

Утверждаю
Директор ГКОУ Самарской области
"Учебно-методический центр по ГО и ЧС"
С.А. Дьяков
«30» декабря 2022 г.

ПОЛИТИКА

**обработке и защиты персональных данных работников и слушателей
государственном казённом образовательном учреждении дополнительного
профессионального образования «Учебно-методический центр по гражданской
обороне и чрезвычайным ситуациям Самарской области»**

**Обработка и защита персональных данных работников
ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС»**

1. Общие положения

1.1. Настоящее Положение о защите персональных данных (далее - Положение) разработано на основании: Конституции РФ; главы 14 Трудового Кодекса РФ; Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»; Федерального Закона РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. № 149-ФЗ; постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Заместителем директора ФСТЭК России от 15.02.2008 г.; «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

1.2. Настоящее Положение определяет Политику ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» (далее – Учреждение) в отношении персональных данных работников Учреждения в порядке, установленном Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников Учреждения.

1.4. Настоящее Положение определяет:

-порядок обработки персональных данных работников (субъекта персональных данных);

-гарантии конфиденциальности сведений, предоставляемых работником работодателю.

1.5. При определении объема и содержания, обрабатываемых персональных данных работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом и иными Федеральными законами.

1.6. Персональные данные относятся к конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения.

1.7. Настоящее Положение вступает в силу с момента его утверждения директором Учреждения и действует бессрочно, до замены его новым Положением.

2. Понятие и состав персональных данных

2.1. В настоящем Положении используются следующие основные термины и определения:

– **персональные данные** - любая информация, прямо или косвенно относящаяся к субъекту персональных данных - определенному или определяемому физическому лицу;

– **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

– **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

– **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц или ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.;

– **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

– **общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

– **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

– **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

– **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

– **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.2. Состав персональных данных работника:

- фамилия, имя, отчество;
- пол, возраст;
- анкета;
- автобиография;
- образование;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- размер заработной платы;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные карточки, трудовые книжки и сведения о трудовой деятельности;
- дела, содержащие материалы по повышению квалификации и переподготовке, аттестации, служебным расследованиям;

- копии отчетов, направляемые в органы статистики;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным работника;
- рекомендации, характеристики;
- семейное положение, наличие детей, родственные связи;
- финансовое положение (доходы, долги, владение недвижимым имуществом, денежные вклады и др.);
- деловые и иные личные качества, которые носят оценочный характер;
- прочие сведения, которые могут идентифицировать человека.

2.3. Персональные данные работника содержатся в основном документе персонального учета работников - личной карточке по унифицированной форме. № Т-2

Личная карточка включает в себя:

- фамилию, имя, отчество, пол, дату и место работы, семейное положение, паспортные данные, адрес места жительства, телефон,
- копии документов об образовании;
- выписки (копии) из документов о присвоении почетных званий, ученой степени, награждении государственными наградами;
- аттестационные листы;
- копию свидетельства ИНН;
- копию страхового свидетельства пенсионного страхования;
- копии документов по организации воинского учета;
- другие документы, нахождение которых в личном деле будут признаны целесообразными.

3. Цели и задачи

3.1. Основными целями и задачами Положения являются:

- определение порядка обработки (приема, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, учета) персональных данных работников Учреждения.
- обеспечение защиты прав и свобод работников Учреждения при обработке их персональных данных с использованием средств автоматизации или без использования таких средств, а также устанавливает ответственность лиц, имеющих доступ к персональным данным, за невыполнение требований, регулирующих обработку и защиту персональных данных;
- прогнозирование, своевременное выявление и устранение угроз объектам информационной безопасности на основе правовых, организационных мер и средств обеспечения защиты;
- минимизация ущерба и быстрее восстановление программных и аппаратных средств, информации, пострадавших в результате кризисных ситуаций, расследование причин возникновения таких ситуаций и принятие соответствующих мер по их предотвращению.

4. Пользователи ИСПДн

В ИСПДн Учреждения можно выделить следующие группы пользователей, участвующих в обработке персональных данных:

- администратор безопасности ИСПДн;
- администратор ИСПДн;
- оператор АРМ.

4.1. Администратор безопасности ИСПДн.

Администратор безопасности, работник ответственный за функционирование системы защиты персональных данных, включая обслуживание и настройку административной, серверной и клиентской компонент (Приложение №1).

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты.

4.2. Администратор ИСПДн.

Администратор ИСПДн, работник ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (оператора АРМ) к элементам, хранящим персональные данные (Приложение №2).

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

4.3. Оператор АРМ.

Оператор АРМ - работник, осуществляющий обработку персональных данных (Приложение №3).

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к персональным данным;
- располагает конфиденциальными данными, к которым имеет доступ.

5. Сбор Персональных данных

5.1. Персональные данные следует получать непосредственно у работника. Если Персональные данные возможно получить только у третьей стороны, работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Учреждение должно сообщить работнику о целях, предполагаемых источниках и способах получения Персональных данных, а также о характере подлежащих получению Персональных данных и последствиях отказа работника дать письменное согласие на их получение (п.3 ст.86 ТК РФ).

5.2. Работники и их представители должны быть ознакомлены под роспись с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

5.3. При принятии решений, затрагивающих интересы работника, Работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

6. Обработка и хранение Персональных данных

6.1. Персональные данные работников Учреждения создаются путём внесения сведений на бумажные и электронные носители.

6.2. Основы организации обработки персональных данных работников в Учреждении (принципы, правовые основы, права и обязанности субъектов персональных данных).

6.2.2. Принципы обработки персональных данных:

- законность целей и способов обработки персональных данных;
- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Учреждения;

- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

- достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

- недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем, содержащих персональные данные.

6.2.3. В отношениях по обработке персональных данных субъекты персональных данных имеют право:

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

- знакомиться со сведениями, содержащими свои персональные данные, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;

- выбирать представителей для защиты своих персональных данных;

- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением федерального закона; при отказе оператора исключить или исправить персональные данные субъект персональных данных имеет право заявить об этом в письменной форме директору Учреждения;

- обжаловать в уполномоченном органе по защите прав субъектов персональных данных или в суде любые неправомерные действия или бездействие руководства Учреждения при обработке его персональных данных.

6.2.4. При обращении субъекта персональных данных или его законного представителя по вопросам предоставления информации о персональных данных, относящихся к соответствующему субъекту, Учреждение обязано сообщить данному субъекту информацию о наличии персональных данных, предоставить возможность ознакомления с ней.

6.2.5. В отношениях, связанных с обработкой персональных данных, субъекты персональных данных обязаны лично или через своего законного представителя:

- передавать Учреждению достоверные персональные данные, которые установлены настоящим Положением;

- своевременно сообщать Учреждению об изменении своих персональных данных, либо предоставить соответствующие документы.

6.3. Сроки обработки персональных данных.

6.3.1. Обработка персональных данных начинается с момента их получения Учреждением и заканчивается:

- по достижении заранее заявленных целей обработки;
- по факту утраты необходимости в достижении заранее заявленных целей обработки;
- в сроки, предусмотренные законодательством РФ.

6.3.2. Учреждение осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

6.4. Условия обработки персональных данных.

6.4.1. Общим условием обработки персональных данных является наличие письменного согласия субъектов персональных данных на осуществление такой обработки.

Письменное согласие на обработку персональных данных берется с каждого работника Учреждения.

