

ПОЛОЖЕНИЕ

ГБОУ ЦРО №7 в отношении обработки персональных данных

1. Назначение Положения

Настоящее Положение предназначено для определения концептуальных основ деятельности Государственного бюджетного образовательного учреждения Центр реабилитации и образования №7 Департамента труда и социальной защиты населения г. Москвы (ГБОУ ЦРО № 7) по обеспечению защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2. Область применения

2.1. Настоящее Положение распространяется на деятельность всех подразделений ГБОУ ЦРО № 7, участвующих в обработке персональных данных.

Действующая редакция Положения на бумажном носителе хранится по адресу: Московская область, м.о. Истра, пос. Гидроузла им. Куйбышева, стр. 35А (административный корпус)

3. Срок действия

3.1. Настоящее Положение является бессрочным.

3.2. Настоящее Положение может пересматриваться и заново утверждаться по мере внесения изменений:

- в нормативные правовые акты в сфере персональных данных;
- в локальные акты ГБОУ ЦРО № 7, регламентирующие организацию обработки и обеспечение безопасности персональных данных.

4. Термины и определения

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор 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, представление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Представление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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.

5. Нормативные ссылки

5.1. Настоящая Политика разработана в соответствии с требованиями законодательства Российской Федерации, в том числе:

- Трудовой кодекс Российской Федерации,
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»,
- Федеральный закон от 29.12.2012 N 273-ФЗ «Об образовании в Российской Федерации»,

- Федеральный закон от 24 ноября 1995 г. N 181-ФЗ «О социальной защите инвалидов в Российской Федерации»,
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. Постановлением Правительства Российской Федерации от 01.11.2012 № 1119);
- Постановление Правительства № 719 «Об утверждении Положения о воинском учёте»;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. Постановлением Правительства Российской Федерации от 15.09.2008 № 687);
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21);

6. Описание Положения: принципы, способы обработки персональных данных

6.1 При обработке персональных данных ГБОУ ЦРО №7 соблюдаются следующие **принципы**:

- 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 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 их обработки;

- в ГБОУ ЦРО №7 не обрабатываются биометрические персональные данные (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных), за исключением фотографий.
- ГБОУ ЦРО №7 не осуществляет трансграничную передачу персональных данных.
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных;
- принимаются необходимые меры по удалению или уточнению неполных или неточных персональных данных;
- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации и города Москвы;
- в ГБОУ ЦРО №7 осуществляется как автоматизированная обработка персональных данных, так и неавтоматизированная обработка персональных данных (обработка персональных данных без использования средств автоматизации; обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого субъекта персональных данных осуществляются при непосредственном участии человека).
- обрабатываемые персональные данные уничтожаются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.
- ГБОУ ЦРО №7 осуществляет передачу персональных данных третьим лицам в соответствии с требованиями законодательства Российской Федерации в области обработки и защиты персональных данных.
- ГБОУ ЦРО №7 в ходе своей деятельности вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного контракта, либо путем принятия государственным органом соответствующего акта. При этом обязательным условием предоставления и/или поручения обработки персональных данных другому лицу является обязанность сторон

по соблюдению конфиденциальности и обеспечению безопасности персональных данных при их обработке.

– в случаях, когда ГБОУ ЦРО №7 поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет ГБОУ ЦРО №7. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед ГБОУ ЦРО №7.

– прекращение обработки персональных данных осуществляется при прекращении деятельности ГБОУ ЦРО №7 (ликвидация или реорганизация).

6.2 Обработка персональных данных в ГБОУ ЦРО № 7 включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. В ГБОУ ЦРО № 7 осуществляется обработка персональных данных с использованием средств автоматизации и без использования средств автоматизации.

