



УТВЕРЖДАЮ

Директор

А.Б. Романов

2013

**Политика ООО «Медицинская клиника «Онегомед»
в отношении обработки персональных данных
и сведения о реализуемых требованиях к защите персональных данных**

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика обработки персональных данных в «Медицинская клиника «Онегомед» (далее – Политика) разработана в соответствии с требованиями нормативных правовых актов Российской Федерации, регулирующих процессы обработки персональных данных. Политика определяет принципы обработки (сбора, хранения, передачи, уничтожения) и защиты персональных данных клиентов и работников ООО «Медицинская клиника «Онегомед» (далее – субъекты персональных данных) в ООО «Медицинская клиника «Онегомед» (далее – Общество).

Действие настоящей Политики распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению, использованию, передаче (предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению персональных данных, осуществляемые как с использованием средств автоматизации, так и без использования таких средств.

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Принципы и цели обработки персональных данных

Обработка персональных данных в Обществе должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Обработка персональных данных осуществляется на основе принципов:

- обработка на законной и справедливой основе;
- соблюдение законов и иных нормативных правовых актов, регламентирующих процессы обработки персональных данных;
- осуществление обработки персональных данных с согласия субъекта персональных данных на обработку его персональных данных, за исключением случаев, предусмотренных федеральным законом;
- ограничение обработки персональных данных достижением конкретных, заранее определенных и законных целей;

- недопущение обработки персональных данных, несовместимой с целями сбора персональных данных;
- недопущение объединения баз данных, содержащих персональных данных, обработка которых осуществляется в целях, несовместимых между собой;
- ограничение избыточности обрабатываемых персональных данных заявленным целям обработки;
- обеспечение точности и достаточности, актуальности персональных данных по отношению к заявленным целям их обработки.
- строгое выполнение требований по обеспечению безопасности персональных данных и сведений, составляющих врачебную тайну;
- обязательное удаление или уточнение неполных или неточных данных;
- хранение персональных данных в формах, позволяющих определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- уничтожение или обезличивание персональные данные по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- информирование граждан в доступной форме, в том числе с использованием сети Интернет, об осуществляемой медицинской деятельности и о медицинских работниках, об уровне их образования и об их квалификации;
- осуществление прямых контактов с пациентами с помощью средств связи только при условии предварительного оформления согласия пациента.

Обработка персональных данных в Обществе осуществляется исключительно в следующих целях:

- исполнение обязательств по договору, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- заключение и исполнение иных договоров с контрагентами;
- обеспечение исполнения обязанностей в сфере функционирования ЕГИСЗ;
- выполнение обязанностей, предусмотренных трудовым законодательством, содействие работникам в обучении и продвижении по карьере;
- обеспечение личной безопасности работников, контроль количества и качества выполняемой работы;
- обеспечение сохранности имущества Общества;
- проведение маркетинговых исследований;
- оказание услуг центра обработки вызовов;

- продвижение услуг путем осуществления прямых контактов с клиентами с помощью средств связи, направления рекламно-информационных сообщений;
- обеспечение функционирования сайта onegomed.ru;
- осуществление других видов хозяйственной деятельности, не противоречащей законодательству Российской Федерации.

2.2. Сбор персональных данных

Сбор, накопление, хранение, изменение, использование и передача персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, когда в соответствии с действующим законодательством допускается обработка персональных данных без получения согласия субъекта персональных данных, а именно:

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для осуществления прав и законных интересов Общества или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с действующим законодательством.

2.3. Хранение персональных данных

Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют соответствующие цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки, или в случае утраты необходимости в достижении этих целей.

Персональные данные субъектов могут обрабатываться как на бумажных носителях, так и в электронном виде.

2.4. Передача персональных данных третьим лицам

Общество вправе поручить обработку персональных данных третьему лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. При этом Общество в договоре обязует третье лицо, осуществляющее обработку персональных данных по поручению Общества, соблюдать принципы и правила обработки персональных данных, предусмотренные федеральным законом № 152-ФЗ «О персональных данных» и другими нормативными правовыми актами, регламентирующими процессы обработки персональных данных.

В случае если Общество поручает обработку персональных данных третьему лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Общество. Лицо, осуществляющее обработку персональных данных по поручению Общества, несет ответственность перед Обществом.

Общество обязуется и обязует третьих лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законом.

2.5. Уничтожение персональных данных

В случае достижения целей обработки персональных данных – Общество прекращает обработку персональных данных и уничтожает персональные данные, в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено соглашением между Обществом и субъектом персональных данных.

В случае обращения субъекта персональных данных с заявлением об уничтожении его персональных данных, Общество обязано прекратить обработку или обеспечить прекращение обработки персональных данных данного субъекта и уничтожить указанные в заявлении персональные данные.

Уничтожение персональных данных производится в соответствии с внутренними процессами Общества.

2.6. Защита персональных данных (сведения о реализуемых требованиях к защите персональных данных)

При обработке персональных данных Общество принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИС);
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИС, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИС;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием необходимых мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемых в ИС, а также обеспечением регистрации доступа к персональным данным в ИС;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИС;

- в том числе другими способами.

