

ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ сети стоматологических клиник «Гарант»

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с пунктом 2 статьи 18.1 Федерального закона «О персональных данных» № 152-ФЗ от 27 июля 2006 г., а также иными нормативно-правовыми актами Российской Федерации в области защиты и обработки персональных данных.

1.2. Настоящая 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 Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн, поэтому действует в отношении всех персональных данных (далее – ПД), которые Организация (далее – Оператор) может получить от субъекта ПД, являющегося стороной по гражданско-правовому договору, а также от субъекта ПД, состоящего с Оператором в отношениях, регулируемых трудовым законодательством (далее – Работник).

1.2. Оператор обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1.3. Оператор 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 ее размещения на официальном сайте Организации, если иное не предусмотрено новой редакцией Политики.

1.4. Действующая редакция Политики хранится по адресу: 620027, Свердловская обл. г. Екатеринбург, ул. Восточная 8/а; электронная версия Политики – на сайте по адресу: garant.ur.ru

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** – организация, самостоятельно или совместно с другими лицами организующая обработку персональных данных, а также определяющая цели обработки 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 ПД** – 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. Персональные данные, сделанные общедоступными субъектом персональных данных, – ПД, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

2.12. В соответствии с условиями настоящей политики в качестве Оператора выступает сеть стоматологических клиник «Гарант», а именно:

- ООО «ЮДИС» - 620041, г. Екатеринбург, ул. Уральская, д. 65

- ООО «ЮДИС -П» - 620027, г. Екатеринбург, ул. Восточная 8/а - 8 (почтовый адрес: 620041, г. Екатеринбург, ул. Уральская, 65);
- ООО «Гарант – Б» - 620041, г. Екатеринбург, ул. Уральская 65 (почтовый адрес: 620089, г. Екатеринбург ул. Крестинского 55/1);
- ООО «Гарант - Эл» - 620041, г. Екатеринбург, ул. Уральская 65 (почтовый адрес: 620135, г. Екатеринбург, ул. Красных Командиров, 23);
- ООО «Гарант - О» - 620041, г. Екатеринбург, ул. Уральская 65 (почтовый адрес: 620034, г. Екатеринбург ул. Опалихинская, 42);
- ООО «Гарант - Уралмаш» - 620027, г. Екатеринбург, ул. Восточная 8/а – 9 (почтовый адрес: 620042, г. Екатеринбург, ул. Победы 70-6);
- ООО «Гарант - Центр», расположенному по адресу: 620027, г. Екатеринбург, ул. Восточная 8/а - 5 (почтовый адрес: 620026, г. Екатеринбург, ул. Белинского 76 – Народной воли 60);

3. Принципы обеспечения безопасности персональных данных:

3.1. Основной задачей обеспечения безопасности ПД при их обработке 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 Оператор руководствуется следующими принципами:

- законность: защита ПД основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПД;
- системность: обработка ПД Оператором 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 Оператором в информационных системах и других 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 и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПД, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПД осуществляется Оператором на основании результатов анализа практики обработки ПД с учетом выявления новых способов и средств реализации угроз безопасности ПД;
- 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 Оператора, 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 Оператора предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или 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) и 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. Оператор не осуществляет обработку ПД, несовместимую с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПД, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, Оператор уничтожает или обезличивает ПД;

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

4. Обработка персональных данных

4.1. Правила получения ПД:

4.1.1. Все ПД следует получать от самого субъекта. Если ПД субъекта можно получить только у 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 способах 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:

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

4.2. Правила и условия обработки 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 и выполнения, возложенных законодательством РФ 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).

4.2.2. Цели обработки персональных данных:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011г № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

4.2.3. Категории субъектов ПД, в отношении которых со стороны Оператора производится обработка ПД следующих субъектов ПД:

- физические лица, состоящие с Обществом в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников Общества;
- физические лица, уволившиеся из Общества;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с Обществом в гражданско-правовых отношениях;
- физические лица, обратившиеся к оператору с целью получения медицинской помощи или с целью прохождения диагностического исследования.

4.2.4. ПД, обрабатываемые Оператором:

- данные, полученные при осуществлении трудовых отношений;
- данные, полученные для осуществления отбора кандидатов на работу;
- данные, полученные при осуществлении гражданско-правовых отношений;
- данные, полученные при оказании медицинской помощи неограниченному кругу лиц.

4.2.5. Обработка персональных данных ведется:

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

4.3. Правила хранения ПД:

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

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

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

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

4.3.5. 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.

4.4. Условия уничтожения ПД:

4.4.1. 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.

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

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

4.5. Условия передачи ПД третьим лицам:

4.5.1. Оператор передает ПД третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена действующим законодательством РФ в рамках установленной законодательством процедуры.

4.5.2. Перечень третьих лиц, которым передаются ПД оператором:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Инспекция ФНС (на законных основаниях);
- Фонд социального страхования РФ (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- Страховые медицинские организации добровольного медицинского страхования (на законных основаниях);
- Финансово-кредитные организации (банки) для начисления заработной платы (на основании договора);
- Судебные и правоохранительные органы России в случаях, установленных законодательством.

5. Защита персональных данных

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

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

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

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

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

5.5.1. 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.

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

5.5.3. Разработка политики в отношении обработки персональных данных.

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

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

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

5.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами, что обеспечивает защиту информации от несанкционированного доступа;

5.5.8. Установление правил доступа к обрабатываемым ПД, обеспечение регистрации и учета действий, совершаемых с ПД, а также обнаружение фактов несанкционированного доступа к ПД и принятия мер;

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

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

5.5.11. Осуществление внутреннего контроля и аудита.

6. Основные права субъекта ПД и обязанности Оператора

6.1. Основные права субъекта ПД:

Субъект ПД имеет право на получение информации, касающейся обработки его персональных данных, 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 ПД или которым могут быть раскрыты ПД на основании договора с Оператором или на основании федерального закона;
- перечень обрабатываемых ПД, относящиеся к соответствующему субъекту ПД; источник их получения, если иной порядок представления таких данных не предусмотрен действующим законодательством;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом ПД прав, предусмотренных действующим законодательством РФ;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 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.

Субъект ПД вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Обязанности Оператора:

Оператор обязан:

- при сборе ПД предоставить информацию об обработке 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.