6.4.2. Обработка персональных данных субъекта персональных данных без получения его согласия осуществляется в следующих случаях:

- при поступлении официальных запросов (письменного запроса на бланке организации с печатью и росписью руководителя) из надзорно-контрольных или правоохранительных органов (суд, органы прокуратуры, ФСБ, МВД и т.п.);
- при непосредственном обращении сотрудников правоохранительных или надзорно-контрольных органов при предъявлении ими служебного удостоверения и соответствующих документов о получении персональных данных (запрос, постановление и т.п.), а также в иных случаях, предусмотренных федеральным законом;
- для статистических целей при условии обязательного обезличивания персональных данных;
- для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- при регистрации и отправки корреспонденции почтовой связью.

6.4.3. Учреждение не имеет права получать и обрабатывать персональные данные работников об их политических, религиозных и иных убеждениях и частной жизни, а равно об их членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

6.4.4. Обработка персональных данных осуществляется только должностными лицами (операторами) ответственными за обработку персональных данных, непосредственно использующими их в служебных целях.

Все работники Учреждения имеют право на полную информацию, касающуюся только собственных персональных данных.

6.5. Уточнение, блокирование и уничтожение персональных данных.

6.5.1. Уточнение персональных данных, в том числе их обновление и изменение, имеет своей целью обеспечение достоверности, полноты и актуальности персональных данных, обрабатываемых Учреждением.

6.5.2. Уточнение персональных данных осуществляется Учреждением по собственной инициативе, по требованию субъекта персональных данных или его законного представителя, по требованию уполномоченного органа по защите прав субъектов персональных данных в случае, когда установлено, что персональные данные

являются неполными, устаревшими, недостоверными. Об уточнении персональных данных Учреждение обязан уведомить субъекта персональных данных или его законного представителя.

6.5.3. Блокирование персональных данных осуществляется Учреждением по требованию субъекта персональных данных или его законного представителя, а также по требованию уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними. О блокировании персональных данных Учреждение обязан уведомить субъекта персональных данных или его законного представителя.

6.5.4. Уничтожение персональных данных осуществляется:

- по достижении цели обработки персональных данных;
- в случае утраты необходимости в достижении целей обработки персональных данных;

- по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных в случае выявления фактов совершения Учреждением неправомерных действий с персональными данными, когда устранить соответствующие нарушения не представляется возможным.

6.5.5. В целях обеспечения законности при обработке персональных данных и устранения факторов, влекущих или могущих повлечь неправомерные действия с персональными данными, Учреждение вправе по собственной инициативе осуществить блокирование и (или) уничтожение персональных данных.

6.5.6. В ИСПДн Учреждения можно выделить следующие группы пользователей, участвующих в обработке персональных данных слушателей:

- Администратор безопасности ИСПДн;
- Администратор ИСПДн;
- Оператор АРМ.

7. Доступ к персональным данным

7.1. Внутренний доступ.

Право доступа к персональным данным работника имеют:

- директор Учреждения;
- заместители директора;
- специалист по кадрам;
- ведущий экономист;
- сам работник;
- другие работники Учреждения, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей, и в том объеме, который необходим для исполнения трудовых обязанностей;

- в целях выполнения порученного задания и на основании служебной записки с положительной резолюцией директора Учреждения, доступ к персональным данным работника может быть предоставлен иному работнику, должность которого не включена в Перечень должностей работников, имеющих доступ к персональным данным, и которым они необходимы в связи с выполнением трудовых обязанностей.

Перечень работников, имеющих доступ к персональным данным работников Учреждения, утвержден в Приложении № 5.

При работе с персональными данными работник подписывает обязательство о соблюдении режима конфиденциальности персональных данных работника (Приложение № 6).

7.2. Внешний доступ.

Персональные данные могут быть предоставлены органам государственной власти в порядке, установленном законодательством РФ:

- инспекции труда;
- правоохранительные органы;
- налоговые инспекции;
- органы статистики;
- страховые агентства;
- военные комиссариаты;
- пенсионные фонды;
- органы социального страхования.

Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции, в порядке, установленном законодательством РФ.

7.3. Сведения о работающем или уже уволенном работнике могут быть предоставлены сторонней организации только с письменного запроса на бланке организации с согласия работника.

7.4. Персональные данные работника могут быть представлены родственникам или членам его семьи только с письменного разрешения самого работника. В случае развода и отсутствия соглашения сторон об уплате алиментов справка о заработной плате работника может быть представлена в суд без его согласия на основании письменного запроса и опережения суда.

7.5. Письменное согласие работника на обработку персональных данных, разрешенных для распространения, оформляется отдельно от других согласий на обработку его персональных данных. При этом соблюдаются условия, предусмотренные, в частности, ст. 10.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных". Требования к содержанию такого согласия устанавливаются уполномоченным органом по защите прав субъектов персональных данных (Приложение № 7).

7.6. Согласие на обработку персональных данных, разрешенных для распространения, работник предоставляет Работодателю:

- непосредственно;
- с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

7.7. Работодатель обязан не позднее трех рабочих дней с момента получения указанного согласия опубликовать информацию об условиях обработки, о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных для распространения.

7.8. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес), а также перечень персональных данных, обработка которых подлежит прекращению.

7.9. Согласие на обработку персональных данных, разрешенных для распространения, прекращает свое действие с момента поступления Работодателю требования Работника, указанного в п.7.8 настоящего положения.

7.10. Доступ к информационным системам, содержащим Персональные данные, должен быть защищен паролями (Приложение №8).

8. Передача Персональных данных Субъекта

8.1. Передача персональных данных субъекта производится после подписания им Соглашения на передачу его персональных данных третьей стороне (приложение № 8).

8.2. При передаче персональных данных Учреждение должно соблюдать следующие требования:

– не передавать персональные данные третьей стороне без письменного согласия Субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта;

– предупредить 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 соблюдения правил обработки и хранения персональных данных. Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными в порядке, установленном законодательством РФ;

– осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым работник должен быть ознакомлен под роспись.

До начала осуществления трансграничной передачи персональных данных оператор персональных данных обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

9. Безопасность персональных данных

9.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

9.2. При обработке персональных данных, ответственное лицо обязано принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

9.3. Администратор ИСПДн для защиты информационных систем Учреждения от разрушающего воздействия компьютерных вирусов в работе руководствуется Инструкцией по антивирусной защите (Приложение № 9).

9.4. В целях предупреждения нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечения безопасности информации в процессе управленческой деятельности Учреждения устанавливается Комплекс мер по защите персональных данных.

Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности Персональных данных и обеспечивает безопасность информации в процессе управленческой деятельности Учреждения.

Комплекс мер включает в себя:

Внутренняя защита.

Регламентация доступа к конфиденциальным сведениям Учреждения, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий.

Для защиты персональных данных Субъекта Учреждение обязано соблюдать следующие меры безопасности:

– ограничивать и регламентировать состав Работников Учреждения, функциональные обязанности которых требуют доступа к персональным данным;

– избирательно и обосновано распределять документы и информацию между работниками Учреждения;

– рационально размещать рабочие места работников, при котором исключается бесконтрольное использование конфиденциальной информации;

- организовать необходимые условия в помещении для работы с конфиденциальными документами и базами данных;
- регламентировать порядок уничтожения информации;
- выявлять нарушения доступа к персональным данным;
- проводить работы по предупреждению утраты сведений при работе с персональными данными;
- защищать персональные компьютеры паролями доступа.

Внешняя защита.

