**ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ**

УТВЕРЖДЕНО
приказом главного врача
КОГБУЗ «Кировский областной СПИД-центр»
№61 от «07» марта 2013 г.

**Политика КОГБУЗ «Кировский областной СПИД-центр»
в отношении обработки персональных данных**

**Общие положения**

Настоящая Политика разработана во исполнение требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее 152-ФЗ), определяет основные понятия, направления деятельности КОГБУЗ «Кировский областной СПИД-центр», необходимые для обеспечения единообразия взглядов на обработку персональных данных и их защиты.

Содержание Политики не затрагивает последовательность действий и процедуры обработки персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Персональные данные являются конфиденциальной, строго охраняемой информацией и на них распространяются все требования, установленные внутренними документами КОГБУЗ «Кировский областной СПИД-центр» в области защиты персональных данных и конфиденциальной информации.

**Основные понятия и определения**

В целях соблюдения настоящей Политики применяются следующие понятия:

**персональные данные**– любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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), 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;

**автоматизированная обработка персональных данных**– обработка персональных данных с помощью средств вычислительной техники;

**распространение персональных данных**– действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

**предоставление персональных данных**– действия, направленные на раскрытие персональных данных определенному лицу или определенному 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.

**Обработка персональных данных**

В зависимости от субъекта персональных данных Учреждение обрабатывает персональные данные следующих категорий субъектов персональных данных:

* персональные данные работника Учреждения;
* персональные данные, полученные из общедоступных источников;
* персональные данные лиц, давших согласие на обработку персональных данных, во исполнение заключенных договоров или с целью их заключения, а также в иных целях в соответствии с требованиями законодательства Российской федерации

Учреждение применяет процедуры обработки персональных данных в соответствии с технологическим процессом обработки информации и обеспечивает соответствующий уровень их защиты, предоставляет находящиеся в его распоряжении персональные данные третьим лицам только в установленных законодательством Российской Федерации случаях.

**Цели обработки**

Обработка персональных данных в Учреждении осуществляется для следующих целей:

* оказание специализированной медицинской помощи гражданам Кировской области, больным ВИЧ-инфекцией, а также организация и проведение мероприятий по предупреждению распространения ВИЧ-инфекции и инфекционных заболеваний среди населения;
* оказание социальных услуг;
* ведение кадрового делопроизводства;
* заключение договоров гражданско-правового характера;
* ведение бухгалтерского учета по начислению заработной платы;
* оказания психологической помощи.

**Принципы обработки**

Учреждение предпринимает все возможные меры для обеспечения законности обработки персональных данных и стремится к обеспечению необходимого уровня безопасности их обработки.

Обработка персональных данных в Учреждении строится на принципах:

* законности – обработка персональных данных должна осуществляться на законной основе;
* конкретности – обработка персональных данных должна ограничиваться достижением конкретных, заранее оговоренных целей;
* точности – при обработке персональных данных должна быть обеспечена их точность и актуальность;
* конфиденциальности – к обработке персональных данных допускаются только специально назначенные лица и осуществляются меры по недопущению несанкционированной передачи и (или) распространения персональных данных;
* персональной ответственности – специально назначенные должностные лица несут ответственность за соблюдение принципов обработки и выполнение установленных процедур;
* достаточности – содержание и объем используемых персональных данных должны соответствовать целям их обработки;
* разграничения доступа – содержание баз персональных данных и доступ к ним должностных лиц должны соответствовать целям обработки и обязанностям должностных лиц.

**Права и обязанности**

**Права и обязанности Учреждения**

Учреждение как оператор персональных данных, вправе:

* отстаивать свои интересы в суде;
* предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
* отказывать в предоставлении персональных данных в случаях предусмотренных законодательством;
* использовать персональные данные субъекта без его согласия, в случаях предусмотренных законодательством.

**Права и обязанности субъекта персональных данных**

Субъект персональных данных имеет право:

* дать согласие на обработку своих персональных данных, в том числе на трансграничную передачу его персональных данных;
* в любое время отозвать свое согласие на обработку персональных, в том числе на трансграничную передачу его персональных данных;
* требовать 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;
* требовать перечень своих персональных данных, обрабатываемых Учреждения и источник их получения;
* получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;
* требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
* обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;
* на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

**Основы обеспечения безопасности персональных данных**

Учреждение предполагает достичь снижения вероятности реализации угроз безопасности персональных данных за счет проведения сбалансированной организационной и технической политики.

Организационные мероприятия по обеспечению безопасности персональных данных основываются:

* на установлении персональной ответственности должностных лиц Учреждения за соблюдение установленных правил и процедур обработки персональных данных;
* на доведении до должностных лиц Учреждения установленных правил и процедур обработки персональных данных;
* на разграничении доступа должностных лиц Учреждения к персональным данным;
* на регламентации деятельности должностных лиц Учреждения при обработке персональных данных;
* на учете материальных носителей персональных данных;
* на обеспечении физической защиты помещений, в которых обрабатываются или хранятся материальные носители персональных данных, и на ограничении доступа в эти помещения;
* на назначении лица, ответственного за организацию работ и координацию мероприятий по обработке персональных данных;
* на организации проверки наличия материальных носителей персональных данных и выполнения установленных правил обработки персональных данных;
* на своевременном уничтожении материальных носителей персональных данных, надобность в которых миновала, за исключением архивных материалов;
* на периодическом контроле достаточности принимаемых организационных мер для обеспечения безопасности персональных данных.

Технические мероприятия по обеспечению безопасности персональных данных основываются:

* на определении угроз безопасности персональных данных и определении необходимых мер защиты при их обработке в информационной системе персональных данных;
* на учете машинных носителей информации;
* на применении технических мер по обеспечению безопасности персональных данных, установленных законодательством Российской Федерации, и оценке их эффективности;
* на применении средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в информационной системе персональных данных и в других средствах автоматизации;
* на установлении правил доступа к персональным данным и их обработки в информационной системе персональных данных;
* на использовании только лицензионного программного обеспечения в информационной системе персональных данных и в других средствах автоматизации;
* на назначении должностного лица, ответственного за проведение технической политики обеспечения безопасности персональных данных;
* на использовании процедур регистрации и учета всех действий, совершаемых в информационной системе персональных данных;
* на использовании процедур восстановления персональных данных, измененных или уничтоженных в информационной системе персональных данных;
* на своевременном уничтожении пришедших в негодность машинных носителей информации;
* на своевременном уничтожении (обезличивании) персональных данных, цели обработки которых достигнуты;
* на периодическом контроле достаточности принимаемых технических мер для обеспечения безопасности персональных данных.

**Заключительные положения**

Настоящая Политика действует с момента её утверждения и официального опубликования.

Настоящая Политика является внутренним документом Учреждения, общедоступной и подлежит размещению на официальном сайте Учреждения.

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

Подготовка предложений по внесению изменений в настоящую Политику возлагается на ответственного за организацию обработки персональных данных в Учреждении.

Ответственность должностных лиц Учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Учреждения.