|  |  |
| --- | --- |
|  | Приложение № 1 |
|  | к Приказу № 57 |
|  | От « 21» июля\_\_ 2023 г. |

**ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

в АО «Центр семейной медицины»

2023 г.

1. **Назначение и область действия**
	1. Настоящий документ (далее – Политика) определяет цели и общие принципы обработки персональных данных, а также реализуемые меры защиты персональных данных
	в АО «Центр семейной медицины» (далее – организация). Политика является общедоступным документом и предусматривает возможность ознакомления с ней любых лиц.
	2. Политика действует бессрочно после утверждения и до ее замены новой версией.
	3. В Политике используются термины и определения в соответствии с их значениями,
	как они определены Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».
	4. Политика распространяется на всех сотрудников организации и все структурные подразделения.
	5. Требования Политики также учитываются и предъявляются в отношении иных лиц при необходимости их участия в процессе обработки персональных данных, а также в случаях передачи им в установленном порядке персональных данных на основании соглашений, договоров, поручений на обработку.
2. **Сведения об обработке персональных данных**
	1. Обработка персональных данных в организации ведется смешанным способом:
	с использованием средств автоматизации и без их использования.
	2. Возможные действия с персональными данными включают сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение.
	3. Обработка персональных данных осуществляется на законной и справедливой основе, правовыми основания для обработки являются:

 - федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью оператора;

 - уставные документы оператора;

 - договоры, заключаемые между оператором и субъектом персональных данных;

 - согласие на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям оператора).

