

**БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ХАНТЫ-МАНСКИЙСКОГО АВТОНОМНОГО ОКРУГА-ЮГРЫ
«СОВЕТСКИЙ РАЙОННЫЙ СОЦИАЛЬНО-РЕАБИЛИТАЦИОННЫЙ
ЦЕНТР ДЛЯ НЕСОВЕРШЕННОЛЕТНИХ»
(БУ «СОВЕТСКИЙ РАЙОННЫЙ ЦЕНТР ДЛЯ НЕСОВЕРШЕННОЛЕТНИХ»)**

ПРИКАЗ

« 19 » марта 2018 г.
г.п. Пионерский

№ 84 -р

Об утверждении организационно-
распорядительной документации
по защите информации

Во исполнение требований Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативно-правовых актов, в соответствии с пунктом 2.2. протокола заседания постоянно действующей технической комиссии Депсоцразвития Югры от 30.01.2018 № 33

ПРИКАЗЫВАЮ:

1. Утвердить Политику в отношении обработки персональных данных в БУ «Советский районный центр для несовершеннолетних» (приложение 1).
2. Инженеру по автоматизированным системам управления производством И.А. Кандаурову разместить на официальном сайте БУ «Советский районный центр для несовершеннолетних» утверждённую Политику в отношении обработки персональных данных в БУ «Советский районный центр для несовершеннолетних». Срок: 23.03.2018.
3. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (приложение 2).
4. Контроль за исполнением настоящего приказа возложить на заместителя директора А.В. Воронцова.



Т.А. Емелина

**ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В
БУ «СОВЕТСКИЙ РАЙОННЫЙ ЦЕНТР ДЛЯ
НЕСОВЕРШЕННОЛЕТНИХ»**

пгт. Пионерский
2018

Содержание:

1. Термины и определения
2. Назначение и область применения
3. Принципы обработки персональных данных
4. Условия обработки персональных данных
5. Цели обработки персональных данных
6. Особенности обработки персональных данных и их передача третьим лицам
7. Права субъектов персональных данных
8. Обеспечение безопасности персональных данных

1. Термины и определения

1.1. Персональные данные (далее – ПДн) – любая информация, относящаяся к прямо или косвенно определённом или определяемому физическому лицу.

1.2. 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.

1.3. 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 ПДн.

1.4. Автоматизированная обработка персональных данных – обработка ПДн с помощью средств вычислительной техники.

1.5. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.6. Использование персональных данных – действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом, затрагивающих права и свободы субъекта ПДн или других лиц.

1.7. Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

1.8. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

1.9. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

1.10. Информационная система персональных данных (далее ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.11. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства Учреждению иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Назначение и область применения

3.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Советский районный социально-реабилитационный центр для несовершеннолетних» (далее – Учреждение) разработана в соответствии со статьей 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон №152-ФЗ) и действует в отношении всех персональных данных, которые Департамент социального развития Ханты-Мансийского автономного округа – Югры (далее – Оператор) может получить от субъектов персональных данных.

3.2. Политика распространяется на персональные данные, полученные как до, так и после её утверждения приказом Оператора.

3.3. Действие настоящей Политики распространяется на все процессы обработки персональных данных Оператором, как с использованием средств автоматизации, так и без использования таких средств, на всех работников Оператора, участвующих в таких процессах, а также на информационные системы Учреждения, используемые в процессах обработки персональных данных.

4. Принципы обработки персональных данных

4.1. Обработка персональных данных осуществляется Оператором на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей. Оператором не допускается обработка персональных данных, несовместимая с целями сбора персональных данных и объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.2. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых Оператором персональных данных соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.

4.3. При обработке персональных данных Оператором обеспечивается точность персональных данных, их достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. Оператором принимаются необходимые меры (обеспечивается их принятие) по удалению или уточнению неполных или неточных персональных данных.

4.4. При определении состава обрабатываемых персональных данных субъектов персональных данных Оператор руководствуется минимально необходимым составом персональных данных для достижения целей получения персональных данных.

4.5. Хранение персональных данных Оператором осуществляется в форме, позволяющей 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. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5. Условия обработки персональных данных

5.1. Обработка персональных данных осуществляется в соответствии с целями, заранее определенными и заявленными при сборе персональных данных, а также полномочиями Оператора, определенными действующим законодательством Российской Федерации и договорными отношениями с Оператором.

5.2. Получение и обработка персональных данных в случаях, предусмотренных законом № 152-ФЗ, осуществляется Оператором только с письменного согласия субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью.

5.3. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законом № 152-ФЗ. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Оператором.

5.4. Оператор вправе обрабатывать персональные данные без согласия субъекта персональных данных (или при отзыве субъектом персональных данных согласия на обработку персональных данных) при наличии оснований, указанных в законе № 152-ФЗ.

5.5. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, Оператором не осуществляется.

5.6. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные) и сведения о состоянии здоровья, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных или иных оснований, предусмотренных федеральным законодательством.

5.7. Персональные данные субъекта могут быть получены Оператором от лица, не являющегося субъектом персональных данных, при условии предоставления Оператору подтверждения наличия оснований, указанных в законе № 152-ФЗ или иных оснований, предусмотренных федеральным законодательством.

5.8. Право доступа к персональным данным субъектов персональных данных на бумажных и электронных носителях имеют работники Оператора в соответствии с их должностными обязанностями.

5.9. Оператором не осуществляется трансграничная передача персональных данных и не принимаются решения, основанные

исключительно на автоматизированной обработке персональных данных субъекта.

