

Муниципальное учреждение дополнительного образования
«Центр дополнительного образования «Созвездие»
Тутаевского муниципального района



ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных сотрудников муниципального учреждения дополнительного образования «Центр дополнительного образования «Созвездие» Тутаевского муниципального района

1 Термины и определения

1.1 Ниже приведён перечень определений, используемых при подготовке настоящего Положения.

Безопасность информации — состояние защищённости информации, характеризующееся способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, то есть сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Доступ к информации — возможность получения информации и ее использования.

Доступность информации — состояние информации, характеризующееся способностью автоматизированной системы обеспечить беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защита информации от несанкционированного доступа или воздействия — деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию).

Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информация — сведения (сообщения, данные) независимо от их формы представления.

Информация ограниченного доступа — информация, доступ к которой ограничен федеральными законами.

Конфиденциальная информация — информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к такой информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Несанкционированный доступ — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средством вычислительной техники или автоматизированной системой.

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.

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

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

Средства вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Технические средства информационной системы персональных данных — средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки 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.

Целостность информации — состояние защищённости информации, характеризующее способность автоматизированной системы обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки и хранения.

1 Основные положения

1.1 Настоящее Положение принято в целях определения основных принципов обработки и защиты персональных данных (далее по тексту – ПДн) сотрудников муниципального учреждения дополнительного образования «Центр дополнительного образования «Созвездие» Тутаевского муниципального района (далее по тексту – Учреждение) от несанкционированного доступа, неправомерного использования или утраты.

1.2 Настоящее Положение разработано на основе и во исполнение Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», положений Трудового кодекса Российской Федерации.

1.3 Настоящее Положение является обязательным для исполнения всеми сотрудниками Учреждения, имеющими доступ к ПДн сотрудников.

1.4 Все сотрудники должны быть ознакомлены под роспись с настоящим Положением и иными документами Учреждения, устанавливающими порядок обработки ПДн сотрудников.

1.5 Настоящее Положение вступает в силу с даты его утверждения и действует до его отмены либо замены новым Положением.

2 Понятие и состав ПДн сотрудника

2.1 ПДн сотрудника – любая информация, относящаяся к прямо или косвенно определенному или определяемому сотруднику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, гражданство, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, указания о возможности занимать лицом те или иные должности, сведения о предыдущих местах работы и другая информация, необходимая работодателю в связи с организацией трудовых отношений между сотрудником и работодателем.

2.2 ПДн сотрудника составляют:

- сведения о сотруднике, позволяющие идентифицировать его и получить о нем дополнительную информацию;
- служебные и иные сведения, связанные с профессиональной деятельностью сотрудника.

3 Документы, содержащие ПДн

3.1 Информация, представляемая сотрудником при заключении трудового договора с Центром «Созвездие» как работодателем, должна иметь документальную форму.

3.2 При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или сотрудник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования (при его наличии);
- документы воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);
- документ об образовании, о квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);
- свидетельство о присвоении идентификационного номера налогоплательщика;
- справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, связанную с деятельностью, к осуществлению которой не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию).

В отдельных случаях с учетом специфики работы может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

3.3 После оформления и заключения трудового договора ответственным сотрудником Учреждения заполняется унифицированная форма Т-2 «Личная карточка сотрудника», в которой отражаются следующие анкетные и биографические данные сотрудника:

- табельный номер сотрудника, идентификационный номер налогоплательщика, номер страхового свидетельства государственного пенсионного страхования, сведения о характере и виде работы, пол сотрудника;
- общие сведения (фамилия, имя, отчество сотрудника, дата рождения, место рождения, гражданство, сведения о знании иностранных языков, сведения об образовании,

профессия, сведения о стаже работы, сведения о составе семьи, сведения о паспорте, адрес прописки и фактического проживания, телефон, номер трудового договора);

- сведения о воинском учете;
- данные о приеме на работу.

В дальнейшем в личную карточку вносятся:

- сведения о занимаемых сотрудником должностях;
- сведения о переводах на другую работу;
- сведения об аттестации сотрудника;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных льготах, на которые сотрудник имеет право в соответствии с законодательством.

3.4 ПДн сотрудников содержатся также и в иных документах, сопровождающих процесс оформления трудовой деятельности сотрудников Учреждения:

- подлинники и копии приказов (распоряжений) по личному составу;
- командировочные удостоверения;
- документы, содержащие сведения о расчете оплаты труда, доплатах, надбавках, единовременных выплатах;
- документы, предоставляемые самим сотрудником (заявления, справки, листы временной нетрудоспособности);
- графики отпусков.