Для защиты Персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение информацией. Под посторонним лицом понимается любое лицо, не имеющее санкционированного доступа к персональным данным, в том числе непосредственного отношения к деятельности Учреждения, посетители, работники других организаций и иные лица.

Для защиты персональных данных Субъектов необходимо соблюдать:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим Учреждения;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и беседах.

Лица, не являющиеся работниками Учреждения не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в организации.

В отдельных случаях возможно предоставление доступа к персональным данным для третьих лиц, осуществляющих внедрение, сопровождение и аудит процессов в Учреждении, при условии, что с ними заключено Соглашение о конфиденциальности.

10. Права и обязанности

10.1. Обязанности Учреждения при обработке персональных данных.

10.1.1. При обработке персональных данных Работодатель обязан соблюдать следующие требования:

- защита персональных данных от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет его средств и в порядке, установленном действующим законодательством РФ;
- субъекты организации должны быть ознакомлены под расписку с документами Учреждения, устанавливающими порядок обработки Персональных данных, а также об их правах и обязанностях в этой области.

10.1.2. Работодатель не имеет право:

- получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст.24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия (п.4 ст.86 ТК РФ);
- получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом (п.5. ст.86 ТК РФ);
- получать и обрабатывать информацию о национальной принадлежности работника (ст.26 Конституции РФ).

10.2. Права и обязанности Работника в области защиты персональных данных.

10.2.1. Субъект обязан:

- передавать Учреждению достоверные, документированные персональные данные, состав которых установлен нормативно-правовыми актами РФ;

-при изменении персональных данных Субъект уведомляет Учреждение о таких изменениях в 10-дневный срок.

Обязанности Субъекта фиксируются в письменном виде в тексте Согласия на обработку персональных данных, которое он подписывает при приеме на работу.

10.2.2. Субъект в целях обеспечения защиты персональных данных, хранящихся в Учреждении, имеет право на:

– свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством РФ;

– исключение или исправление неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства РФ;

– персональные данные оценочного характера Субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

– требование об извещении Учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях и дополнениях;

– отзыв согласия на обработку персональных данных;

– обжалование в суде любых неправомерных действий или бездействия Учреждения при обработке и защите его персональных данных.

– получение от Учреждения сведений о том, какие юридические последствия может повлечь за собой обработка его персональных данных.

11. Ответственность

11.1. Все лица, непосредственно имеющие отношение к персональной базе данных, должны подписывать обязательство о неразглашении персональной информации работников.

11.2. Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

11.3. Каждый работник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Заместитель директора по учебной работе



А.А. Варламов

Оператор персональных данных работника:
ГКОУ Самарской области
«Учебно-методический центр по ГО и ЧС»

Адрес оператора:
инд.443099, г. Самара
ул. Комсомольская, 18

**Согласие
на обработку персональных данных
(образец)**

Я, _____,
Паспорт серия _____ номер _____, кем и когда выдан _____,
_____, зарегистрированный (ая)
по адресу: _____,

_____, согласен(а) на обработку предоставленных мной в процессе работы в ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» персональных данных (ФИО, дата и место рождения, сведения о гражданстве, паспортные данные, сведения об образовании, сведения о воинской обязанности, сведения о социальных льготах, адрес фактического места жительства, адрес по прописке, номера личных телефонов, контактная информация, фотографии, информация о трудовой деятельности, информация о страховом пенсионном свидетельстве, информация о идентификационном номере налогоплательщика, и т.п.) и внесение их в базу данных бухгалтерии и кадровой службы.

Я согласен(а) на включение нижеперечисленных сведений в общедоступный источник персональных данных ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» (корпоративный справочник Учреждения):

- 1.Фамилия, имя, отчество;
- 2.Должность;
- 3.Контактный телефон (рабочий, домашний, сотовый).

Я согласен(а) на размещение моей фотографии, фамилии, имени, отчества, занимаемой должности, информации по награждениям, информации о воинском звании на информационном стенде, интернет-сайте ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС»

Я предоставляю ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

Я проинформирован(а), что ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» будет обрабатывать персональные данные как неавтоматизированным, так и автоматизированным способом обработки.

Я проинформирован(а), что под обработкой персональных данных понимаются действия (операции) с персональными данными в рамках выполнения Федерального закона от 27.07.2006 № 152-ФЗ, а конфиденциальность персональных данных соблюдается ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» в соответствии с требованиями законодательства Российской Федерации.

Данное согласие действует на период работы в ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС»

и хранится в личном деле работника.

Я проинформирован(а) о том, что настоящее согласие может быть отозвано мной в письменной форме в любое время.

Дата « ____ » _____ 202__ г. Подпись _____

Директору ГКОУ Самарской области
«Учебно-методический центр по ГО и ЧС»
Дьякову С.А.

от _____,
зарегистрированной (ого) по адресу:

паспорт серия _____ № _____
выдан _____

**Обязательство
о соблюдении режима конфиденциальности
персональных данных работника
(образец)**

Я, _____,
занимая должность _____ даю обязательство:

1. Не разглашать и не передавать третьим лицам, не раскрывать публично сведения, составляющие персональные данные работников, которые мне будут доверены или станут известны по работе.

2. Выполнять относящиеся ко мне требования Положения о защите персональных данных работников, приказов, распоряжений, инструкций и других локальных нормативных актов по обеспечению режима конфиденциальности персональных данных работников и соблюдению правил их обработки.

3. В случае попытки посторонних лиц получить от меня сведения, составляющие персональные данные работника, немедленно сообщить руководителю структурного подразделения и директору Учреждения.

4. В случае моего увольнения все носители, содержащие персональные данные работников (документы, копии документов, дискеты, диски, распечатки на принтерах, черновики и пр.), которые находились в моем распоряжении в связи с выполнением мною трудовых обязанностей во время работы у работодателя, передать руководителю структурного подразделения или другому работнику по указанию руководителя структурного подразделения.

5. Об утрате или недостатке документов или иных носителей, содержащих персональные данные работников, удостоверений, ключей от помещений и сейфов (металлических шкафов) и о других фактах, которые могут привести к разглашению персональных данных работников, а также о причинах и условиях возможной утечки сведений немедленно сообщить руководителю структурного подразделения и директору Учреждения.

Я ознакомлен под роспись с Положением о защите персональных данных работников, приказами, распоряжениями, инструкциями и другими локальными нормативными актами по обеспечению режима конфиденциальности персональных данных работников и соблюдению правил их обработки.

Мне известно, что нарушение мною обязанностей по защите персональных данных работников может повлечь дисциплинарную, гражданско-правовую, уголовную и иную ответственность в соответствии с законодательством РФ.

Дата « ____ » _____ 202__ г. Подпись _____

Оператор персональных данных работника:
ГКОУ Самарской области
«Учебно-методический центр по ГО и ЧС»

Адрес оператора:
инд.443099, г. Самара
ул. Комсомольская, 18

**Согласие работника
на передачу его персональных данных третьей стороне
(образец)**

Я, _____,
Паспорт серия _____ номер _____, кем и когда выдан _____,
_____ зарегистрированный (ая)
по адресу: _____

_____ согласен(а), что мои персональные данные (ФИО, дата и место рождения, сведения о гражданстве, паспортные данные, сведения о воинской обязанности, сведения о месте работы, сведения о социальных льготах, адрес фактического места жительства, адрес по прописке, номера личных телефонов, информация об образовании, информация о трудовой деятельности, информация о страховом пенсионном свидетельстве, информация о идентификационном номере налогоплательщика, свидетельства о рождении детей, информация о индивидуальных сведениях о начисленных и уплаченных страховых взносах на обязательное пенсионное страхование, справка 2 НДФЛ) будут передаваться представителям Министерства финансов Самарской области, Министерства образования Самарской области, кредитных организаций, осуществляющих обслуживание в рамках зарплатного проекта, органов налоговой инспекции РФ по месту нахождения организации, социального фонда России, военных комиссариатов г. Самара в целях обеспечения исполнения ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» своих обязанностей, обязательств определенных законодательством РФ.