7. Субъекты персональных данных, правовые основания и цели обработки персональных данных

7.1 Правовым основанием обработки персональных данных субъектов персональных данных ГБОУ ЦРО №7 является исполнение возложенных на ГБОУ ЦРО №7 законодательством Российской Федерации функций, полномочий и обязанностей в соответствии с федеральными законами, в том числе, но не ограничиваясь:

Трудовой кодекс Российской Федерации, Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федеральный закон от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральный закон от 29.12.2012 N 273-ФЗ «Об образовании в Российской Федерации», Федеральный закон от 24 ноября 1995 г. N 181-ФЗ «О социальной защите инвалидов в Российской Федерации», Постановление Правительства от 27 ноября 2006 г. № 719 «Об утверждении Положения о воинском учете». Правовым основанием также является: Устав ГБОУ ЦРО №7, договоры, заключаемые между ГБОУ ЦРО №7 и субъектами персональных данных, согласие субъектов персональных данных на обработку их персональных данных.

7.2 Субъектами персональных данных, данные которых обрабатываются в ГБОУ ЦРО №7, являются:

- Учащиеся. Состав данных: фамилия, имя, отчество; пол, дата рождения, данные свидетельства о рождении; СНИЛС; данные медицинской карты; адрес проживания; адрес регистрации, данные о состоянии здоровья несовершеннолетнего ребенка
- Законные представители несовершеннолетнего. Состав данных: фамилия, имя, отчество, пол, дата рождения, паспортные данные, СНИЛС, адрес проживания, контактный телефон, статус законного представителя по отношению к ребенку
- Сотрудники. Состав данных: фамилия, имя и отчество, фотография, номер телефона, адрес электронной почты, место работы и должность, тип документа, удостоверяющего личность, данные документа, удостоверяющего личность, данные страхового Свидетельства государственного пенсионного страхования, данные документа воинского учета, сведения о наградах и почетных званиях, документы об образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются), анкетные данные - автобиография, сведения о семейном положении, перемене фамилии, наличии детей и иждивенцев, данные трудового договора и соглашений к нему, данные кадровых приказов о приеме, переводах, увольнении, данные личной карточки по форме Т-2, данные документов о прохождении аттестации, собеседования, результатов оценки и обучения
- Взрослые и несовершеннолетние лица, участвующие в съёмках, интервью и иных мероприятиях проекта Радиоцентр 7, персональные данные которых (в том числе фото-, аудио- и видеозаписи) планируется распространять (публиковать) на сайте, в социальных сетях и иных открытых источниках, делая их доступными неограниченному кругу лиц. Состав данных: фамилия, имя, отчество

7.3 Обработка персональных данных субъектов ПДн в ГБОУ ЦРО №7 осуществляется **в целях:**

- Предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на ГБОУ ЦРО №7 функций, полномочий и обязанностей.
- Исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти города Москвы и иных субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и

муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта ПДн в государственной информационной системе «Портал государственных и муниципальных услуг (функций) города Москвы».

- Исполнения договора, стороной которого либо выгодоприобретателем, или поручителем, по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем.

- Осуществления прав и законных интересов ГБОУ ЦРО №7 или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн.

– Доступа неограниченного круга лиц, к которым предоставлен субъектом ПДн либо по его просьбе.

– Опубликования или обязательного раскрытия в соответствии с законодательством Российской Федерации и города Москвы.

– Подготовки и публикации материалов (фото, аудио, видео) в открытом доступе (на сайтах, в соцсетях Учреждения) — при наличии отдельного согласия на распространение

8. Меры по надлежащей организации обработки и обеспечению безопасности персональных данных

8.1 Обеспечение безопасности персональных данных в ГБОУ ЦРО № 7 достигается, в частности, следующими способами:

— назначением ответственного лица за организацию обработки персональных данных, права и обязанности которого определяются локальными актами ГБОУ ЦРО № 7;

— осуществлением внутреннего контроля и/или аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, требованиями к защите персональных данных, локальными актами ГБОУ ЦРО № 7;

— ознакомлением сотрудников ГБОУ ЦРО №7, 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;

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;
- учетом машинных (материальных) 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 информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- внедрением системы контроля и управления доступом для исключения несанкционированного доступа к серверному оборудованию

8.2 Обязанности сотрудников ГБОУ ЦРО №7, непосредственно осуществляющих обработку персональных данных, а также их ответственность определяются в локальных актах ГБОУ ЦРО № 7.

