

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
КРАСНОДАРСКОГО КРАЯ ШКОЛА-ИНТЕРНАТ СПОРТИВНОГО ПРОФИЛЯ
(ГБОУ КК ШИСП)

П Р И К А З

« 20 » 11 2025 г.

№ 252

г. Краснодар

Об утверждении
Положения об обработке и
защите персональных данных
в государственном бюджетном
общеобразовательном учреждении
Краснодарского края школе-
интернате спортивного профиля

В целях соблюдения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», регламентации порядка сбора, хранения, обработки и защиты персональных данных работников, обучающихся (воспитанников), контрагентов и иных субъектов персональных данных, п р и к а з ы в а ю:

1. Утвердить Положение об обработке и защите персональных данных в государственном бюджетном общеобразовательном учреждении Краснодарского края школе-интернате спортивного профиля (приложение № 1).

2. Секретарю учебной части Степченковой Анастасии Павловне ознакомить работников государственного бюджетного общеобразовательного учреждения Краснодарского края школы-интерната спортивного профиля с настоящим приказом.

3. Контроль исполнения настоящего приказа возложить на заместителя директора Любичева Игоря Ивановича.

4. Приказ вступает в силу со дня его подписания.

Директор



Н.М. Лесной

УТВЕРЖДЕНО
приказом директора
ГБОУ КК ШИСП
от 20.11.2025 № 252

ПОЛОЖЕНИЕ

об обработке и защите персональных данных
в государственном бюджетном общеобразовательном учреждении
Краснодарского края школе-интернате спортивного профиля
(далее – Положение)

1. Основные понятия

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

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

Безопасность персональных данных – состояние защищенности персональных данных, при котором обеспечиваются конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных субъектов, в том числе их передачи.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение

(обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральным законодательством не распространяется требование соблюдения конфиденциальности.

Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту.

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Распространение персональных данных — действия, направленные на передачу персональных данных субъектов определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных субъектов в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным лиц каким-либо иным способом.

Технические средства информационной системы персональных данных — средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Угрозы безопасности персональных данных — совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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.

2. Общие положения

2.1. Настоящее Положение разработано для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных государственного бюджетного общеобразовательного учреждения Краснодарского края школы-интерната спортивного профиля (далее – Учреждение), защиты прав и свобод граждан при обработке их персональных данных, в том числе право на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2.2. Положение разработано в соответствии со следующими нормативно-правовыми актами Российской Федерации:

- 1) Конституцией Российской Федерации;
- 2) Федеральным законом от 19 декабря 2005 года № 160 «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- 3) Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- 4) Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- 5) Федеральным законом от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;
- 6) Гражданским кодексом Российской Федерации от 30 ноября 1994 года № 51-ФЗ;
- 7) Кодексом об административных правонарушениях Российской Федерации от 30 декабря 2001 года № 195-ФЗ;
- 8) Трудовым кодексом Российской Федерации от 30 декабря 2001 года № 197-ФЗ;
- 9) Уголовным кодексом Российской Федерации от 13 июня 1996 года № 63-ФЗ;
- 10) Указом Президента Российской Федерации от 06 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»;
- 11) Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- 12) Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.5. Персональные данные субъектов являются конфиденциальной информацией, за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации.

2.3. Положение устанавливает порядок обработки персональных данных субъектов Учреждения.

Под обработкой персональных данных понимаются действия (операции) с персональными данными, включающие:

- 1) сбор, хранение, уточнение (обновление, изменение);
- 2) систематизацию, накопление;
- 3) использование, распространение, передачу;
- 4) обезличивание, блокирование, уничтожение.

2.4. Положение определяет необходимый минимальный объем мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.

2.5. Деятельность по организации обработки и защиты персональных данных в соответствии с требованиями законодательства Российской Федерации о персональных данных осуществляет сотрудник учреждения, ответственный за организацию обработки персональных данных.

Деятельность по администрированию средств и механизмов защиты осуществляет сотрудник учреждения, назначенный администратором информационной безопасности учреждения.

Техническое обслуживание информационных систем персональных данных осуществляет сотрудник учреждения, назначенный ответственным за техническое обслуживание информационных систем персональных данных учреждения.

Ответственный за организацию обработки персональных данных, администратор информационной безопасности и ответственный за техническое обслуживание информационных систем персональных данных назначаются приказом директора учреждения.

