отношении обработки Персональных Данных (далее - Политика) разработана во исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о ПД) в целях обеспечения защиты прав и свобод человека и гражданина при обработке его ПД, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика определяет общий порядок, принципы и условия обработки персональных данных Оператором и обеспечивает защиту прав субъектов персональных данных при обработке их персональных данных.

Политика действует в отношении всех персональных данных, которые обрабатывает общество с ограниченной ответственностью «Дентал Диагностика» (далее - Оператор, ООО «Дентал Диагностика»).

1.3. Политика распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики.

1.4. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных настоящая Политика публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на сайте Оператора.

2. Термины и принятые сокращения

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

Персональные данные, разрешенные субъектом персональных данных для распространения – это персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

Оператор персональных данных (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.

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 в том числе:

- сбор;

- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (предоставление, доступ);
- распространение;
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

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

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

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному 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.

Защита персональных данных – деятельность, направленная на предотвращение утечки защищаемых персональных данных, несанкционированных и непреднамеренных воздействий на защищаемые персональные данные.

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.

3. Правовое основание обработки персональных данных

3.1. Правовым основанием обработки ПД является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку ПД.

3.2. Оператор обрабатывает ПД на основании:

- Трудового кодекса Российской Федерации;
- Федерального закона «Об основах охраны здоровья граждан в Российской Федерации»

и принятых на его основе нормативно-правовых актов, регулирующих отношения, связанные с оказанием медицинских услуг;

- иных федеральных законов и прочих нормативных правовых актов;
- устава Оператора;
- договоров, заключаемых между Оператором и субъектами ПД;
- согласий на обработку ПД.

4. Порядок и условия обработки и хранение ПД

4.1. Обработка ПД осуществляется после принятия необходимых мер по защите ПД.

4.2. Оператор не вправе обрабатывать ПД субъекта ПД без его письменного согласия, за исключением случаев, предусмотренных статьей 6 Федерального закона «О ПД».

4.3. Равнозначным содержащему собственноручную подпись субъекта ПД согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

4.4. Письменное согласие субъекта ПД должно включать:

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

4.5. Обработка ПД осуществляется Оператором следующими способами:

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

4.6. Оператор организует обработку ПД в следующем порядке:

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

4.7. Оператор при обработке ПД принимает необходимые правовые, организационные и технические меры, в том числе:

- 1) определяет угрозы безопасности ПД при их обработке в информационных системах ПД;
- 2) применяет организационные и технические меры по обеспечению безопасности ПД при их обработке в информационных системах ПД, необходимые для выполнения требований к защите ПД, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПД;
- 3) применяет прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;
- 4) оценивает эффективность принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию информационной системы ПД;
- 5) учитывает машинные носители ПД;
- 6) обнаруживает факты несанкционированного доступа к персональным данным и принимает меры;
- 7) восстанавливает ПД, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
- 8) устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе ПД, а также обеспечивает регистрацию и учет всех действий, совершаемых с ПД в информационной системе ПД

4.8. При обработке ПД оператор выполняет, в частности, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПД.

4.9. В целях обеспечения сохранности и конфиденциальности ПД все операции с ПД должны выполняться только работниками Оператора, осуществляющими данную работу в соответствии с трудовыми обязанностями.

4.10. Оператор получает ПД непосредственно от субъектов ПД или их представителей, наделенных соответствующими полномочиями. Согласия субъекта на получение его ПД от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его ПД третьим лицам получено от него в письменном виде при заключении договора с Оператором, а так же в случаях, установленных федеральным законом.

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

4.12. ПД, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа.

4.13. ПД субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках.

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

4.15. 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.

4.16. Уничтожение ПД.

4.17. Уничтожение документов (носителей), содержащих ПД, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение shreddera.

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

4.19. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей.

4.20. Запрещается хранение документов с ПД и их копий на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода работника из рабочего помещения.

4.21. В электронном виде документы, содержащие ПД, разрешается хранить в специализированных базах данных или в специально отведенных для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.

4.22. При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие ПД, сдаются работником своему непосредственному руководителю.

5. Порядок обработки ПД в информационных системах

5.1. Обработка ПД в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности ПД, определенных с учетом актуальных угроз безопасности ПД и информационных технологий, используемых в информационных системах.