Я проинформирован(а), что ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» будет обрабатывать персональные данные как неавтоматизированным, так и автоматизированным способом обработки.

Я проинформирован(а), что под обработкой персональных данных понимаются действия (операции) с персональными данными в рамках выполнения Федерального закона от 27.07.2006 № 152-ФЗ, а конфиденциальность персональных данных соблюдается ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» в соответствии с требованиями законодательства Российской Федерации.

Данное согласие действует на период работы в ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» и хранится в личном деле работника.

Я проинформирован(а) о том, что настоящее согласие может быть отозвано мной в письменной форме в любое время.

Дата « ____ » _____ 202 ____ г.

Подпись _____

Директору ГКОУ Самарской области «Учебно-методический Учреждение по ГО и ЧС»
 Адрес местонахождения: 443099, г. Самара, ул. Комсомольская, 18
 ОГРН 1026301421178, ИНН 6317026305, КПП 631701001 БИК 013601205

от _____ (Ф.И.О.)

Паспорт серия _____ № _____
 кем выдан, дата выдачи _____

зарегистрированного по адресу: _____

Адрес электронной почты: _____

Телефон: _____

**Согласие на обработку персональных данных,
 разрешенных субъектом персональных данных для распространения
 (образец)**

Настоящим я, _____, руководствуясь статьей 10.1 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных», заявляю о согласии на распространение ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» моих персональных данных с целью размещения информации обо мне на официальном сайте, информационном табло, на стендах Учреждения, слайдах «Инструктаж слушателей», в следующем порядке:

Категория персональных данных	II Перечень персональных данных	Разрешаю к распространению (да/нет) подчеркнуть	Разрешаю к распространению неограниченному кругу лиц (да/нет) подчеркнуть	Условия и запреты	Дополнительные условия
Общие персональные данные	Фамилия	Да / Нет	Да / Нет		
	Имя	Да / Нет	Да / Нет		
	Отчество	Да / Нет	Да / Нет		
	Год рождения	Да / Нет	Да / Нет		
	Месяц рождения	Да / Нет	Да / Нет		
	Дата рождения	Да / Нет	Да / Нет		
	Место рождения	Да / Нет	Да / Нет		
	Семейное положение	Да / Нет	Да / Нет		
	Образование	Да / Нет	Да / Нет		
	Профессия	Да / Нет	Да / Нет		
Специальные категории персональных данных	Сведения о состоянии здоровья	Да / Нет	Да / Нет		

Категория персональных данных	II Перечень персональных данных	Разрешаю к распространению (да/нет) подчеркнуть	Разрешаю к распространению неограниченному кругу лиц (да/нет) подчеркнуть	Условия и запреты	Дополнительные условия
	Сведения о судимости	Да / Нет	Да / Нет		
Биометрические персональные данные	фотографическое изображение лица	Да / Нет	Да / Нет		
	Видеозапись с изображением лица	Да / Нет	Да / Нет		

Сведения об информационных ресурсах, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
Сайт Учреждения: УМЦСАМАРА.РФ	Предоставление сведений неограниченному кругу лиц
Информационное табло	Предоставление сведений сотрудникам и слушателям Учреждения
Информационные стенды	Предоставление сведений сотрудникам и слушателям Учреждения
Слайд «Инструктаж слушателей»	Предоставление сведений сотрудникам и слушателям Учреждения

Настоящее согласие дано мною добровольно и действует с «___» _____ 202__года по «31» декабря 2026 года.

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования Оператор обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

Дата «___» _____ 2023 года.

Подпись _____

Инструкция по организации парольной защиты

Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на Администратора безопасности информационной системы персональных данных (далее – ИСПДн).

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее установленной (обычно 6-8 символов);
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в заданном числе (например, в 6-ти) позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора безопасности ИСПДн.

Для генерации "стойких" значений паролей могут применяться специальные программные средства.

Система централизованной генерации и распределения паролей должна исключать возможность ознакомления Администратора безопасности ИСПДн, а также работников Учреждения с паролями других работников Учреждения.

При наличии технологической необходимости использования имен и паролей некоторых работников в их отсутствие (например, в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.), такие работники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение Администратору безопасности ИСПДн.

Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе.

Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать Администратора безопасности ИСПДн.

Полная плановая смена паролей пользователей должна проводиться регулярно, например, не реже одного раза в месяц.

Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться Администратором безопасности ИСПДн в соответствии с «Инструкцией по внесению изменений в списки пользователей АС и наделению их полномочиями доступа к ресурсам системы» немедленно после окончания последнего сеанса работы данного пользователя с системой.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) Администратора безопасности ИСПДн и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры по внеплановой смене паролей (в зависимости от полномочий владельца скомпрометированного пароля).

Хранение работником Учреждения значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у Администратора безопасности ИСПДн (возможно вместе с персональными ключевыми дискетами и идентификатором TouchMemory).

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора безопасности ИСПДн.

Заместитель директора по учебной работе



А.А. Варламов

Инструкция по организации антивирусной защиты

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты Учреждения от разрушающего воздействия компьютерных вирусов и устанавливает ответственность работников Учреждения, эксплуатирующих и сопровождающих АС, за их выполнение.

1.2. К использованию в Учреждении допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.3. Установка и настройка средств антивирусного контроля на компьютерах на серверах и рабочих станциях АС осуществляется работником сектора информационного обеспечения.

2. Применение средств антивирусного контроля

2.1. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD - ROM и т.п.).

2.3. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля.

2.4. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

2.6. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.7. Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации».

2.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка:

- на защищаемых серверах и РС - ответственным за обеспечение информационной безопасности подразделения;

- на других серверах и РС АС не требующих защиты, - лицом, установившим (изменившим) программное обеспечение, - в присутствии и под контролем руководителя данного подразделения или работника, им уполномоченного.

2.9. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале Учреждения за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

3. Действия при обнаружении вирусов

3.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник обязан приостановить работу и сообщить об этом Администратору безопасности ИСПДн.

3.2. Администратора безопасности ИСПДн должен:

- провести внеочередной антивирусный контроль. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники Учреждения обязаны:

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов смежные структурные подразделения, использующие эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов;

- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, отправить его в организацию, с которой заключен договор на антивирусную поддержку;

- по факту обнаружения зараженных вирусом файлов составить служебную записку заместителю директора Учреждения, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

4. Ответственность

4.1. Ответственность за организацию антивирусного контроля в Учреждении, в соответствии с требованиями настоящей Инструкции, возлагается на Администратора безопасности ИСПДн.

4.2. Ответственность за проведение мероприятий антивирусного контроля в Учреждении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности информации и всех работников Учреждения, являющихся пользователями, АС.

4.3. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции работниками Учреждения осуществляется Администратором безопасности ИСПДн.