2.6. На основании договора Учреждение может поручать обработку персональных данных третьим лицам. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных». В поручении, должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечить безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2.7. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, Учреждение

вправе получать и обрабатывать данные о частной жизни сотрудника только с его письменного согласия.

2.8. Учреждение не имеет права получать и обрабатывать персональные данные субъекта о членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законодательством.

2.9. Настоящее Положение вступает в силу с момента его утверждения и действует до замены его новым Положением.

2.10. Все изменения в Положение вносятся приказом директора учреждения.

3. Цель и содержание обработки персональных данных

3.1. Целями обработки персональных данных являются:

- 1) реализация трудовых прав работников, бывших работников;
- 2) осуществление образовательной деятельности;
- 3) исполнение договорных обязательств.

3.2. Обработка персональных данных субъектов Учреждения осуществляются для обеспечения:

- 1) соблюдения законов и иных нормативных правовых актов;
- 2) содействия в трудоустройстве, обучении;
- 3) обеспечения личной безопасности;
- 4) контроля качества и количества выполняемой работы;
- 5) оплаты труда;
- 6) пользования льготами, предусмотренными законодательством РФ и локальными актами Учреждения.

3.3. Цель «реализация трудовых прав работников» достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) члены профсоюза: фамилия, имя, отчество, занимаемая должность, паспортные данные, контактные сведения;

2) работники: фамилия, имя, отчество; пол; гражданство; дата и место рождения; изображение (фотография); паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; данные документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС), сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации, ученой степени, ученого звания; семейное положение, наличие детей, родственные связи; сведения о трудовой деятельности, в том числе наличие поощрений, наград и (или) дисциплинарных взысканий; данные о регистрации брака; сведения о воинском учете; сведения об инвалидности; сведения о судимости, привлечении к уголовной ответственности, ИНН, владение иностранными языками, сведения о доходах, занимаемая должность, реквизиты лицевого счета, сведения об удержании алиментов; иные

персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства Российской Федерации;

3) ближайшие родственники работника: фамилия, имя, отчество, год рождения, степень родства, гражданство, место работы, данные свидетельств о государственной регистрации актов гражданского состояния, занимаемая должность;

4) уволенные (бывшие) работники и их ближайшие родственники: фамилия, имя, отчество; пол; гражданство; дата и место рождения; паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; данные документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС), сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации, ученой степени, ученого звания; семейное положение, наличие детей, родственные связи; сведения о трудовой деятельности, в том числе наличие поощрений, наград и (или) дисциплинарных взысканий; данные о регистрации брака; сведения о воинском учете; сведения об инвалидности; сведения о судимости, привлечении к уголовной ответственности; ИНН; владение иностранными языками; сведения о доходах; занимаемая должность; реквизиты лицевого счета.

3.4. Цель «осуществление образовательной деятельности» достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) обучающиеся (воспитанники): фамилия, имя, отчество; дата и место рождения; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; свидетельство о рождении; изображение (фотография); паспортные данные; пол; гражданство; состав семьи; степень родства; данные документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС); данные полиса ОМС; сведения об инвалидности; данные аттестата об образовании, сведения о состоянии здоровья;

2) родители (законные представители) обучающихся (воспитанников): фамилия, имя, отчество; пол; дата и место рождения; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; паспортные данные; гражданство; степень родства; информация о трудовой деятельности; данные документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС); адрес электронной почты.

3.5. Цель «исполнение договорных обязательств» достигается посредством обработки персональных данных следующих категорий субъектов:

1) контрагенты: фамилия, имя, отчество, пол, дата и место рождения; контактные данные; индивидуальный номер налогоплательщика; данные документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС); занимаемая должность, реквизиты расчетного счета, сумма контракта.