* 1. Содержание и объем обрабатываемых персональных данных определяются исходя из целей обработки. Не обрабатываются персональные данные, избыточные или несовместимые
	по отношению к следующим основным целям:
* выполнения требований трудового законодательства РФ в части ведения кадрового учета, заключение трудовых и иных договоров, ведение личных дел, ведение воинского учета, ведение бухгалтерского учета, осуществления пропускного режима;
* обеспечение соблюдения законов и иных нормативных правовых актов, установление медицинского диагноза и оказания медицинских услуг пациенту.
	1. К основным категориям субъектов персональных данных относятся:
* физические лица, состоящие в отношениях с организацией;
* физические лица, состоящие в отношениях с контрагентами организации;
* кандидаты на замещение вакантных должностей.
	1. Для указанных категорий субъектов могут обрабатываться: фамилия, имя, отчество; год, месяц, дата рождения; место рождения, адрес; семейное положение; паспортные данные, социальное положение; имущественное положение; сведения об образовании; сведения о квалификации; сведения о наличии/отсутствии судимости; доходы; ИНН, СНИЛС, контактная информация, иные сведения, предусмотренные типовыми формами и установленным порядком обработки.
	2. При обработке обеспечиваются точность персональных данных, их достаточность
	и актуальность по отношению к целям обработки персональных данных. При обнаружении неточных или неполных персональных данных производится их уточнение и актуализация.
	3. Для персональных данных, не являющихся общедоступными, обеспечивается конфиденциальность.
	4. Обработка и хранение персональных данных осуществляются не дольше, чем этого требуют цели обработки персональных данных, если отсутствуют законные основания для дальнейшей обработки, например, если федеральным законом или согласием с субъектом персональных данных не установлен соответствующий срок хранения. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию при наступлении следующий условий:
* достижение целей обработки персональных данных или максимальных сроков хранения – в течение 30 дней;
* утрата необходимости в достижении целей обработки персональных данных –
в течение 30 дней;
* предоставление субъектом персональных данных или его законным представителем подтверждения того, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки – в течение 7 дней;
* невозможность обеспечения правомерности обработки персональных данных –
в течение 10 дней;
* отзыв субъектом персональных данных согласия на обработку персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных – в течение 30 дней;
* отзыв субъектом персональных данных согласия на использование персональных данных для контактов с потенциальными потребителями при продвижении товаров
и услуг – в течение 2 дней;
* истечение сроков исковой давности для правоотношений, в рамках которых осуществляется либо осуществлялась обработка персональных данных;
* ликвидация (реорганизация) оператора.
	1. Обработка персональных данных на основании договоров и иных соглашений
	организации, поручений на обработку персональных данных осуществляется в соответствии
	с условиями этих договоров, соглашений, а также соглашений с лицами, которым поручена обработка или которые поручили обработку на законных основаниях. Такие соглашения могут определять, в частности:
* цели, условия, сроки обработки персональных данных;
* обязательства сторон, в том числе меры по обеспечению конфиденциальности;
* права, обязанности и ответственность сторон, касающиеся обработки персональных данных.
	1. В случаях, не предусмотренных явно действующим законодательством или договором, обработка осуществляется после получения согласия субъекта персональных данных. Согласие может быть выражено в форме совершения действий, принятия условий договора-оферты, проставления соответствующих отметок, заполнения полей в формах, бланках, или оформлено в письменной форме в соответствии с законодательством. Обязательным случаем получения предварительного согласия является, например, контакт с потенциальным потребителем при продвижении товаров и услуг организации на рынке.
	2. Организация должна быть зарегистрирована в реестре уполномоченного органа
	по защите прав субъектов персональных данных. В реестре указаны сведения об операторе,
	в том числе: полное наименование, контактная информация для обращений, сведения
	об обработке персональных данных и мерах по обеспечению безопасности.
1. **Меры по обеспечению безопасности персональных данных**
	1. Организация предпринимает необходимые правовые, организационные и технические меры для обеспечения безопасности персональных данных для их защиты от несанкционированного (в том числе, случайного) доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий. К таким мерам, в частности, относятся:
* назначение сотрудников, ответственных за организацию обработки и обеспечение безопасности персональных данных;
* проверка наличия в договорах и включение при необходимости в договоры пунктов
об обеспечении конфиденциальности персональных данных;
* издание локальных актов по вопросам обработки персональных данных, ознакомление с ними работников, обучение пользователей;
* обеспечение физической безопасности помещений и средств обработки, пропускной режим, охрана, видеонаблюдение;
* ограничение и разграничение доступа сотрудников и иных лиц к персональным данным и средствам обработки, мониторинг действий с персональными данными;
* определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;
* применение средств обеспечения безопасности (антивирусных средств, межсетевых экранов, средств защиты от несанкционированного доступа, средств криптографической защиты информации), в том числе прошедших процедуру оценки соответствия в установленном порядке;
* учёт и хранение носителей информации, исключающее их хищение, подмену, несанкционированное копирование и уничтожение;
* резервное копирование информации для возможности восстановления;
* осуществление внутреннего контроля за соблюдением установленного порядка, проверка эффективности принятых мер, реагирование на инциденты.
1. **Права субъектов персональных данных**
	1. Субъект персональных данных имеет право отозвать согласие на обработку персональных данных, направив соответствующий запрос в организацию по почте или обратившись лично.
	2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
* подтверждение факта обработки персональных данных организацией;
* правовые основания и цели обработки персональных данных;
* цели и применяемые организацией способы обработки персональных данных;
* наименование и место нахождения организации, сведения о лицах за исключением сотрудников/работников, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с организацией
или на основании федерального закона;
* обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
* сроки обработки персональных данных, в том числе сроки их хранения; порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
* информацию об осуществленной или о предполагаемой трансграничной передаче данных;
* наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению организации, если обработка поручена или будет поручена такому лицу;
* иные сведения, предусмотренные федеральными законами.
	1. Субъект персональных данных вправе требовать от организации 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.
	2. Если субъект персональных данных считает, что организация осуществляет обработку его персональных данных с нарушением требований законодательства, или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие организации в уполномоченном органе по защите прав субъектов персональных данных (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций – Роскомнадзор) или в судебном порядке.
	3. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда
	в судебном порядке.
1. **Роли и ответственность**
	1. Права и обязанности организацией определяются действующим законодательством
	и соглашениями организации.
	2. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных в организации.
	3. Ответственность лиц, участвующих в обработке персональных данных на основании поручений организации, за неправомерное использование персональных данных устанавливается в соответствии с условиями заключенного между организацией и контрагентом гражданско-правового договора или соглашения о конфиденциальности информации.
	4. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами, локальными актами, соглашениями организации.
	5. Политика разрабатывается ответственным за организацию обработки персональных данных и вводится в действие после утверждения руководителем организации. Политика пересматривается ежегодно для поддержания в актуальном состоянии и актуализируется по мере необходимости.