Заместитель директора по учебной работе



А.А. Варламов

**Обработка и защита персональных данных слушателей
ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС»**

1. Общие положения

1.1. Настоящее Положение определяет порядок обработки (получения, использования, хранения, уточнения (обновления, изменения), распространения (в том числе передачи), обезличивания, блокирования, уничтожения, защиты) персональных данных слушателей ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» (далее - Учреждение).

1.2. Настоящее Положение определяет политику Учреждения в отношении персональных данных слушателей в порядке, установленном Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Настоящее Положение разработано на основании: Конституции Российской Федерации, Гражданского кодекса Российской Федерации, Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», Приказа Федеральной службы по техническому и экспортному контролю от 05.02.2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», Письма Рособразования от 29.07.2009 г. № 17-110 «Об обеспечении защиты персональных данных».

1.4. Настоящее Положение определяет:

- порядок обработки персональных данных слушателей Учреждения (субъект персональных данных);
- гарантии конфиденциальности сведений, предоставляемых слушателем Учреждения.

1.5. Настоящее положение и изменения к нему утверждаются по решению директора Учреждения и вводятся в действие приказом директора Учреждения.

2. Основные понятия

В настоящем Положении используются следующие понятия и термины:

слушатели - повышающие квалификацию в Учреждении;

субъекты персональных данных - слушатели Учреждения;

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, адрес, образование, профессия, другая информация, необходимая Учреждению в связи с организацией образовательного процесса;

оператор - Учреждение и должностные лица Учреждения, организующие и (или) осуществляющие обработку персональных данных;

обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), защиту, использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающие права и свободы субъекта персональных данных или других лиц;

блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

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;

обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

конфиденциальность персональных данных - обязательное для соблюдения должностным лицом Учреждения, иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

информация - сведения (сообщения, данные) независимо от формы их представления;

доступ к информации - возможность получения информации и ее использования.

3. Цели и задачи

3.1. Целями настоящего Положения выступают:

- обеспечение соответствия законодательству Российской Федерации действий работников Учреждения, направленных на обработку персональных данных слушателей;
- обеспечение защиты персональных данных от несанкционированного доступа, утраты, неправомерного их использования или распространения.

3.2. Задачами настоящего Положения являются:

- определение принципов, порядка обработки персональных данных;
- определение условий обработки персональных данных, способов защиты персональных данных;
- определение прав и обязанностей Учреждения и субъектов персональных данных при обработке персональных данных.

4. Состав персональных данных

4.1. Персональные данные включают в себя: фамилию, имя, отчество, паспортные данные, данные СНИЛС, должность, место работы, служебный телефон и другие данные, представляемые слушателем.

4.2. Информация о персональных данных может содержаться:

- на бумажных носителях;
- в информационных системах.

4.3. Учреждение использует следующие способы обработки персональных данных:

- автоматизированная обработка (с применением объектов вычислительной техники);
- без использования средств автоматизации;
- смешанная обработка.

4.4. Учреждение самостоятельно устанавливает способы обработки персональных данных в зависимости от целей такой обработки и материально-технических возможностей Учреждения.

4.5. Персональные данные слушателей Учреждения могут содержаться в следующих документах:

- договор об оказании платных образовательных услуг;
- список слушателей, прибывших на повышение квалификации;
- анкета слушателя, прибывшего на повышение квалификации;
- приказы по слушателям, выписки из приказов;
- удостоверение о повышении квалификации;
- другие документы, содержащие персональные данные и предназначенные для использования в целях организации образовательного процесса.

5. Обработка персональных данных

5.1. Персональные данные слушателей создаются путём внесения сведений на бумажные и электронные носители.

5.2. Основы организации обработки персональных данных слушателей в Учреждении (принципы, правовые основы, права и обязанности субъектов персональных данных).

5.2.2. Принципы обработки персональных данных:

- законность целей и способов обработки персональных данных;
- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Учреждения;
- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем, содержащих персональные данные.

5.2.3. Правовыми основаниями обработки персональных данных слушателей выступает законодательство об образовании РФ, а также локальные нормативные акты Учреждения.

5.2.4. В отношении по обработке персональных данных субъекты персональных данных имеют право:

- получать полную информацию о своих персональных данных и об обработке этих данных (в том числе автоматизированной);
- знакомиться со сведениями, содержащими свои персональные данные, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;
- выбирать представителей для защиты своих персональных данных;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением федерального закона; при отказе оператора исключить или исправить персональные данные субъект персональных данных имеет право заявить об этом в письменной форме директору Учреждения;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в суд любые неправомерные действия или бездействие руководства Учреждения при обработке его персональных данных.

5.2.5. При обращении субъекта персональных данных или его законного представителя по вопросам предоставления информации о персональных данных,

относящихся к соответствующему субъекту, Учреждение обязано сообщить данному субъекту информацию о наличии персональных данных, предоставить возможность ознакомления с ней.

5.2.6. В отношениях, связанных с обработкой персональных данных, субъекты персональных данных обязаны лично или через своего законного представителя:

- передавать Учреждению достоверные персональные данные, которые установлены настоящим Положением;
- своевременно сообщать Учреждению об изменении своих персональных данных, либо предоставить соответствующие документы.

5.3. Сроки обработки персональных данных.

5.3.1. Обработка персональных данных начинается с момента их получения Учреждением и заканчивается:

- по достижении заранее заявленных целей обработки;
- по факту утраты необходимости в достижении заранее заявленных целей обработки;
- в сроки, предусмотренные законодательством РФ.

5.3.2. Учреждение осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

5.4. Условия обработки персональных данных.

5.4.1. Общим условием обработки персональных данных является наличие письменного согласия субъектов персональных данных на осуществление такой обработки.

Письменное согласие на обработку персональных данных берется с каждого слушателя.

5.4.2. Обработка персональных данных субъекта персональных данных без получения его согласия осуществляется в следующих случаях:

- при поступлении официальных запросов (письменного запроса на бланке организации с печатью и росписью руководителя) из надзорно-контрольных или правоохранительных органов (суд, органы прокуратуры, ФСБ, МВД и т.п.);
- при непосредственном обращении сотрудников правоохранительных или надзорно-контрольных органов при предъявлении ими служебного удостоверения и соответствующих документов о получении персональных данных (запрос, постановление и т.п.), а также в иных случаях, предусмотренных федеральным законом;
- для статистических целей при условии обязательного обезличивания персональных данных;
- для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- при регистрации и отправки корреспонденции почтовой связью.

5.4.3. Учреждение не имеет права получать и обрабатывать персональные данные слушателей об их политических, религиозных и иных убеждениях и частной жизни, а равно об их членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

5.4.4. Обработка персональных данных осуществляется только должностными лицами (операторами) ответственными за обработку персональных данных, непосредственно использующими их в служебных целях.

Все слушатели Учреждения имеют право на полную информацию, касающуюся только собственных персональных данных.

5.5. Уточнение, блокирование и уничтожение персональных данных.

5.5.1. Уточнение персональных данных, в том числе их обновление и изменение, имеет своей целью обеспечение достоверности, полноты и актуальности персональных данных, обрабатываемых Учреждением.

5.5.2. Уточнение персональных данных осуществляется Учреждением по собственной инициативе, по требованию субъекта персональных данных или его законного представителя, по требованию уполномоченного органа по защите прав субъектов персональных данных в случае, когда установлено, что персональные данные являются неполными, устаревшими, недостоверными. Об уточнении персональных данных Учреждение обязан уведомить субъекта персональных данных или его законного представителя.