3.6. В Учреждении предусмотрены следующие формы фиксации персональных данных:

1) работники: заявления на налоговые вычеты, индивидуальные сведения по форме 2-НДФЛ, листки нетрудоспособности, копии свидетельства о рождении детей, личная карточка формы Т-2, личные дела сотрудников (заявление о приеме, сведения об образовании, повышении квалификации, профессиональной переподготовке, паспортные данные, сведения, подтверждающие регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС), ИНН, аттестационный лист, трудовой договор и дополнительные соглашения к нему, согласие на обработку персональных данных, согласие на распространение персональных данных, обязательство, справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования, расчетные листы, реестры выплат заработной платы, личные медицинские книжки (санитарные), справка с места учебы, трудовые книжки и (или) сведения о трудовой деятельности работника;

2) ближайшие родственники работника: заявления на налоговые вычеты, копия свидетельства о рождении ребенка, личная карточка по форме Т-2, справка с места учебы;

3) члены профсоюза: заявления о вступлении в профсоюз, заявления от членов профсоюза;

4) обучающиеся (воспитанники): книга выдачи аттестатов за 9 и 11 класс, алфавитная книга обучающихся (воспитанников), журнал вакцинации, заявления от родителей, карта профилактического медицинского осмотра несовершеннолетнего по форме 030-ПО-у-12, классные журналы, личные дела обучающихся (воспитанников), заявление о приеме на обучение, заявление на пребывание обучающегося (воспитанника), заявление родителей или законных представителей о согласии на обработку персональных данных своих и своего ребенка, копия свидетельства о рождении, копия паспорта (обучающегося (воспитанника), родителей), справка о составе семьи, справка о регистрации по месту жительства, договор об образовании на обучение, соглашение на медицинское обслуживание, копия полиса ОМС, медицинская карта, эпидемиологическая справка, копия документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС), фотография, сведения о выпускнике для регистрации в региональной базе ОГЭ, ЕГЭ, анкеты, тесты, аттестат;

5) родители или законные представители обучающихся (воспитанников), заявление родителя или законного представителя о согласии на обработку персональных данных, заявления от родителей или законных представителей, классные журналы, справки о составе семьи;

6) контрагенты: акты выполненных работ, договоры с контрагентами, накладные, счета, счета-фактуры.

4. Порядок обработки персональных данных

4.1. Все персональные данные субъектов Учреждение получает от них самих либо от их законных представителей. Обработка персональных данных осуществляется в соответствии с действующим законодательством РФ на основании согласия субъекта персональных данных.

4.2. Обработка персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации на основании согласия субъекта персональных данных, кроме случаев, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных». Форма согласия утверждается приказом директора Учреждения. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащими персональные данные субъекта (например: анкеты, бланки).

4.3. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе.

4.4. Получение персональных данных субъекта у третьих лиц, возможно только при уведомлении субъекта об этом заранее и с его письменного согласия. Форма согласия утверждается приказом директора Учреждения. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

4.5. Персональные данные субъектов Учреждения обрабатываются в соответствии с исполняемыми функциями.

4.6. Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии с утвержденным списком.

4.7. Доступ к персональным данным, обрабатываемым в информационных системах персональных данных (далее – ИСПДн), осуществляется в соответствии со списком, утвержденным в порядке, определяемом в Учреждении.

4.8. Уполномоченные лица, допущенные к персональным данным субъектов Учреждения, имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностной инструкцией уполномоченных лиц.

4.9. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687.

Персональные данные при такой их обработке, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

4.10. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

4.11. Персональные данные подлежат уничтожению либо обезличиванию в следующих случаях:

1) достижения целей обработки или в случае утраты необходимости в их достижении;

2) отзыва согласия субъекта персональных данных на обработку персональных данных;

3) представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

4) выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя и невозможности обеспечить правомерную обработку персональных данных.

4.12. Хранения материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах.

4.13. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение вносит в них необходимые изменения, а также уведомляет субъекта о внесенных изменениях.

4.14. Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами Российской Федерации.

4.15. Уничтожение персональных данных осуществляется в срок не превышающий 30 рабочих дней с момента отзыва согласия субъекта персональных данных на обработку персональных данных.

4.16. Уничтожение персональных данных осуществляется в срок, не превышающий 7 рабочих дней с момента представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

4.17. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя и невозможности обеспечить правомерную обработку персональных данных уничтожение персональных данных осуществляется в срок, не превышающий 10 рабочих дней с момента выявления неправомерной обработки персональных данных. Решение о неправомерности обработки персональных данных и необходимости уничтожения персональных данных принимает ответственный за организацию обработки персональных данных, который доводит соответствующую информацию до директора Учреждения. Учреждение

уведомляет субъекта персональных данных или его законного представителя об уничтожении персональных данных.