6. Цели обработки персональных данных

6.1. В соответствии с принципами и условиями обработки персональных данных, Оператором определены следующие цели обработки ПДн:

выполнение обязательств, предусмотренных служебным контрактом;
выполнение требований Трудового кодекса Российской Федерации других нормативных актов Российской Федерации (в том числе предоставление персональных данных в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования);

принятие решений и выполнение обязательств по обращениям граждан Российской Федерации в соответствии с законодательством Российской Федерации;

оказание государственных услуг гражданам.

7. Особенности обработки персональных данных и их передача третьим лицам

7.1. Обработка персональных данных Оператором осуществляется как с использованием средств автоматизации, так и без использования таких средств.

При обработке персональных данных Оператор осуществляет следующие действия с персональными данными: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

7.2. Передача персональных данных субъектов персональных данных третьим лицам осуществляется Оператором в соответствии с требованиями действующего законодательства.

7.3. Оператор вправе поручить обработку персональных данных третьей стороне с согласия субъекта персональных данных и в иных случаях, предусмотренных действующим законодательством Российской Федерации, на основании заключаемого с этой стороной соглашения, (далее - поручение). Третья сторона, осуществляющая обработку персональных данных по поручению Оператора, обязана соблюдать принципы и правила обработки персональных данных, предусмотренные законом № 152-ФЗ, обеспечивая конфиденциальность и безопасность персональных данных при их обработке.

8. Права субъектов персональных данных

8.1. Субъект персональных данных 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.

8.2. Субъект персональных данных 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, применяемые Оператором способы обработки ПДн;

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 ПДн прав, предусмотренных законом № 152-ФЗ;

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 законом № 152-ФЗ.

9. Обеспечение безопасности персональных данных

9.1. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие 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. К данным мерам в частности относятся:

назначение лица, ответственного за организацию обработки персональных данных;

осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

ознакомление работников Оператора с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных, требованиями к защите персональных данных;

издание локальных актов по вопросам обработки персональных данных и локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации;

определение угроз безопасности персональных данных и необходимого уровня защищённости персональных данных, при их обработке в ИСПДн;

применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн;

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;

осуществление оценки эффективности применяемых мер по обеспечению безопасности персональных данных.

**Правила
осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных**

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных (далее - ПДн) в Учреждении требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Правила), разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных, а также определяют основания, порядок и методы проведения внутреннего контроля соответствия обработки ПДн требованиям законодательства Российской Федерации.

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных к требованиям защиты персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям к защите ПДн в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Советский районный социально-реабилитационный центр для несовершеннолетних» (далее – Учреждение) организовывается проведение ежегодных проверок.

2.2. Проверки проводятся ответственным за организацию обработки ПДн совместно с ответственным за обеспечение безопасности ПДн и другой защищаемой информации, обрабатываемой в Учреждении и ответственными за эксплуатацию информационных систем персональных данных Учреждения (далее - ИСПДн Учреждения).

2.3. Плановые проверки условий обработки ПДн проводятся на основании утвержденного руководителем Учреждения ежегодного плана внутренних проверок режима защиты ПДн (плановые проверки).

2.4. Внеплановые проверки проводятся на основании поступившей информации о нарушениях правил обработки ПДн, по инициативе ответственного за организацию обработки ПДн, либо ответственного за обеспечение безопасности ПДн и другой защищаемой информации, обрабатываемой в Учреждении. Проведение внеплановой проверки организуется в течение 10 (десяти) рабочих дней со дня поступления информации о нарушениях правил обработки ПДн.

2.5. В проведении проверки условий обработки ПДн не могут участвовать сотрудники Учреждения, прямо или косвенно заинтересованных в ее результате.

2.6. Проверки условий обработки ПДн осуществляются непосредственно на месте обработки ПДн путем опроса либо, при необходимости, путем осмотра служебных мест сотрудников Учреждения, участвующих в процессе обработки ПДн.

2.7. При проведении проверки должны быть полностью, объективно и всесторонне, установлены:

- соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Учреждения;

- соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;

- достаточность (избыточность) ПДн для целей обработки ПДн, заявленных при сборе ПДн;

- отсутствие (наличие) объединения, созданных для несовместимых между собой целей, баз данных ИСПДн;

- порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн;

- порядок и условия соблюдения парольной защиты;

- порядок и условия соблюдения антивирусной защиты;

- порядок и условия обеспечения резервного копирования;

- эффективность принимаемых мер по обеспечению безопасности ПДн до их ввода в ИСПДн;

- условия соблюдения режима защиты при подключении к информационно-телекоммуникационным сетям;

- порядок и условия обновления программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн;

- порядок и условия применения средств защиты информации;

- соблюдение учета носителей ПДн;

- соблюдение правил доступа к ПДн;

соблюдение порядка доступа в помещения, в которых ведется обработка ПДн;

наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;

мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

осуществление мероприятий по обеспечению целостности ПДн.

2.8. Ответственный за организацию обработки ПДн и ответственный за обеспечение безопасности ПДн и другой защищаемой информации, обрабатываемой в Учреждении, а также ответственные за эксплуатацию ИСПДн Департамента в ходе проверки имеют право:

запрашивать у сотрудников информацию, необходимую для реализации своих полномочий;

требовать от уполномоченных на обработку ПДн сотрудников уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;

принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;

вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПДн при их обработке;

вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПДн.

2.9. Проверка условий обработки ПДн должна быть завершена не позднее чем через тридцать календарных дней со дня принятия решения о ее проведении.

2.10. По результатам проведенной проверки условий обработки ПДн ответственный за организацию обработки ПДн предоставляет руководителю Учреждения письменное заключение с указанием мер, необходимых для устранения выявленных нарушений.