

**ПОЛИТИКА
КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
БЮДЖЕТНОГО УЧРЕЖДЕНИЯ
ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА — ЮГРЫ
«УРАЙСКАЯ ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА»
(вторая редакция)**

1. Общие положения

Настоящая политика конфиденциальности персональных данных (далее - Политика) разработана в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных» (далее - Закон о ПДн) и является основополагающим внутренним регулятивным документом бюджетного учреждения Ханты-Мансийского автономного округа — Югры «Урайская городская клиническая больница» (далее — Учреждение или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Учреждение.

Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Учреждении, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Учреждением как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

Если в отношениях с Учреждением участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Учреждение становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние регулятивные документы Учреждения распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних регулятивных документах прямо не упоминаются, но фактически участвуют в правоотношениях с Учреждением.

Учреждение 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 её размещения на официальном сайте Учреждения, если иное не предусмотрено новой редакцией Политики.

Действующая редакция хранится на месте нахождения Учреждения по адресу: г. Урай, ул. Пионеров, д. 1; электронная версия Политики - на официальном сайте Учреждения по адресу: www.uraycgb.ru.

2. Информация об Операторе

Наименование организации: бюджетное учреждение Ханты-Мансийского автономного округа – Югры «Урайская городская клиническая больница».

ОГРН: 1028601392335.

Руководитель: главный врач.

Адрес: 628285, Ханты-Мансийский автономный округ – Югра, г. Урай, ул. Пионеров, д.1.

Тел., факс: 8 (34676) 9-13-12.

Адрес электронной почты: odo@uraycgb.ru.

3. Термины и принятые сокращения

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Защищаемая информация - информация, подлежащая защите в соответствии с требованиями нормативных документов в области безопасности информации или требованиями, устанавливаемыми собственником информации.

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.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определённому лицу или определённому 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.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Информационная система персональных данных (ИСПД) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Нарушитель безопасности - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при её обработке техническими средствами в информационных системах.

Угроза безопасности информации - некая совокупность факторов и условий, которая создает опасность в отношении защищаемой информации.

Правила разграничения доступа - совокупность правил,, регламентирующих порядок и условия доступа субъектов доступа (сотрудников, программ) к объектам доступа (информации, её носителям, процессам и другим ресурсам).

Несанкционированный доступ (несанкционированные действия, НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Контролируемая зона - это территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

Дополнительные устройства обмена информацией - портативные жесткие диски, съемные флэш-носители, CD, DVD - диски.

Пациент - физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

4. Правовые основания обработки ПДн

Обработка ПДн в Учреждении осуществляется в связи с выполнением Учреждением функций, предусмотренных её учредительными документами, и определяемых:

- Федеральным законом от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи";
- Трудовым кодексом Российской Федерации (Федеральный закон от 30.12.2001 № 197-ФЗ, ст. 85-90);
- Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации. Кроме того, обработка ПДн в Учреждении осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Учреждение выступает в качестве работодателя (гл. 14 Трудового кодекса Российской Федерации), в связи с реализацией Учреждением своих прав и обязанностей как юридического лица.

5. Цели сбора и обработки ПДн

Оператор осуществляет сбор и обработку ПДн исключительно в целях:

- обеспечения 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 2012г. №1006;
- осуществления трудовых отношений;

- осуществления гражданско-правовых отношений.

В Учреждении не производится обработка ПДн, несовместимая с целями их сбора.

При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Учреждение принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

6. Категории субъектов персональных данных

В Учреждении обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющие близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за медицинской помощью.

7. Сведения о третьих лицах, участвующих в обработке ПДн

В целях соблюдения законодательства Российской Федерации, для достижения целей обработки, а также в интересах и с согласия субъектов.

Оператор в ходе своей деятельности предоставляет ПДн следующим организациям:

- Федеральной налоговой службе;
- Кредитно-финансовым организациям (в рамках действующих договоров по ведению заработных проектов);
- федеральному и территориальному фондам обязательного медицинского страхования;
- пенсионному фонду Российской Федерации, включая его территориальные органы;
- страховым организациям, осуществляющим обязательное медицинское страхование;
- организациям (учреждениям), осуществляющим на законном основании обработку медико-статистической информации.

Оператор не поручает обработку ПДн другим лицам.

8. Порядок и условия обработки ПДн

Оператор в своей деятельности обеспечивает соблюдение принципов обработки ПДн, указанных в ст. 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Оператор не осуществляет обработку биометрических ПДн (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

Оператор выполняет обработку специальных категорий ПДн, касающихся состояния здоровья.

Оператор не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу ПДн.

Оператором созданы общедоступные источники ПДн (справочники, адресные книги). ПДн, сообщаемые субъектом (фамилия, имя, отчество, год и место рождения, адрес, сведения о профессии и др.), включаются в такие источники только с письменного разрешения субъекта ПДн.

Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников по требованию субъекта ПДн.

ПДн, обрабатываемые Учреждением:

- данные полученные при осуществлении трудовых отношений;
- данные полученные для осуществления отбора кандидатов на работу в организацию;
- данные полученные при осуществлении гражданско-правовых отношений;
- данные полученные при оказании медицинской помощи.

Полный список ПДн представлен в Перечне ПДн, утвержденном главным врачом Учреждения.

