

Политика

обработки и защиты персональных данных

Общие положения

- 1) Настоящий документ (далее – Политика) определяет политику ОГБУЗ ГБ г. Костромы (далее – Организация) в отношении обработки персональных данных, содержащихся в информационных системах персональных данных и на бумажных носителях.
- 2) Настоящая Политика разработана в соответствии с Конституцией Российской Федерации, Федеральными законами Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» и иными нормативно-правовыми актами в сфере защиты информации и персональных данных в частности.
- 3) Настоящая Политика, все дополнения и изменения к ней утверждаются руководителем Организации.

Основные понятия, используемые в настоящей Политике

- 1) **Персональные данные** (далее – ПДн) - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных). Все ПДн, обрабатываемые в Организации закреплены в «**Перечне ПДн, обрабатываемых в Организации**».
- 2) **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации (или без использования таких средств) с ПДн, включая:
 - Сбор;
 - Запись;
 - Систематизацию;
 - Накопление;
 - Хранение;
 - Уточнение (обновление, изменение);
 - Извлечение;
 - Использование;
 - Передачу (распространение, предоставление, доступ);
 - Обезличивание;
 - Блокирование;

- Удаление;
 - Уничтожение.
- 3) **Информационная система персональных данных (далее – ИСПДн)** – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.
- 4) **Бумажные носители ПДн** – документы или иные физические формы выражения, на которых с помощью символов закрепляются ПДн.

Цель обработки ПДн

- 1) Основные цели:
- Выполнение требований законодательства в сфере здравоохранения;
 - Оказание специализированной, амбулаторно-поликлинической, стационарной помощи населению;
 - Выполнение уставных задач.
- 2) Детальные цели обработки для каждой группы субъектов ПДн Организации закрепляются в **«Перечне ПДн, обрабатываемых в Организации»**.

Принципы обработки ПДн

Обработка ПДн осуществляется Организацией на основе принципов:

- Обработка ПДн осуществляется на законной и справедливой основе;
- Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;
- Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- Содержание и объем обрабатываемых ПДн соответствуют целям обработки и обрабатываемые ПДн не избыточны по отношению к заявленным целям их обработки;
- При обработке ПДн обеспечивается точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Организация принимает необходимые меры по удалению или уточнению неполных, или неточных данных;
- Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или

поручителем, по которому является субъект ПДн (пункт 7 статьи 5 главы 2 Федерального закона № 152-ФЗ).

- Обрабатываемые ПДн уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Условия обработки ПДн

- 1) Обработка ПДн осуществляется на законной основе.
- 2) Условия обработки ПДн соответствуют требованиям статьи 6 Федерального закона № 152-ФЗ.
- 3) Правила обработки ПДн Организации закреплены в **«Правилах безопасной обработки персональных данных ОГБУЗ ГБ г. Кострома»**

Права субъектов ПДн

Субъекты ПДн, чьи ПДн обрабатываются в ИСПДн, имеют право на получение информации, касающейся обработки их ПДн, в том числе содержащей:

- Подтверждение факта обработки ПДн Организацией;
- Правовые основания и цели обработки ПДн;
- Цели и применяемые Организацией способы обработки ПДн;
- Наименование и место нахождения Организации, сведения о лицах (за исключением работников Организации), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Организацией или на основании федеральных законов Российской Федерации;
- Обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральными законами Российской Федерации;
- Сроки обработки ПДн, в том числе сроки их хранения;
- Иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами;
- Субъекты ПДн вправе требовать от Организации уточнения их ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленных целей обработки, а также принимать предусмотренные законом меры по защите своих прав;

- Субъекты ПДн вправе обжаловать действия или бездействие Организации в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке;
- Субъекты ПДн имеют право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Реализация требований к защите ПДн

1) Реализация требований к защите ПДн в Организации осуществляется в соответствии с Приказом ФСТЭК от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2) Реализация требований к защите ПДн в Организации включает в себя проведение следующих мероприятий:

- определение категории ПДн, обрабатываемых в ИСПДн;
- определение угроз безопасности ПДн;
- определение необходимого уровня защищенности ПДн на основе анализа угроз безопасности и возможного ущерба Организации при реализации угроз безопасности ПДн.

- Реализация технических и организационных мер по защите ПДн, обрабатываемых в ИСПДн, на основе требований постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и требований Приказа ФСТЭК от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

- Иные мероприятия в соответствии с законодательством РФ и последующие законные меры, которые будут приниматься для актуализации процесса обеспечения безопасности ПДн.

Заключительные положения

1) Настоящая Политика является внутренним документом Организации, общедоступной и подлежит размещению на официальном сайте Организации.

- 2) Настоящая Политика подлежит изменению, дополнению в случае необходимости либо принятия новых законодательных актов и специальных нормативных документов по обработке и защите ПДн.
- 3) Сотрудники Организации несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Политикой, в пределах, определенных действующим законодательством Российской Федерации.