5.5.3. Блокирование персональных данных осуществляется Учреждением по требованию субъекта персональных данных или его законного представителя, а также по требованию уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними. О блокировании персональных данных Учреждение обязан уведомить субъекта персональных данных или его законного представителя.

5.5.4. Уничтожение персональных данных осуществляется:

- по достижении цели обработки персональных данных;
- в случае утраты необходимости в достижении целей обработки персональных данных;
- по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных в случае выявления фактов совершения Учреждением неправомерных действий с персональными данными, когда устранить соответствующие нарушения не представляется возможным.

5.5.5. В целях обеспечения законности при обработке персональных данных и устранения факторов, влекущих или могущих повлечь неправомерные действия с персональными данными, Учреждение вправе по собственной инициативе осуществить блокирование и (или) уничтожение персональных данных.

5.5.6. В ИСПДн Учреждения можно выделить следующие группы пользователей, участвующих в обработке персональных данных слушателей:

- Администратор безопасности ИСПДн;
- Администратор ИСПДн;
- Оператор АРМ.

6. Доступ к персональным данным

6.1. Внутренний доступ (работники Учреждения).

6.1.2. Доступ к персональным данным слушателей имеют следующие должностные лица Учреждения, непосредственно использующие их в рамках выполнения своих должностных обязанностей:

- директор Учреждения;
- заместители директора;
- сам слушатель;
- другие работники Учреждения, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей, и в том объеме, который необходим для исполнения трудовых обязанностей;
- в целях выполнения порученного задания и на основании служебной записки с положительной резолюцией директора Учреждения, доступ к персональным данным слушателя может быть предоставлен иному работнику, должность которого не включена в Перечень должностей работников, имеющих доступ к персональным данным, и которым они необходимы в связи с выполнением трудовых обязанностей.

6.2. Должностные лица Учреждения, имеющие в силу исполнения ими своих должностных обязанностей доступ к персональным данным, при их обработке должны обеспечивать конфиденциальность этих данных.

Перечень работников, имеющих доступ к персональным данным, утвержден в Приложении №4.

6.3. Внешний доступ (другие организации и граждане):

- правоохранительные органы;
- органы статистики.

6.4. Внешний доступ к персональным данным разрешается только при наличии заявления запросившего их лица с указанием перечня необходимой информации, целей для которых она будет использована, с письменного согласия слушателя, персональные данные которого затребованы.

7. Защита персональных данных

7.1. Учреждение при обработке персональных данных принимает необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

7.2. В целях обеспечения защиты персональных данных разрабатываются и утверждаются:

- планы внутренних проверок состояния защиты персональных данных;
- списки лиц, ответственных (уполномоченных) на обработку персональных данных слушателей;
- локальные нормативные акты, регулирующие порядок обработки и обеспечения безопасности и конфиденциальности персональных данных.

7.3. Защита персональных данных от неправомерного их использования или утраты обеспечивается за счёт средств Учреждения в порядке, установленном законодательством РФ.

7.4. В случае выявления неправомерных действий с персональными данными Учреждение обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Учреждение обязан уничтожить персональные данные.

7.5. Персональные данные в зависимости от способа их фиксации (бумажный носитель, электронный носитель) подлежат обработке таким образом, чтобы исключить возможность ознакомления с содержанием указанной информации сторонними лицами.

8. Ответственность за нарушение обработки и защиты персональных данных

8.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную, гражданскую и уголовную ответственность в соответствии с законодательством РФ.

8.2. Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

8.3. Каждый работник Учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Заместитель директора по учебной работе



А.А. Варламов

Оператор персональных данных слушателя:
ГКОУ Самарской области
«Учебно-методический центр по ГО и ЧС»

Адрес оператора:
инд.443099, г. Самара
ул. Комсомольская, 18

СОГЛАСИЕ на обработку персональных данных

Я (далее - Субъект), _____,
(фамилия, имя, отчество)
документ, удостоверяющий личность _____ № _____,
(вид документа)
выдан _____,
(кем и когда)
зарегистрированный (ая) по адресу: _____,

даю свое согласие Государственному казенному образовательному учреждению Самарской области «Учебно-методический центр по Гражданской обороне и Чрезвычайным ситуациям» далее (ГКОУ Самарской области «УМЦ по ГО и ЧС») адресу: 443099, город Самара, улица Комсомольская, дом 18, ИНН 6317026305, ОГРН 1026301421178 на обработку моих персональных данных в соответствии со следующими условиями: Цель:

- обеспечение соблюдения Конституции Российской Федерации, федерального и регионального законодательства;
- содействия в освоении образовательных программ;
- учета выполнения учебного плана и качества полученных знаний;
- формирования и ведения делопроизводства и документооборота, в том числе и в электронном виде;
- обеспечения личной безопасности в период обучения;

Перечень персональных данных:

- фамилия, имя, отчество (при наличии) (в том числе предыдущие фамилии, имена, отчества (при наличии) в случае их изменения);
- число, месяц, год рождения;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, его копия (при необходимости);
- адрес места жительства (адрес регистрации, адрес фактического места проживания);
- контактные данные (номер телефона, адрес электронной почты);
- уникальный номер индивидуального лицевого счёта застрахованного лица в системе обязательного пенсионного страхования (СНИЛС);
- сведения о предыдущем образовании (уровень образования, подуровень образования, специальность по диплому, категория квалификации, наименование образовательного учреждения, дата окончания, серия и номер документа об образовании, отличие, форма обучения), копии документов об образовании (при необходимости);
- сведения о договоре об оказании образовательных услуг для обучающихся (слушателей), обучающихся за счет средств физических и (или) юридических лиц (на платной основе);
- сведения о повышении квалификации, профессиональной переподготовке (наименование образовательной программы, объем, начало (окончание) обучения, профессия, квалификация,

сведения о документах о повышении квалификации (профессиональной переподготовке), копии документов об образовании (при необходимости);

Обработка поручена (при необходимости):

Способы обработки: смешанный способ обработки персональных данных

Перечень действий с персональными данными:

- сбор, систематизация, накопление, хранение персональных данных (в электронном виде и (или) бумажном носителе);

- уточнение (обновление, изменение), передача (предоставление, доступ), обезличивание, блокирование, уничтожение персональных данных;

- использование персональных данных в целях, обозначенных выше;

Настоящее согласие действует в течение срока обучения и на период хранения документов согласно действующему законодательству Российской Федерации.

Способ отзыва настоящего согласия: данное согласие может быть отозвано полностью или частично по моей инициативе на основании личного письменного заявления, которое может быть направлено мной в адрес Государственному казенному образовательному учреждению Самарской области «Учебно-методический центр по Гражданской обороне и Чрезвычайным ситуациям» 443099, город Самара, улица Комсомольская, дом 18, по почте заказным письмом с уведомлением о вручении, либо вручен лично под расписку.

Я ознакомлен(а) с тем, что в случае отзыва согласия на обработку персональных данных ГКОУ Самарской области «УМЦ по ГО и ЧС» вправе продолжить обработку персональных данных при наличии оснований, указанных в пунктах 2 – 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

_____ / _____ / «__» _____ 20__ года
подпись расшифровка подписи

Подтверждаю, что ознакомлен (а) с положениями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

«__» _____ 20__ г.

_____ *Подпись*

_____ *ФИО*

**Правила
осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных в
ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС»**

1. Настоящими правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – правила) в ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» (далее - Учреждение) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие правила разработаны в соответствии Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и другими нормативными правовыми актами.