Обработка персональных данных ведется:

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

8.1. Получение ПДн

Все ПД следует получать от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

В случае недееспособности либо несовершеннолетия субъекта ПДн все ПДн субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении ПДн своего подопечного и дает письменное согласие на их обработку оператором.

Согласие на обработку ПДн может быть отозвано субъектом ПДн либо законным представителем субъекта ПДн.

В случаях, когда оператор может получить необходимые ПДн субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее. В уведомлении оператор обязан указать:

- наименование и адрес оператора;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- права субъекта ПДн;
- источник получения ПДн.

Запрещается получать и обрабатывать ПДн субъекта о его политических, религиозных и иных убеждениях и частной жизни.

Запрещается получать и обрабатывать ПДн субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

8.2. Обработка ПДн

Обработка персональных данных осуществляется в следующих случаях:

- обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;
- обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн за исключением целей, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных»;

Обработка ПДн должна осуществляться на законной и справедливой основе.

Субъекты ПДн не должны отказываться от своих прав на сохранение и защиту ПДн.

Порядок рассмотрения запросов субъектов ПДн или их представителей осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

8.3. Хранение ПДн

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

Хранение ПДн в форме, позволяющей определить субъекта ПДн, 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

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

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

Подразделения, хранящие ПДн на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно постановлению Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

8.4. Передача ПДн

При передаче ПДн субъекта оператор обязан соблюдать следующие требования:

- не сообщать ПДн субъекта третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами.
- предупредить лиц, получающих ПДн субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих

лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн субъекта, обязаны соблюдать требования конфиденциальности;

- передавать ПДн субъекта представителям субъектов в порядке, установленном Трудовым Кодексом Российской Федерации, и ограничивать эту информацию только теми ПДн субъекта, которые необходимы для выполнения указанными представителями их функций;

- все сведения о передаче ПДн субъекта регистрируются в Журнале учета передачи ПДн в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи ПДн или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

Все меры конфиденциальности при сборе, обработке и хранении ПДн субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

Доступ работников к ПДн разрешен в соответствии со списками, утвержденными Оператором.

Все сотрудники, имеющие доступ к ПДн субъектов, обязаны подписать обязательство о неразглашении ПДн.

Передача ПДн осуществляется в соответствии с пунктом 7 настоящей Политики.

8.5. Уничтожение ПДн

ПДн субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Документы, содержащие ПДн, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

Уничтожение или обезличивание части ПДн производится способом, исключающим дальнейшую обработку.

При необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию.

Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение shreddera.

ПДн на электронных носителях уничтожаются способом гарантированного уничтожения конфиденциальной информации с носителя. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии. Состав комиссии утверждается главным врачом Учреждения.

9. Принципы обеспечения безопасности персональных данных

Основной задачей обеспечения безопасности ПДн при их обработке в Учреждении является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

Для обеспечения безопасности ПДн Учреждение руководствуется следующими принципами:

- **законность:** защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;
- **системность:** обработка ПДн в Учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;
- **комплексность:** защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Учреждения (далее - ИС) и других имеющихся в Учреждении систем и средств защиты;
- **непрерывность:** защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;
- **своевременность:** меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
- **преемственность и непрерывность совершенствования:** модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Учреждении с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
- **персональная ответственность:** ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;
- **минимизация прав доступа:** доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- **гибкость:** обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Учреждения (далее - ИСПДн), а также объема и состава обрабатываемых ПДн;
- **открытость алгоритмов и механизмов защиты:** структура, технологии и алгоритмы функционирования системы защиты ПДн Учреждения (далее - СЗПДн) не дают возможности преодоления имеющихся в Учреждении систем защиты возможными нарушителями безопасности ПДн;
- **научная обоснованность и техническая реализуемость:** уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;
- **специализация и профессионализм:** реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;
- **эффективность процедур отбора кадров и выбора контрагентов:** кадровая политика Учреждения предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Учреждения до заключения договоров;
- **наблюдаемость и прозрачность:** меры по обеспечению безопасности ПДн 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 ПДн, а результаты контроля регулярно

анализируются.

10. Защита персональных данных

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

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

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.

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

Основными необходимыми мерами защиты ПДн в Учреждении, являются:

- назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПДн;
- определение актуальных угроз безопасности ПДн при их обработке в ИСПД, и разработка мер и мероприятий по защите ПДн;
- разработка политики в отношении обработки персональных данных;
- установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн в ИСПД;
- установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности;
- сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
- сертифицированное программное средство защиты информации от несанкционированного доступа;
- сертифицированные межсетевой экран и средство обнаружения вторжения;
- соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;
- установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение работников Учреждения непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;
- осуществление внутреннего контроля и аудита.

11. Основные права субъекта ПДн и обязанности Учреждения

11.1. Основные права субъекта ПДн:

Субъект ПДн имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором 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 «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 оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Субъект ПДн 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.

11.2. Обязанности Учреждения

Учреждение обязано:

- при сборе ПДн предоставить информацию об обработке его ПДн;
- в случаях если ПДн были получены не от субъекта ПДн уведомить субъекта;
- при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн;
- давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.

12. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Лица, виновные в нарушении положений законодательства РФ в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

Обязательства по соблюдению конфиденциальности ПДн остаются в силе и после окончания работы с ними вышеуказанных лиц.