3.5 ПДн сотрудников Учреждения могут содержаться в документах бухгалтерского учета и отчетности (первичных учетных документах, актах, журналах, книгах, ведомостях, платежных поручениях, отчетных формах и т. д.).

3.6 ПДн сотрудников Учреждения могут быть включены в документацию, связанную с организацией работы Учреждения (штатное расписание (штатная расстановка); приказы, распоряжения, указания руководства Учреждения, иные внутренние нормативные акты; внутренние списки различного назначения).

4 Принципы обработки ПДн сотрудника в Учреждении

4.1 В Учреждении обработка ПДн сотрудника осуществляется в целях обеспечения условий трудового договора (служебного контракта), заключенного между работодателем и сотрудником, обеспечения соблюдения законов Российской Федерации и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества либо в иных целях с согласия сотрудника.

4.2 В Учреждении не допускается принятие решений, затрагивающих интересы сотрудника, основанных исключительно на ПДн сотрудника, полученных в электронном виде либо в результате их автоматизированной обработки.

5 Создание ПДн сотрудника

5.1 Документы, содержащие ПДн сотрудника, создаются путём:

- копирования оригиналов документов (паспорт, документ об образовании) либо получения заверенных копий;

- получения (создания) оригиналов документов (трудовая книжка, личная карточка);
- внесения сведений в документы, файлы, учетные формы;
- дополнения документов путем формирования (расчета) сведений на основе имеющихся данных, в том числе с использованием средств автоматизации.

5.2 Необходимые ПДн сотрудника вносятся ответственными сотрудниками структурных подразделений Учреждения в специализированные электронные системы.

5.3 Дальнейшая обработка ПДн сотрудника (в процессе трудовой деятельности) осуществляется как на бумажных носителях, в неавтоматизированном режиме, так и с использованием средств автоматизации.

6 Доступ к ПДн сотрудников

6.1 Доступ к ПДн сотрудников Учреждения, не являющимся общедоступными, могут иметь сотрудники Учреждения, замещающие должности, включенные в Перечень должностей, замещение которых предусматривает осуществление обработки ПДн или доступа к ним, утверждаемый директором Учреждения, а также уполномоченные представители органов и организаций в случаях, определенных законодательством РФ.

6.2 Уполномоченные лица имеют право доступа к тем и только тем ПДн сотрудников, которые необходимы для выполнения конкретных функций в соответствии с должностными инструкциями (регламентами) указанных лиц.

7 Хранение ПДн сотрудников

7.1 Личные дела (личные карточки) сотрудников хранятся в запертом шкафу Учреждения. Трудовая книжка, документы воинского учёта хранятся в запертом металлическом сейфе.

7.2 Хранение бумажных и электронных носителей информации, содержащих ПДн сотрудников, должно осуществляться в закрытых помещениях, шкафах и сейфах. При приеме посетителей данные носители информации должны быть убраны в стол, шкаф, сейф либо иное место с целью исключения возможности несанкционированного доступа к ним. Места хранения носителей, содержащих ПДн, утверждаются руководителями структурных подразделений Учреждения, в которых осуществляется обработка ПДн с использованием бумажных или электронных носителей информации.

7.3 В электронном виде ПДн сотрудников могут содержаться в файлах (в том числе файлах баз данных).

7.4 В случае увольнения сотрудника его ПДн должны быть выведены из рабочей базы данных в архив. Личное дело (личная карточка) уволенного сотрудника также передается в архив.

8 Возможность получения ПДн у третьих лиц

8.1 ПДн сотрудника, обрабатываемые в Учреждении, предоставляет сам сотрудник.

8.2 Получение ПДн сотрудника от третьей стороны допускается только при условии предварительного уведомления сотрудника и наличия его письменного согласия, если иное не предусмотрено федеральным законом. Сотрудник должен быть уведомлен о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа сотрудника дать письменное согласие на их получение.

9 Возможность предоставления ПДн третьим лицам

9.1 Передача сотрудниками Учреждения ПДн сотрудника, не являющихся общедоступными, третьей стороне возможна только с согласия сотрудника или в случаях, прямо предусмотренных законодательством РФ.