5.2. Обеспечение безопасности при обработке ПД, 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 ПД при их обработке в информационных системах ПД, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

5.3. Уполномоченному работнику, имеющему право осуществлять обработку ПД в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными обязанностями работника.

5.4. Информация может вноситься как в автоматическом режиме при получении ПД 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.

5.5. Обеспечение безопасности ПД, обрабатываемых в информационных системах органов, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

5.6. В случае выявления нарушений порядка обработки ПД уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.

5.7. В состав мер по обеспечению безопасности ПД, реализуемых в рамках системы защиты ПД с учетом актуальных угроз безопасности ПД 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 ПД;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности ПД;
- обеспечение целостности информационной системы и ПД;
- обеспечение доступности ПД;

- 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 ПД, и реагирование на них;
- управление конфигурацией информационной системы и системы защиты ПД.

5.8. Под актуальными угрозами безопасности ПД 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 ПД, а также иные неправомерные действия.

Угрозы первого типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы второго типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы третьего типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности ПД, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О ПД».

5.9. В соответствии с пунктом 11 статьи 19 Федерального закона «О ПД» под уровнем защищенности ПД понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПД при их обработке в информационных системах ПД.

При обработке ПД в информационных системах устанавливаются четыре уровня защищенности ПД.

5.9.1. Необходимость обеспечения первого уровня защищенности ПД при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы первого типа и информационная система обрабатывает либо специальные категории ПД, либо биометрические ПД, либо иные категории ПД;

б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории ПД более чем 100 000 субъектов ПД, не являющихся сотрудниками Оператора.

5.9.2. Необходимость обеспечения второго уровня защищенности ПД при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы первого типа и информационная система обрабатывает общедоступные ПД;

б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории ПД сотрудников Оператора или специальные категории ПД менее чем 100 000 субъектов ПД, не являющихся сотрудниками Оператора;

- в) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает биометрические ПД;
- г) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные ПД более чем 100 000 субъектов ПД, не являющихся сотрудниками Оператора;
- д) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории ПД более чем 100 000 субъектов ПД, не являющихся сотрудниками Оператора;
- е) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории ПД более чем 100 000 субъектов ПД, не являющихся сотрудниками Оператора.

5.9.3. Необходимость обеспечения третьего уровня защищенности ПД при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные ПД сотрудников Оператора или общедоступные ПД менее чем 100 000 субъектов ПД, не являющихся сотрудниками Оператора;
- б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории ПД сотрудников Оператора или иные категории ПД менее чем 100 000 субъектов ПД, не являющихся сотрудниками Оператора;
- в) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории ПД сотрудников Оператора или специальные категории ПД менее чем 100 000 субъектов ПД, не являющихся сотрудниками Оператора;
- г) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает биометрические ПД;
- д) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории ПД более чем 100 000 субъектов ПД, не являющихся сотрудниками Оператора.

5.9.4. Необходимость обеспечения четвертого уровня защищенности ПД при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает общедоступные ПД;
- б) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории ПД сотрудников Оператора или иные категории ПД менее чем 100 000 субъектов ПД, не являющихся сотрудниками Оператора.

5.10. Состав и содержание мер по обеспечению безопасности ПД, необходимых для обеспечения каждого из уровней защищенности ПД, приведены в приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности ПД при их обработке в информационных системах ПД, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

6. Цели обработки персональных данных.

6.1. Оператор обрабатывает ПД в целях:

- оформления трудовых отношений, ведения кадрового делопроизводства, действия в трудоустройстве, обучении, повышении по службе, пользовании различными льготами и гарантиями, обеспечения личной безопасности

работников, контроля количества и качества выполняемой работы и сохранности имущества;

- заключения, исполнения и прекращения гражданско-правовых договоров;
- 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.

6.2. Обработка ПД должна осуществляться на законной и справедливой основе.

6.3. Обработка ПД должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПД, несовместимая с целями сбора ПД.

6.4. Не допускается объединение баз данных, содержащих ПД, обработка которых осуществляется в целях, несовместимых между собой.

6.5. Обработке подлежат только ПД, которые отвечают целям их обработки.

6.6. Содержание и объем обрабатываемых ПД должны соответствовать заявленным целям обработки. Обрабатываемые ПД не должны быть избыточными по отношению к заявленным целям их обработки.

7. Объем и категории обрабатываемых ПД, категории субъектов ПД

7.1. Категории субъектов ПД, чьи данные обрабатываются.