9. Взаимодействие с субъектами персональных данных

9.1 Права субъектов персональных данных определяются статьями 14–17 Федерального закона № 152-ФЗ «О персональных данных».

9.2 Для осуществления своих прав субъект персональных данных может лично или через законного представителя обратиться в ГБОУ ЦРО №7 путем направления письменного запроса по адресу: 143513, Московская область, м.о. Истра, пос. Гидроузла им. Куйбышева, стр. 35А.

9.3 Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в отношениях с ГБОУ ЦРО №7 (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным

образом подтверждающие факт обработки персональных данных ГБОУ ЦРО №7;

– подпись субъекта персональных данных или его представителя.

9.4 Порядок рассмотрения запросов осуществляется ГБОУ ЦРО №7 в порядке, установленном Законом «О персональных данных».

10. Сроки обработки персональных данных

10.1 Сроки обработки (в т.ч. хранения) персональных данных, обрабатываемых ГБОУ ЦРО №7, определяются исходя из целей обработки персональных данных и в соответствии с требованиями федеральных законов Российской Федерации.

11. Распределение ролей и ответственности

11.1. Ответственным за организацию обработки персональных данных в ГБОУ ЦРО № 7 назначается приказом директора учреждения конкретное должностное лицо.

11.2. В обязанности ответственного лица входит:

- организация разработки, актуализации и контроля исполнения локальных актов по обработке и защите персональных данных;
- координация взаимодействия с Роскомнадзором и иными контролирующими органами;
- организация обучения и инструктажа сотрудников, допущенных к обработке персональных данных;
- контроль за соблюдением требований по защите персональных данных в информационных системах и при неавтоматизированной обработке;
- обеспечение своевременного реагирования на инциденты, связанные с нарушением безопасности персональных данных.

11.3. Руководители подразделений ГБОУ ЦРО № 7 несут ответственность за соблюдение требований Положения в пределах своих подразделений, в том числе за допуск сотрудников к работе с персональными данными и контроль их действий.

11.4. Сотрудники, непосредственно обрабатывающие персональные данные, обязаны:

- соблюдать требования законодательства и локальных актов ГБОУ ЦРО № 7 по обработке и защите персональных данных;

- обеспечивать конфиденциальность персональных данных и не передавать их третьим лицам без установленных оснований;
- своевременно информировать ответственное лицо о выявленных нарушениях, инцидентах или рисках безопасности;
- использовать только предоставленные и разрешённые средства доступа к информационным системам персональных данных.

12. Порядок сбора персональных данных и оформления согласий

12.1. Сбор персональных данных осуществляется:

- при личном обращении субъекта персональных данных или его представителя;
- посредством заполнения форм на официальном сайте ГБОУ ЦРО № 7;
- в рамках исполнения трудовых и гражданско-правовых договоров;
- на основании актов и документов, поступающих от государственных органов и иных уполномоченных лиц.

12.2. Согласие субъекта персональных данных на обработку оформляется отдельным письменным документом по утверждённой форме, если иное не предусмотрено федеральным законом.

12.3. При сборе персональных данных субъект персональных данных информируется о целях, правовых основаниях, перечне данных, сроках обработки, а также о его правах в соответствии с ФЗ-152. Факт информирования фиксируется в журнале учёта согласий либо в электронной системе (с обеспечением возможности подтверждения даты и содержания информирования).

13. Хранение, учёт и сроки хранения персональных данных

13.1. Персональные данные хранятся:

- в информационных системах персональных данных — на серверах и рабочих станциях, защищённых средствами контроля доступа, антивирусной защиты и резервного копирования;
- на бумажных носителях — в запираемых шкафах/сейфах в специально отведённых помещениях;

13.2. Сроки хранения персональных данных устанавливаются в соответствии с номенклатурой дел и требованиями законодательства (в том числе архивного).

13.3. По истечении сроков хранения персональные данные подлежат уничтожению в порядке, установленном разделом 16 Положения.

14. Передача персональных данных третьим лицам и поручение обработки

14.1. Передача персональных данных третьим лицам допускается только при наличии одного из правовых оснований, предусмотренных ФЗ-152, в том числе:

- исполнение договора, стороной которого является субъект персональных данных;
- наличие согласия субъекта персональных данных (если требуется);
- исполнение требований законодательства (запросы госорганов, судов и т. д.).