4.18. Уничтожение персональных данных осуществляет комиссия в составе работников, обрабатывавших персональные данные субъекта и установивших необходимость уничтожения персональных данных под контролем председателя комиссии.

4.19. Способ уничтожения материальных носителей персональных данных определяется комиссией.

Допускается применение следующих способов:

- 1) сжигание;
- 2) шредирование (измельчение);
- 3) передача на специализированные полигоны (свалки);
- 4) химическая обработка.

При этом составляется акт, подписываемый председателем комиссии, проводившей уничтожение материальных носителей персональных данных.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия Учреждения должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

4.20. Уничтожение осуществляет комиссия, в состав которой входят лица, ответственные за техническое обслуживание автоматизированных систем, которым принадлежат базы данных.

4.21. Уничтожение достигается путем затирания информации на носителях информации (в том числе и резервных копиях). При этом составляется акт, утверждаемый лицом, ответственным за техническое обслуживание автоматизированных систем, которому принадлежат базы данных.

4.22. Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами.

4.23. При отсутствии технической возможности осуществлять уничтожение персональных данных, содержащихся в базах данных допускается проведение обезличивания путем перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта персональных данных была невозможна.

4.24. Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных.

4.25. Обработка биометрических персональных данных (фотография, используемая для идентификации, отпечатки пальцев, изображение сетчатки глаза и т.д.), в соответствии со статьей 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», допускается при наличии согласия

субъекта. Форма согласия утверждается приказом директора Учреждения. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

4.26. Решение порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

4.27. Работники должны быть ознакомлены под подпись с настоящим Положением и другими документами Учреждения, устанавливающие порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

5. Правила работы с обезличенными данными

5.1. Порядок обезличивания включает в себя замену идентифицирующей информации о субъекте (например: фамилию, имя отчество) на произвольный код (далее – идентификатор).

5.2. Обезличивание должно проводиться таким образом, чтобы определить принадлежность персональных данных конкретному субъекту персональных данных было невозможно без использования дополнительной информации.

5.3. В случае, если обезличенные персональные данные используются в статистических или иных исследовательских целях, сроки обработки и хранения персональных данных устанавливаются директором Учреждения исходя из служебной необходимости, и получение согласия на обработку его персональных данных не требуется на основании пункта 9 части первой статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

5.4. Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности обезличенных персональных данных в информационных системах и целесообразность их применения определяются ответственным за организацию обработки персональных данных Учреждения индивидуально для каждой информационной системы персональных данных.

6. Передача персональных данных третьим лицам

6.1. При обработке персональных данных субъекта должны соблюдаться следующие требования:

1) не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта;

2) предупреждать лиц, получающих персональные данные 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 персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных.

6.2. При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, Учреждение запрашивает согласие субъекта персональных данных в письменной форме. Форма согласия утверждается приказом директора Учреждения. Допускается совмещение формы согласия субъекта с типовой формой документов, содержащих персональные данные субъекта (например: анкеты). Допускается совмещение формы согласия субъекта с другими формами согласий.

7. Права субъектов персональных данных

7.1. В целях обеспечения своих интересов, субъекты имеют право:

1) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

2) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

3) требовать исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». Субъект при отказе Учреждения исключить или исправить персональные данные субъекта имеет право заявлять в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

4) требовать от Учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;

5) обжаловать в суд любые неправомерные действия или бездействие Учреждения при обработке и защите персональных данных субъекта.

8. Порядок обработки обращений и запросов субъектов

8.1. При обращении либо письменном запросе субъекта персональных данных или его законного представителя, на доступ к своим персональным данным Учреждение руководствуется требованиями статей 14, 18 и 20 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

8.2. Доступ субъекта персональных данных или его законного представителя к своим персональным данным Учреждение предоставляет только под

контролем ответственного за организацию обработки персональных данных Учреждения.

8.3. Обращение субъекта персональных данных или его законного представителя фиксируется в журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных.

8.4. Письменный запрос субъекта персональных данных или его законного представителя фиксируются в журнале регистрации письменных запросов граждан на доступ к своим персональным данным.

8.5. Ответственный за организацию обработки персональных данных принимает решение о предоставлении доступа субъекта к персональным данным.