7.1.1. Работники Оператора, бывшие работники, кандидаты на трудоустройство, а также члены семьи работников.

7.1.2. Пациенты, законные представители пациентов.

7.1.3. Прочие клиенты и контрагенты Оператора (физические лица).

7.1.4. Представители/работники клиентов и контрагентов Оператора (юридических лиц).

7.2. В отношении категории, указанной в пункте 7.1.1 (за исключением членов семьи работников), обрабатываются:

- фамилия, имя, отчество;
- дата и место рождения;
- адреса места жительства и регистрации;
- контактный телефон;
- гражданство;
- образование;
- профессия, должность;
- стаж работы;
- семейное положение, наличие детей;
- серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- данные страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- табельный номер;
- сведения о доходах;
- сведения о воинском учете;
- сведения о судимостях;
- сведения о повышении квалификации, о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения о социальных гарантиях;
- сведения о состоянии здоровья, влияющие на выполнение трудовой функции.

7.3. ПД родственников работников обрабатываются в объеме, переданном работником и необходимым для предоставления гарантий и компенсаций работнику, предусмотренных трудовым законодательством:

- фамилия, имя, отчество;
- дата и место рождения;
- серия и номер документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- серия и номер свидетельства о рождении ребенка, сведения о выдаче указанного документа и выдавшем его органе;
- серия и номер свидетельства о заключении брака, сведения о выдаче указанного документа и выдавшем его органе.

7.4. 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 ПД;
- 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.

7.5. В отношении категорий, указанных в пунктах 7.1.3 и 7.1.4, обрабатываются:

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

7.6. В отношении законных представителей или представителей по доверенности указанных лиц обрабатываются:

- фамилия, имя, отчество;
- пол;
- возраст;
- дата и место рождения;
- адреса места жительства и регистрации;
- контактный 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.

8. Защита персональных данных

8.1. В соответствии с требованиями нормативных документов Оператором создана система защиты ПД(СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

8.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

8.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами.

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

8.5. Основными мерами защиты ПД, используемыми Оператором, являются:

8.5.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПД.

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

8.5.3. Разработка политики в отношении обработки ПД.

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

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

8.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

8.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

8.5.8. Соблюдение условий, обеспечивающих сохранность ПД и исключаящих несанкционированный к ним доступ.

8.5.9. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.

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

8.5.11. Обучение работников Оператора, непосредственно осуществляющих обработку ПД, положениям законодательства РФ о ПД, в том числе требованиям к защите ПД, документам, определяющим политику Оператора в отношении обработки ПД, локальным актам по вопросам обработки ПД.

8.5.12. Осуществление внутреннего контроля и аудита.

9. Основные права субъекта персональных данных и обязанности Оператора

9.1. Основные права субъекта ПД.

Субъект имеет право на доступ к его персональным данным и следующим сведениям:

- подтверждение факта обработки ПД Оператором;
- правовые основания и цели обработки ПД;
- цели и применяемые Оператором способы обработки ПД;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПД или которым могут быть раскрыты ПД на основании договора с Оператором или на основании федерального закона;
- сроки обработки ПД, в том числе сроки их хранения;

- порядок осуществления субъектом ПД прав, предусмотренных настоящим Федеральным законом;
- наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- обращение к Оператору и направление ему запросов;
- обжалование действий или бездействия Оператора.

9.2. Обязанности Оператора.

Оператор обязан:

- при сборе ПД предоставить субъекту ПД по его просьбе информацию, касающуюся обработки 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 документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;
- принимать необходимые правовые, организационные и технические меры или 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 уполномоченного органа по защите прав субъектов ПД.

10. Актуализация, исправление, удаление и уничтожение ПД, ответы на запросы субъектов на доступ к персональным данным

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

- подтверждение факта обработки ПД оператором;
- правовые основания и цели обработки ПД;
- цели и применяемые оператором способы обработки ПД;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты ПД на основании договора с Оператором или на основании федерального закона;
- обрабатываемые ПД, относящиеся к соответствующему субъекту ПД, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПД, в том числе сроки их хранения;
- порядок осуществления субъектом ПД прав, предусмотренных Федеральным законом «О ПД»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

10.2. Указанные выше сведения должны быть предоставлены субъекту ПД Оператором в доступной форме и в них не должны содержаться ПД, относящиеся к другим субъектам ПД, за исключением случаев, если имеются законные основания для раскрытия таких ПД.