3. В настоящих правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организовывается проведение периодических проверок условий обработки персональных данных.

5. Проверки осуществляются комиссией, образуемой приказом директора Учреждения. В проведении проверки не может участвовать работник Учреждения, прямо или косвенно заинтересованный в её результатах.

6. Проверки соответствия обработки персональных данных установленным требованиям в Учреждении проводятся 1 раз в квартал и на основании письменного заявления работника Учреждения в случае нарушений требований ФЗ «О персональных данных» (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

7. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

8. Комиссия имеет право:

- запрашивать у работников Учреждения информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить директору Учреждения предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить директору Учреждения предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. Проверка должна быть завершена не позднее чем через неделю со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, комиссией подготавливается письменное заключение.

Заместитель директора по учебной работе



А.А. Варламов

Правила обработки персональных данных в ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС»

1. Принципы, цели и условия обработки персональных данных

1.1. Обработка персональных данных в ГКОУ Самарской области «Учебно-методический центр по ГО и ЧС» (далее — Учреждение) осуществляется с учетом необходимости обеспечения защиты прав и свобод работников Учреждения и других субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

– обработка персональных данных осуществляется в Учреждении 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 соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

– при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Учреждением 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 того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является Учреждение;

– обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

1.2 Персональные данные обрабатываются в Учреждении в целях: предоставления государственных услуг физическим и юридическим лицам, выполнения государственных работ;

- регулирования трудовых отношений с работниками Учреждения;
- подготовки, заключения и исполнения договоров с контрагентами.

1.3 Обработка персональных данных в Учреждении осуществляется следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

1.4 Информация о персональных данных может содержаться:

- на бумажных носителях;
- на электронных носителях;
- в информационно-телекоммуникационных сетях (на официальном сайте) и иных информационных системах Учреждения.

2. Условия, порядок обработки персональных данных работников.

2.1 Персональные данные работников Учреждения, а также лиц, претендующих на замещение вакантных должностей, обрабатываются в целях осуществления кадровой работы, а именно: оформления трудовых отношений, обучения и обеспечения должностного роста, учета результатов исполнения должностных обязанностей, расчета и выдачи заработной платы или других доходов, осуществления налоговых и пенсионных отчислений, обеспечения личной безопасности, обеспечения работникам установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, а также в целях противодействия коррупции.

2.2 В целях, указанных в пункте 2.1. настоящего Порядка, обрабатываются персональные данные работников Учреждения, граждан, претендующих на замещение вакантных должностей, включенные в Перечень персональных данных, обрабатываемых в Учреждении по вопросам деятельности в связи с реализацией служебных (трудовых) отношений.

2.3 Обработка персональных данных работников и граждан, претендующих на замещение вакантных должностей в Учреждении, осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 4.1 настоящего Положения, в соответствии с пп. 2, 11 части 1, п. 3.1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных» и положениями Трудового кодекса Российской Федерации.

2.4 Обработка персональных данных работников Учреждения и граждан, претендующих на замещение вакантных должностей в Учреждении, осуществляется при условии получения согласия указанных лиц в следующих случаях:

- при передаче (распространении, предоставлении) персональных данных

третьим лицам в случаях, не предусмотренных действующим законодательством

- при трансграничной передаче персональных данных;
- при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных;
- при опубликовании персональных данных в средствах массовой информации и размещении их на официальном сайте Учреждения, за исключением размещения информации о проведении мероприятий (работ) или участия в них в рамках исполнения должностных обязанностей, участия в массовых мероприятиях, на которых официально велась фото- и видеосъемка.

2.5 В случаях, предусмотренных пунктом 2.4 настоящего Порядка, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

2.6 Обработка персональных данных работников Учреждения и граждан, претендующих на замещение вакантных должностей в Учреждении, осуществляется специалистом по кадрам, Заместителем директора по финансово-экономическим вопросам, ведущим экономистом, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.7 Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных работников Учреждения и граждан, претендующих на замещение вакантных должностей в Учреждении, осуществляется путем:

- получения **оригиналов** необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые в отдел кадровой работы), предъявляемых при заключении трудового договора на основании ст. 65 Трудового кодекса Российской Федерации;

- внесения сведений в учетные формы (на бумажных и электронных носителях);

- формирования персональных данных в ходе кадровой работы;

- сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от работников Учреждения, а также граждан, претендующих на замещение вакантных должностей Учреждения.

2.8 В случае возникновения необходимости получения персональных данных работников Учреждения у третьей стороны, следует известить об этом вышеназванных работников заранее, получить их письменное согласие и сообщить им о целях, предполагаемых источниках и способах получения персональных данных.

2.9 Запрещается получать, обрабатывать и приобщать к личному делу работников Учреждений персональные данные, не предусмотренные Перечнем персональных данных, обрабатываемых в Учреждении по вопросам деятельности, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.10 Передача (распространение, предоставление) и использование персональных данных работников Учреждения осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

2.11 Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных законодательством.

3. Условия и порядок обработки персональных данных слушателей Учреждения.

3.1. В Учреждении обработка персональных данных физических лиц осуществляется в целях предоставления государственных услуг в сфере дополнительного профессионального образования (далее – Государственных Услуг).

3.2. Персональные данные граждан, обратившихся в Учреждение лично, а также направивших индивидуальные или коллективные письменные обращения, или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений.

3.3. Обработка персональных данных, необходимых в связи с предоставлением Государственных Услуг, осуществляется с согласия субъектов персональных данных работниками Учреждения.

3.4. Обработка персональных данных, необходимых в связи с предоставлением Государственных Услуг включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.5. В связи с оказанием Государственных Услуг обрабатываются персональные данные граждан, включенные в Перечень персональных данных слушателей Учреждения.

3.6. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных граждан, обратившихся в Учреждение за оказанием Государственных Услуг:

- получение оригиналов необходимых документов (заявлений);
- заверения копий документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);

– внесения персональных данных в информационные системы Учреждения.

3.7. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (заявителей), а также от юридических лиц при направлении ими межведомственного запроса при предоставлении Государственных Услуг.

3.8. При предоставлении Государственных Услуг Учреждением запрещается запрашивать у субъектов персональных данных и третьих лиц персональные данные, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

3.9. При сборе персональных данных уполномоченное должностное лицо Учреждения, осуществляющее получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением Государственных Услуг, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

3.10. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) Учреждением осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

3.11. Обработка персональных данных контрагентов – физических лиц (в том числе физических лиц, являющихся индивидуальными предпринимателями), с которыми непосредственно у Учреждения заключен договор, может осуществляться без согласия на обработку персональных данных при условии, что эти данные не будут распространяться и предоставляться третьим лицам без согласия субъекта персональных данных и будут обрабатываться только в целях исполнения заключенных с ними договоров гражданско-правового характера.

4. Права субъектов персональных данных

4.1 Субъекты персональных данных имеют право на:

– полную информацию об их персональных данных, обрабатываемых в Учреждении;

– доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;

– уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– отзыв согласия на обработку персональных данных;

– принятия предусмотренных действующим законодательством мер по защите своих прав;

– обжалование действия или бездействия Учреждения, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;

– осуществление иных прав, предусмотренных законодательством Российской Федерации.

5. Меры по обеспечению защиты персональных данных при их неавтоматизированной обработке.

5.1 Учреждение 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 в соответствии с действующим законодательством и нормативными актами Учреждения.

