

МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР РАЗВИТИЯ И ПОДДЕРЖКИ СИСТЕМЫ ОБРАЗОВАНИЯ»
(МКУ ЦР и ПСО)

П Р И К А З

27 декабря 2024 г.

г. Светлоград

№ 122

Об утверждении Политики муниципального казенного учреждения «Центр развития и поддержки системы образования» в отношении обработки персональных данных и реализации требований к их защите

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в целях совершенствования деятельности по работе с персональными данными

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Политику муниципального казенного учреждения «Центр развития и поддержки системы образования» в отношении обработки персональных данных и реализации требований к их защите.
2. Зубенко Е.Ю., заведующему хозяйством, исполняющему обязанности инженера-техника, опубликовать настоящий приказ на официальном МКУ ЦР и ПСО в информационно-телекоммуникационной сети «Интернет».
3. Капиносковой О.В., специалисту по закупкам, исполняющему обязанности специалиста по кадрам, довести настоящий приказ до сведения работников.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор
муниципального казенного учреждения
«Центр развития и поддержки системы образования»  Т.В.Таранушенко

Ознакомлены: О.В. Капинослова
Е.Ю.Зубенко 



Утверждена
приказом муниципального казенного
учреждения «Центр развития и
поддержки системы образования»
от 27 декабря 2024 г. № 122

Политика
муниципального казенного учреждения «Центр развития и поддержки
системы образования» в отношении обработки персональных данных
и реализации требований к их защите

1. Общие положения

1.1. Настоящий документ определяет цели обработки персональных данных в муниципальном казенном учреждении «Центр развития и поддержки системы образования» (далее — Оператор), принципы их обработки, а также содержит сведения о передаче персональных данных взаимодействующим организациям и реализуемых требованиях по защите персональных данных.

1.2. Политика Оператора в отношении обработки персональных данных и реализации требований к их защите (далее — Политика) разработана в соответствии с пунктом 2 статьи 18.1 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» и действует в отношении всех персональных данных, обрабатываемых Оператором.

1.3. Политика распространяется на персональные данные, полученные как до, так и после утверждения настоящей Политики.

1.4. Политика является публичным документом.

1.5. Действие Политики не распространяется на отношения, возникающие при:

организации хранения, комплектования, учета и использования содержащих персональные данные архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

2. Информация об операторе

2.1. Наименование: муниципальное казенное учреждение «Центр развития и поддержки системы образования» (МКУ ЦР и ПСО)

ИНН: 2617800032

КПП: 261701001

ОГРН 001112651000318

Юридический адрес: 356530, Ставропольский край, Петровский муниципальный округ, город Светлоград, улица Ленина, здание 29.

Тел. 8(86547) 4-14-70.

Адрес электронной почты: obrazovanie@petrgosk.ru.

3. Цели обработки персональных данных

3.1. Оператор обрабатывает персональные данные исключительно в следующих целях:

- предоставление государственных и муниципальных услуг;
- регулирование трудовых отношений и иных непосредственно связанных с ними отношений с сотрудниками Оператора;
- рассмотрение обращений граждан;
- осуществление гражданско-правовых отношений;
- выполнение других задач, возложенных на Оператора.

4. Категории субъектов персональных данных, обрабатываемых Оператором

4.1. К категориям субъектов персональных данных, обрабатываемых Оператором, относятся:

- сотрудники Оператора;
- бывшие сотрудники Оператора;
- близкие родственники сотрудника (супруг(-а), дети, родители) Оператора;
- лица, претендующие на замещение должностей муниципальной службы;
- лица, замещающие должности руководителей муниципальных учреждений, подведомственных Оператору;
- лица, претендующие на замещение должностей руководителей муниципальных учреждений, подведомственных Оператору;
- граждане, обратившиеся с обращением (жалобой или заявлением);
- граждане, состоящие в договорных отношениях с Оператором;
- граждане, персональные данные которых обрабатываются Оператором в связи с предоставлением Оператором государственных и муниципальных услуг;
- иные лица, связанные с исполнением Оператором муниципальных функций по решению вопросов местного значения, определенных Уставом Петровского муниципального округа Ставропольского края.

5. Перечень действий с персональными данными

5.1. Оператор осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), удаление, уничтожение персональных данных.

5.2. Обработка персональных данных Оператором ведется с использованием средств автоматизации (электронные носители

персональных данных) и без использования средств автоматизации (бумажные носители персональных данных).

5.3. Хранение персональных данных Оператором осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, за исключением случаев, когда срок хранения персональных данных установлен федеральными законами или договором, стороной которого является субъект персональных данных.

5.4. Персональные данные, полученные Оператором от субъекта персональных данных, хранятся как на бумажных носителях, так и в электронном виде.

5.5. Персональные данные на бумажных носителях хранятся в сейфах.

5.6. Персональные данные в электронном виде хранятся на жестких дисках компьютеров сотрудников Оператора.

5.7. Оператором запрещено размещать электронные документы, содержащие персональные данные, в открытых электронных каталогах (файловых хостингах).

5.8. Уничтожение персональных данных субъекта осуществляется Оператором в течение 30 (тридцати) дней с даты достижения целей обработки персональных данных. В указанный же срок Оператор должен уничтожить персональные данные субъекта при поступлении от него отзыва согласия на их обработку.