10.3. Сведения, указанные в пункте 10.1, предоставляются субъекту ПД или его представителю Оператором при обращении либо при получении запроса субъекта ПД или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПД или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПД в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПД Оператором, подпись субъекта ПД или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

10.4. В случае если сведения, указанные в пункте 10.1, а также обрабатываемые ПД были предоставлены для ознакомления субъекту ПД по его запросу, субъект ПД вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 10.1, и ознакомления с такими ПД не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПД.

10.5. Субъект ПД вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 10.1, а также в целях ознакомления с обрабатываемыми ПД до истечения срока, указанного в пункте 10.4, в случае если такие сведения и (или) обрабатываемые ПД не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 10.1, должен содержать обоснование направления повторного запроса.

10.6. Оператор вправе отказать субъекту ПД в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 10.4 и 10.5. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

10.7. Оператор обязан сообщить субъекту ПД или его представителю информацию о наличии ПД, относящихся к соответствующему субъекту ПД, а также предоставить возможность ознакомления с этими ПД при обращении субъекта ПД или его представителя либо в течение 30 дней с даты получения запроса субъекта ПД или его представителя.

10.8. Оператор обязан предоставить безвозмездно субъекту ПД или его представителю возможность ознакомления с ПД, относящимися к этому субъекту ПД.

10.9. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПД или его представителем сведений, подтверждающих, что ПД являются неполными, не точными или неактуальными, Оператор обязан внести в них необходимые изменения.

10.10. В срок, не превышающий семи рабочих дней со дня представления субъектом ПД или его представителем сведений, подтверждающих, что такие ПД являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие ПД.

10.11. Оператор обязан уведомить субъекта ПД или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПД этого субъекта были переданы.

10.12. В случае выявления неправомерной обработки ПД при обращении субъекта ПД или его представителя, либо по запросу субъекта ПД или его представителя, либо уполномоченного органа по защите прав субъектов ПД Оператор

обязан осуществить блокирование неправомерно обрабатываемых ПД, относящихся к этому субъекту ПД, или обеспечить их блокирование (если обработка ПД осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки.

10.13. В случае выявления неточных ПД при обращении субъекта ПД или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПД Оператор обязан осуществить блокирование ПД, относящихся к этому субъекту ПД, или обеспечить их блокирование (если обработка ПД осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПД не нарушает права и законные интересы субъекта ПД или третьих лиц.

10.14. В случае подтверждения факта неточности ПД Оператор на основании сведений, представленных субъектом ПД или его представителем либо уполномоченным органом по защите прав субъектов ПД, или иных необходимых документов обязан уточнить ПД либо обеспечить их уточнение (если обработка ПД осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПД.

10.15. В случае выявления неправомерной обработки ПД, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПД или обеспечить прекращение неправомерной обработки ПД лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки ПД невозможно, Оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки ПД, обязан уничтожить такие ПД или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПД Оператор обязан уведомить субъекта ПД или его представителя, а в случае, если обращение субъекта ПД или его представителя либо запрос уполномоченного органа по защите прав субъектов ПД были направлены уполномоченным органом по защите прав субъектов ПД, также указанный орган.

10.16. В случае достижения цели обработки ПД Оператор обязан прекратить обработку ПД или обеспечить ее прекращение (если обработка ПД осуществляется другим лицом, действующим по поручению Оператора) и уничтожить ПД или обеспечить их уничтожение (если обработка ПД осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПД, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПД, иным соглашением между Оператором и субъектом ПД либо если Оператор не вправе осуществлять обработку ПД без согласия субъекта ПД на основаниях, предусмотренных Федеральным законом «О ПД» или другими федеральными законами.

10.17. В случае отзыва субъектом ПД согласия на обработку его ПД Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПД осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение ПД более не требуется для целей обработки ПД, уничтожить ПД или обеспечить их уничтожение (если обработка ПД осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем

11. Заключительные положения

11.1. Ответственность за нарушение требований законодательства Российской Федерации и нормативных документов ООО «Дентал Диагностика» в области ПД определяется в соответствии с законодательством Российской Федерации.

11.2. Настоящая Политика вступает в силу с момента утверждения и действует бессрочно до принятия новой Политики.

11.3. Все изменения и дополнения к настоящей Политике должны быть утверждены директором ООО «Дентал Диагностика».

Директор

01.02.2023

А.С. Карпов