В Обществе в соответствии с действующим законодательством Российской Федерации разработан и введен в действие комплекс организационно-распорядительных и функциональных мер, регламентирующих и обеспечивающих безопасность обрабатываемых персональных данных:

- назначены ответственные лица за организацию и обеспечение безопасности персональных данных;
- обеспечена защита помещений, в которых осуществляется обработка и хранение носителей персональных данных;
- установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
- определен круг лиц, имеющих право обработки персональных данных, разработаны инструкции пользователям по защите персональных данных, антивирусной защите, действиям в кризисных ситуациях;
- определены требования к персоналу, степень ответственности работников за обеспечение безопасности персональных данных;
- проведено ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации по обеспечению безопасности персональных данных и требованиями к защите персональных данных, документами, определяющими политику Общества в отношении обработки персональных данных, и другими локальными актами по вопросам обработки персональных данных; проводится периодическое обучение работников, осуществляющих обработку персональных данных, правилам обработки персональных данных;
- осуществляется контроль за соблюдением работниками, допущенных к обработке персональных данных, требований, установленных законодательством РФ в области персональных данных, локальными нормативными актами.

Общество предпринимает необходимые и достаточные технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий:

- введена система разграничения доступа работников к информации, содержащей персональные данные субъектов персональных данных, в соответствии с их должностными (функциональными) обязанностями;
- установлена защита от несанкционированного доступа к автоматизированным рабочим местам, информационным сетям и базам персональных данных;
- установлена защита от вредоносного программно-математического воздействия (воздействия на компьютерные системы с помощью вредоносных программ); осуществляется регулярное резервное копирование информации и баз данных, содержащих персональные данные субъектов персональных данных;
- передача информации с использованием информационно-телекоммуникационных сетей осуществляется по защищенным каналам;
- организована система контроля за порядком обработки персональных данных и обеспечения их безопасности;

- проводятся регулярные проверки соответствия системы защиты персональных данных, уровня защищенности персональных данных в информационных системах персональных данных, функционирования средств защиты информации, выявления изменений в режиме обработки и защиты персональных данных.

2.7. Правовые основания обработки персональных данных

Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Общество осуществляет обработку персональных данных:

- статья 13 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- статьями 86 – 90 Трудового кодекса Российской Федерации от 30.12.2001 N 197-ФЗ;
- уставные документы Общества;
- договоры, заключаемые между Обществом и субъектом персональных данных;
- согласие на обработку персональных данных.

2.8. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

К категориям субъектов персональных данных могут быть отнесены:

- представители/работники клиентов и контрагентов Общества (юридических лиц);
- клиенты и контрагенты Общества;
- работники Общества.

В рамках категорий субъектов и применительно к конкретным целям случаи обработки специальных и биометрических персональных данных:

- специальные категории персональных данных – сведения о состоянии здоровья;
- биометрические персональные данные - фотографии сотрудников, в некоторых случаях – фотографии клиентов (пациентов) Общества.

2.9. Порядок и условия обработки персональных данных

Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача, обезличивание, удаление, блокирование, уничтожение.

Обработка вышеуказанных персональных данных может осуществляться путем смешанной обработки с передачей по внутренней сети юридического лица с передачей по

сети Интернет.

Передача персональных данных третьим лицам осуществляется только на основании договора, условием которого является обязанность обеспечения третьим лицом безопасности персональных данных при их обработке (в том числе конфиденциальности персональных данных), а также меры, предусмотренные ч. 2 ст. 18.1, ч. 1 ст. 19 Федерального закона «О персональных данных».

Условия прекращения обработки персональных данных:

- достижение целей обработки персональных данных;
- истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных;
- реорганизация или ликвидация Общества.
- Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

При осуществлении хранения персональных данных Общество использует базы данных, находящиеся на территории Российской Федерации, в соответствии с ч. 5 ст. 18 Федерального закона "О персональных данных".

2.10. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональные данные подлежат их актуализации (исправлению) Обществом.

При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

Общество обязано сообщить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу последнего.

3. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

Общество обеспечивает конфиденциальность персональных данных, то есть не допускает их распространения без согласия субъекта персональных данных или наличия иного законного основания. Обеспечение конфиденциальности обезличенных и общедоступных персональных данных осуществляется аналогично обеспечению конфиденциальности иных данных, обрабатываемых в Обществе.

3.1. Организация доступа к информации, содержащей персональные данные.

Доступ к персональным данным предоставляется только тем работникам Общества, которым он необходим для исполнения их непосредственных должностных обязанностей.

Допуск работников Общества к обработке персональных данных осуществляется на основании утвержденного Перечня должностей работников, допущенных к обработке персональных данных, обрабатываемых в Обществе. Работник Общества допускается к обработке персональных данных только в случае выполнения своих трудовых обязанностей.

Работник Общества допускается к обработке персональных данных только после ознакомления с действующими нормативными правовыми актами, регламентирующими обработку персональных данных, локальными нормативными актами Общества, регламентирующими обработку персональных данных.

3.2. Организация доступа субъектов персональных данных к своим персональным данным

Общество обеспечивает доступ субъектов персональных данных к принадлежащим им персональным данным. Для получения такого доступа субъекту персональных данных необходимо направить в Общество письменный запрос по форме, приведенной в Приложении № 1. Общество осуществляет предоставление персональных данных обратившегося субъекта в доступной для субъекта форме.

В соответствии с Федеральным законом № 152-ФЗ «О персональных данных» субъект персональных данных имеет право:

- Получить сведения касающиеся обработки персональных данных Обществом, а именно:
- Потребовать от Общества уточнения его персональных данных, их блокирования или уничтожения в случае, если персональных данных являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- Отозвать согласие на обработку персональных данных в предусмотренных действующим законодательством случаях.

4. ОТВЕТСТВЕННОСТЬ

Работники Общества, виновные в нарушении нормативных правовых актов и локальных нормативных актов Общества, регулирующих процессы обработки и защиты персональных данных, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой, административной, уголовной ответственности в порядке, установленном действующим законодательством.