14.2. При поручении обработки персональных данных третьему лицу (подрядчику) заключается договор поручения, содержащий обязательства по обеспечению безопасности персональных данных, перечень разрешённых действий и запрет на дальнейшую передачу без согласия оператора.

15. Меры защиты персональных данных (детализация)

15.1. Организационные меры:

- назначение ответственного лица и закрепление зон ответственности;
- проведение регулярных инструктажей и обучения сотрудников;
- разграничение прав доступа к персональным данным по принципу «необходимо для работы»;
- ведение журналов учёта доступа и уничтожения данных;
- периодические внутренние проверки и аудиты соблюдения требований.

15.2. Технические меры (в зависимости от информационной системы):

- идентификация и аутентификация пользователей;
- управление доступом и регистрация действий пользователей;
- антивирусная защита и контроль целостности ПО;
- шифрование данных при хранении и передаче (при необходимости);
- резервное копирование и восстановление данных;
- защита от несанкционированного доступа к серверному оборудованию и помещениям.

15.3. Физическая защита:

- контроль доступа в помещения, где хранятся носители персональных данных;
- использование запираемых шкафов и сейфов для бумажных носителей;
- учёт и контроль перемещения съёмных носителей.

16. Порядок уничтожения и обезличивания персональных данных

16.1. Уничтожение персональных данных производится при достижении целей обработки, отзыве согласия субъекта, выявлении неправомерной обработки либо по истечении сроков хранения.

16.2. Уничтожение на бумажных носителях осуществляется путём shreddирования с составлением Акта об уничтожении.

16.3. Уничтожение в электронной форме производится с применением средств гарантированного удаления данных либо путём физического уничтожения носителя (с составлением соответствующего акта).

16.4. Обезличивание персональных данных допускается в случаях, когда дальнейшая обработка возможна без идентификации субъекта, и осуществляется в соответствии с утверждёнными методиками.

17. Порядок выявления и реагирования на инциденты

17.1. Инцидент — любое событие, которое может привести к неправомерному доступу, утечке, искажению или уничтожению персональных данных.

17.2. Сотрудник, обнаруживший инцидент, обязан немедленно сообщить об этом ответственному лицу за обработку персональных данных.

17.3. Ответственное лицо организует:

- фиксацию инцидента (дата, время, обстоятельства, затронутые данные);
- локализацию и устранение последствий;

- оценку масштаба и последствий;
- уведомление руководства учреждения и, при необходимости, Роскомнадзора в установленные законом сроки.

17.4. По результатам инцидента составляется Акт о выявленном инциденте и принятых мерах (Приложение 6), а также разрабатываются корректирующие мероприятия для исключения повторения.

18. Контроль и аудит соблюдения Положения

18.1. Внутренний контроль за соблюдением Положения осуществляется ответственным лицом не реже 1 раза в год либо внепланово при выявлении нарушений или изменении законодательства.

18.2. Результаты контроля оформляются актом проверки, в котором фиксируются выявленные нарушения и сроки их устранения.

18.3. Обучение сотрудников проводится не реже 1 раза в год, а также при приёме на работу и при существенных изменениях в законодательстве или процессах обработки персональных данных.

19. Порядок пересмотра Положения

19.1. Положение подлежит актуализации не реже 1 раза в 3 года либо при изменении законодательства, появлении новых категорий субъектов персональных данных, изменении целей обработки или выявлении недостатков по результатам проверок и инцидентов.

19.2. Предложения по внесению изменений могут поступать от ответственного лица, руководителей подразделений и иных сотрудников. Решение о внесении изменений принимает директор ГБОУ ЦРО № 7.

20. Ознакомление сотрудников с Положением

20.1. Все сотрудники ГБОУ ЦРО № 7, имеющие доступ к персональным данным, обязаны ознакомиться с Положением под подпись.

20.2. Лист ознакомления хранится в кадровой службе и подлежит актуализации при приёме новых сотрудников и внесении изменений в Положение.