8.6. В случае, если данных предоставленных субъектом недостаточно для установления его личности или предоставление персональных данных нарушает конституционные права и свободы других лиц, ответственный за организацию обработки персональных данных подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» или иного федерального закона, являющегося основанием для такого отказа, в срок, не превышающий 30 рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо от даты получения запроса субъекта персональных данных или его законного представителя.

8.7. Для предоставления доступа субъекта персональных данных или его законного представителя к персональным данным субъекта ответственный за организацию обработки персональных данных привлекает работника (работников), обрабатывающего персональные данные субъекта.

8.8. Сведения о наличии персональных данных Учреждения предоставляет субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Контроль предоставления сведений субъекту или его законному представителю осуществляет ответственный за организацию обработки персональных данных.

8.9. Сведения о наличии персональных данных должны быть предоставлены субъекту при ответе на запрос в течение 30 дней от даты получения запроса субъекта персональных данных или его законного представителя.

9. Порядок действий в случае запросов надзорных органов

9.1. В соответствии с частью 4 статьи 20 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» Учреждение сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 30 дней с даты получения такого запроса.

9.2. Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки

персональных данных при необходимости с привлечением работников Учреждения.

9.3. В течение установленного законодательством срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

10. Защита персональных данных субъекта

10.1. Защиту персональных данных субъектов от неправомерного их использования или утраты Учреждение обеспечивает за счет собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

1) РД ФСТЭК России – «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года;

2) специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 года № 282;

3) внутренними документами Учреждения, действующими в сфере обеспечения информационной безопасности.

10.2. Защита персональных данных предусматривает ограничение к ним доступа.

10.3. Руководящий состав Учреждения, осуществляющий обработку персональных данных:

1) несет ответственность за организацию защиты персональных данных в подчиненном подразделении;

2) закрепляет за работниками, уполномоченными обрабатывать персональные данные, конкретные материальные носители, на которых допускается хранение персональных данных в случае, если такие носители необходимы для выполнения возложенных на работников функций;

3) организывает изучение подчиненными работниками, в чьи обязанности входит обработка персональных данных, нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

4) обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в подразделении;

5) организывает контроль доступа к персональным данным в соответствии с функциональными обязанностями работников подразделения.

10.4. Работники, допущенные к персональным данным, дают письменное обязательство о неразглашении таких данных в установленном порядке.

11. Обязанности лиц, допущенных к обработке персональных данных

11.1. Лица, допущенные к работе с персональными данными, обязаны:

- 1) знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы Учреждения по защите персональных данных;
- 2) сохранять конфиденциальность персональных данных;
- 3) обеспечивать сохранность закрепленных за ними носителей персональных данных;
- 4) контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;
- 5) докладывать своему непосредственному руководителю, руководителю подразделения обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

12. Порядок организации системы видеонаблюдения

12.1. Решение об установке системы видеонаблюдения принимается директором Учреждения, видеоконтроль вводится соответствующим приказом.

12.2. Лица, являющиеся работниками Учреждения на момент введения системы видеоконтроля, должны в письменной форме выразить свое согласие или несогласие на введение данной системы (заполнение согласия на осуществление наблюдения).

12.3. Работники, вновь принимаемые на работу, выражают свое согласие на проведение видеоконтроля путем заполнения формы согласия на осуществление видеонаблюдения.

12.4. Посетители Учреждения информируются о системе видеоконтроля путем размещения специальных информационных табличек в зонах видимости видеокамер.

12.5. Система видеонаблюдения Учреждения входит в систему контроля доступа и включает в себя ряд устройств: камеры, мониторы, записывающие устройства.

12.6. Места установки видеокамер в Учреждении определяются по мере необходимости в соответствии с конкретными задачами.

12.7. Видеокамеры устанавливаются в местах, открытых для общего доступа (территория, входы в здание, коридоры).

12.8. Установка видеокамер не допускается в туалетных комнатах, в спальнях, обучающихся (воспитанников), и в иных местах, связанных с осуществлением личных нужд работников, обучающихся (воспитанников), посетителей.

12.9. Запрещается использование устройств, предназначенных для негласного получения информации (скрытых камер).

13. Ответственность работника за нарушение норм, регулирующих обработку и защиту персональных данных субъектов

13.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности.

13.2. К данным лицам могут быть применены следующие дисциплинарные взыскания:

- 1) замечание;
- 2) выговор;
- 3) увольнение.

13.3. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.