5.2 Обеспечение безопасности персональных данных при их неавтоматизированной обработке в Учреждении достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

– хранением текущей и архивной документации, содержащей персональные данные, в помещениях Учреждения, предназначенных для хранения документации, в соответствии с действующим законодательством и внутренними нормативными актами;

– обеспечением кабинетов, где хранятся документы, содержащие персональные данные, сейфами и запираемыми шкафами, оборудованными для опечатывания;

– хранением персональных данных не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении;

– хранением документов в течение установленных действующими нормативными актами сроков хранения данных документов. По истечении установленных сроков хранения документы подлежат уничтожению;

– обособлением персональных данных, обрабатываемых без использования средств автоматизации, от иной информации, в частности путем их фиксации на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков);

– обеспечением раздельного хранения персональных данных и их материальных носителей, обработка которых осуществляется в разных целях и которые содержат разные категории персональных данных;

– ограничением доступа к персональным данным лицам, не уполномоченным Федеральным законодательством, либо нормативными актами Учреждения для получения соответствующих сведений.

5.3 Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют должностные лица Учреждения ответственные за обработку персональных данных.

6. Порядок обработки персональных данных субъектов персональных данных в информационных системах

6.1. Сотрудникам Учреждения, имеющим право осуществлять обработку персональных данных в информационных системах Учреждения, предоставляется уникальный логин и пароль для доступа к персональному компьютеру, на котором осуществляется автоматизированная обработка персональных данных.

6.2 Информация в информационные системы вносится в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

6.3 Персональные данные, содержащиеся в информационных системах, хранятся на серверах Учреждения. Доступ к указанным серверам строго ограничен кругом лиц, ответственных за обработку персональных данных. Информация на электронных носителях должна быть защищена паролем доступа, который подлежит смене не реже 1 (одного) раза в 6 (шесть) месяцев.

6.4 Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

- применение 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, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией, оценку эффективности принимаемых мер по обеспечению безопасности персональных данных в информационных системах персональных данных;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, машинных носителей персональных данных;

- учет лиц, допущенных к работе с персональными данными в

информационных системах, инструктирование лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
- анализ фактов несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

6.5. В случае выявления нарушений порядка обработки персональных данных уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

6.6. При смешанной обработке персональных данных их защита достигается реализацией комплекса вышеперечисленных мер.

6.7. Персональные данные вне зависимости от способа их фиксации (бумажный носитель, электронный носитель) подлежат обработке таким образом, чтобы исключить возможность ознакомления с содержанием указанной информации сторонними лицами.

7. Рассмотрение запросов субъектов персональных данных или их представителей

7.1. Работники Учреждения, граждане, персональные данные которых обрабатываются в Учреждении в связи с предоставлением Государственных Услуг имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных в Учреждении;
- правовое основание и цели обработки персональных данных;
- применяемые в Учреждении способы обработки персональных данных;
- наименование и место нахождения Учреждения, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании федеральных законов;
- 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 в Учреждении;
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;
- информацию об осуществленной или предполагаемой трансграничной передаче данных;
- наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такой организации;
- иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

7.2. Субъекты персональных данных вправе требовать от Учреждения уточнения их 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.

7.3. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7.4. Сведения предоставляются субъекту персональных данных или его представителю руководителем Учреждения, осуществляющего обработку соответствующих персональных данных при обращении либо при получении запроса субъекта персональных данных или его представителя. 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 правоотношениях с Учреждением (документ, подтверждающий оказание Учреждением мер социальной поддержки), либо сведения, иным образом подтверждающие факт обработки персональных данных в Учреждении, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Учреждение или направить

повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

7.6. Субъект персональных данных вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения сведений, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 7.5 настоящего Порядка в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 7.5 и 7.6 настоящего Порядка. Такой отказ должен быть мотивированным.

7.7. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

8. Заключительные положения

8.1. Настоящий Порядок вступает в силу с даты его утверждения Приказом директора Учреждения и действует бессрочно, до его замены новым.

8.2. Настоящий Порядок распространяется на всех сотрудников Учреждения, в том числе сотрудников Учреждения, имеющих доступ и осуществляющих перечень действий с персональными данными граждан, а также граждан, персональные данные которых обрабатываются в связи с получением мер социальной поддержки.

8.3. В обязанности Учреждения входит ознакомление всех сотрудников с настоящим Порядком и лиц, принимаемых на работу, до подписания трудового договора, под личную подпись.

8.4. Настоящий Порядок является общедоступным, его текст подлежит публикации на официальном сайте Учреждения.

Заместитель директора по учебной работе



А.А. Варламов

Правила работы с обезличенными персональными данными

1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными в ГКОУ Самарской области «Учебно-методический Учреждение по ГО и ЧС» (далее – Учреждение) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила определяют порядок работы с обезличенными персональными данными.

1.3. Настоящие Правила утверждаются директором Учреждения.

2. Термины и определения

2.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»:

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

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

3. Условия обезличивания

3.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение - понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город)
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

4. Порядок работы с обезличенными персональными данными

4.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

4.2. Обезличенные персональные данные могут обрабатываться с использованием и безиспользования средств автоматизации.

4.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями;
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

4.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним в помещения, где они хранятся.

Заместитель директора по учебной работе



А.А. Варламов

**Перечень информационных систем персональных данных
ГКОУ Самарской области «Учебно-методический Учреждение по ГО и ЧС»**

№ п/п	Наименование программных комплексов, входящих в состав ИСПДн	Тип ИСПДн по категории ПДн	Тип ИСПДн по категории субъектов (работники, субъекты, не являющиеся работниками Учреждения)	Количество субъектов ПДн (чел.)
1. Информационная система персональных данных "Бухгалтерский учет и зарплата"				
1.1.	1С: Предприятие	ИСПДн-И	Субъекты, не являющиеся работниками	Менее чем 100000
1.2.	1С: Зарплата и кадры	ИСПДн-И	Работники, субъекты, не являющиеся работниками	Менее чем 100000
1.3.	Пакет офисных приложений Microsoft Office	ИСПДн-И	Работники	Менее чем 100000
1.4.	АС "Клиент-Сбербанк"	ИСПДн-И	Работники	Менее чем 100000
1.5.	УРМ	ИСПДн-И	Работники	Менее чем 100000

1.6.	Контур. Диадок	ИСПДн-И	Субъекты, не являющиеся работниками	Менее чем 100000
2. Информационная система персональных данных "Кадровый учет"				
2.1.	Пакет офисных приложений Microsoft Office	ИСПДн-И	Субъекты, не являющиеся работниками	Менее чем 100000
2.2.	Система "Контур. Экстерн"	ИСПДн-И	Работники	Менее чем 100000
2.3.	1С: Зарплата и кадры	ИСПДн-И	Работники	Менее чем 100000
3. Информационная система персональных данных "Содействие добровольному переселению в Российскую Федерацию соотечественников, проживающих за рубежом"				
3.1.	Пакет офисных приложений Microsoft Office	ИСПДн-С	Субъекты, не являющиеся работниками	Менее чем 100000
4. Информационная система персональных данных "Трудовые договоры"				
4.1.	Пакет офисных приложений Microsoft Office	ИСПДн-И	Субъекты, не являющиеся работниками	Менее чем 100000
5. Информационная система персональных данных "Противодействия коррупции".				
5.1	Пакет офисных приложений	ИСПДн-И	Субъекты, не являющиеся работниками	Менее чем 100000

Заместитель директора по учебной работе



А.А. Варламов