5.9. Уничтожение носителей персональных данных на бумажных носителях производится Оператором путем дробления (измельчения).

Персональные данные на электронных носителях уничтожаются путем форматирования носителя, без возможности последующего восстановления информации.

6. Принципы обработки персональных данных

6.1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в статье 5 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

6.2. Обработка персональных данных Оператором осуществляется на основе следующих принципов:

- обработка персональных данных осуществляется на законной и справедливой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- обработке подлежат только те персональные данные, которые отвечают целям их обработки;

- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям обработки;

- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки;

- хранение персональных данных должно осуществляться 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.

6.3. Оператор при обработке персональных данных обеспечивает необходимые условия для беспрепятственной реализации субъектом персональных данных своих прав.

7. Передача персональных данных

7.1. Передача персональных данных осуществляется Оператором в следующих случаях, если:

- субъект персональных данных выразил свое согласие на передачу своих персональных данных;

- передача персональных данных предусмотрена законодательством Российской Федерации;

- предоставление обрабатываемых персональных данных производится в соответствии с законодательством Российской Федерации органам налоговой службы, внебюджетным фондам, кредитным организациям;

- информация передается по внутренней сети и с использованием информационно-телекоммуникационной сети «Интернет»;

- оператор не поручает обработку персональных данных другим лицам на основании договора.

8. Организация защиты персональных данных

8.1. Персональные данные относятся к сведениям ограниченного доступа и подлежат защите в рамках функционирующей у Оператора системы защиты информации.

8.2. При организации защиты персональных данных при их обработке Оператор руководствуется, в том числе:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами»;

- постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказом Роскомнадзора от 28.10.2022 №179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;

- постановлением Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- Указом Президента Российской Федерации от 06.03.1997 №188 «Об утверждении Перечня сведений конфиденциального характера»,

- Трудовым кодексом Российской Федерации.

8.3. К организационным мерам защиты персональных данных относятся, в том числе:

8.3.1. Назначение ответственных за обеспечение безопасности информации.

8.3.2. Разработка и поддержание в актуальном состоянии организационно-распорядительных документов, регламентирующих порядок обработки персональных данных, создания и функционирования системы защиты персональных данных.

8.3.3. Организация деятельности субъектов информационных отношений, в том числе:

установление перечня должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

информирование лиц, осуществляющих обработку персональных данных, о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

обеспечение раздельной фиксации на материальных носителях персональных данных, имеющих различную цель обработки, или их раздельной обработки;

обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

8.3.4. Осуществление внутреннего контроля соответствия обработки и безопасности персональных данных Оператора требованиям законодательства Российской Федерации и иных нормативных правовых актов о персональных данных, в том числе требованиям к защите персональных данных.

8.3.5. Проведение мероприятий по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с персональными данными.

8.3.6. Обучение, периодическое повышение квалификации сотрудников, ответственных за организацию обработки и обеспечение безопасности информации, сотрудников, непосредственно выполняющих мероприятия по обеспечению безопасности персональных данных.

8.4. К техническим мерам защиты относится использование программно-аппаратных средств, выполняющих самостоятельно или в комплексе с другими средствами функции защиты персональных данных, и методов защиты, в том числе:

программной или программно-технической защиты от несанкционированного доступа к информационным ресурсам автоматизированных рабочих мест, на которых обрабатываются персональные данные;

программно-технических средств, позволяющих восстанавливать персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;

средств защиты персональных данных от утечки по техническим каналам при их обработке, хранении и передаче по каналам связи;

средств межсетевого экранирования при подключении автоматизированных рабочих мест к локальным сетям общего пользования или к сети Интернет;

криптографических средств защиты информации;

средств защиты от вредоносного программного обеспечения.

8.5. Оператором применяются сертифицированные средства защиты информации, соответствующие требованиям, установленным уполномоченными органами в области технической защиты информации.

8.6. В случае принятия решения о проведении работ по обезличиванию персональных данных разрабатываются правила работы с обезличенными данными в соответствии с приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

8.7. Лицо, ответственное за организацию обработки персональных данных Оператора, при обеспечении безопасности персональных данных, в частности, вправе:

иметь доступ к информации, касающейся обработки персональных данных;

привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых отделами Оператора, с возложением на них соответствующих обязанностей и закреплением ответственности.

8.8. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

- документальным оформлением требований к безопасности обрабатываемых персональных данных;
- изданием нормативных правовых документов по организации защиты персональных данных;
- назначением ответственного за организацию обработки персональных данных;
- распределением ответственности по вопросам защиты персональных данных между сотрудниками Оператора;
- установлением персональной ответственности сотрудников Оператора за обеспечение безопасности обрабатываемых персональных данных;
- осуществлением внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- своевременным выявлением угроз безопасности персональных данных и принятием соответствующих мер защиты;
- приданием мероприятиям защиты информации характера обязательных элементов производственного процесса Оператора, а требованиям по их исполнению — элементов производственной дисциплины;
- ознакомлением сотрудников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том

числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных и (или) обучением указанных сотрудников;

- резервным копированием информационных ресурсов;
- применением программных продуктов, отвечающих требованиям защиты персональных данных;
- учетом машинных носителей персональных данных;
- выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;
- своевременным применением критических обновлений общесистемного и прикладного программного обеспечения.