9.2 Предоставление сотрудниками Учреждения ПДн сотрудников третьим лицам без соответствующего их согласия возможно в следующих случаях:

- в целях предупреждения угрозы жизни и здоровья сотрудника;
- при поступлении официальных запросов в соответствии с положениями Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»;
- при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Фонда социального страхования, судебных органов.

9.3 ПДн сотрудника не должны сообщаться по телефону кому бы то ни было.

9.4 При передаче ПДн сотрудника работодатель обязан предупредить лиц, получающих ПДн сотрудника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Лица, получающие ПДн сотрудника, обязаны соблюдать режим конфиденциальности и обеспечивать безопасность полученных ПДн.

10 Защита ПДн

10.1 Защита ПДн представляет собой регламентированный технологический процесс, предупреждающий нарушение доступности, целостности (достоверности, полноты) и конфиденциальности ПДн и, в конечном счете, обеспечивающий безопасность информации в процессе деятельности органов исполнительной власти.

10.2 Защита ПДн сотрудника от неправомерного их использования, разглашения или утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральными законами. В отношении информационных систем ПДн и отдельных технических средств, на которых обрабатываются ПДн сотрудников Учреждения, должен быть проведен полный комплекс технических мероприятий по защите ПДн от несанкционированного доступа в соответствии с требованиями действующих на территории Российской Федерации руководящих и нормативно-методических документов по защите конфиденциальной информации (ПДн).

10.3 Комплекс организационных мер по защите ПДн сотрудников Учреждения включает:

- ограничение круга лиц, доступ к ПДн сотрудников которым необходим для выполнения служебных обязанностей;
- ограничение круга лиц, имеющих доступ в помещения, в которых расположены технические средства, участвующие в обработке ПДн, и хранятся электронные либо бумажные носители ПДн, исключение неконтролируемого пребывания в таких помещениях лиц, не имеющих допуска к ПДн сотрудников Учреждения;
- сопровождение посетителей и иных посторонних лиц в пределах контролируемой зоны постоянными сотрудниками организации либо оборудование мест пребывания посетителей системой видеонаблюдения;
- оснащение помещений, занимаемых Учреждением, системой охранной сигнализации либо обеспечение охраны помещений в нерабочее время;
- уведомление лиц, допущенных к ПДн сотрудников, об обработке ими информации ограниченного доступа и об ответственности за нарушение установленных требований к порядку обработки и защите такой информации (под роспись);
- проведение инструктажей по безопасности ПДн с сотрудниками, имеющими доступ к ПДн сотрудников;

- контроль соблюдения установленного в Учреждении порядка обработки ПДн и обращения с носителями ПДн, проведение разбирательств по фактам несоблюдения установленных в Учреждении требований по защите ПДн сотрудников;
- размещение рабочих мест (средств отображения информации, средств графической обработки информации) способом, исключающим несанкционированный просмотр выводимой информации лицами, не имеющими допуска к ПДн;
- обеспечение своевременного вывода ПДн из обработки (перевода на архивное хранение, уничтожения либо обезличивания).

10.4 Защита ПДн сотрудников, содержащихся на электронных носителях.

Файлы, содержащие ПДн сотрудников Учреждения (в том числе файлы баз данных), должны храниться в специально выделенных каталогах на определенных средствах вычислительной техники. На данные файлы/каталоги должны быть установлены права доступа в соответствии с разрешительной системой доступа (матрицей доступа) к защищаемым ресурсам (матрица доступа к защищаемым ресурсам должна быть документально зафиксирована и составлена таким образом, чтобы сотрудники имели доступ к тем и только тем ПДн, которые необходимы им для выполнения своих служебных обязанностей).

Хранение файлов, содержащих ПДн, на внешних (отчуждаемых) носителях разрешается только в случае ведения учета данных носителей. Копирование файлов, содержащих ПДн, на неучтенные внешние носители информации запрещено и является нарушением трудовой дисциплины.

11 Права и обязанности сотрудника как субъекта ПДн

11.1 В целях обеспечения защиты своих ПДн сотрудники имеют право на:

- полную информацию об их ПДн и обработке этих данных;
- свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн сотрудника, за исключением случаев, предусмотренных федеральным законодательством. Право сотрудника на доступ к своим ПДн ограничивается в случае, если предоставление ПДн нарушает конституционные права и свободы других лиц;
- исключение или исправление неверных или неполных ПДн, а также данных, обрабатываемых с нарушением федерального законодательства. При отказе работодателя исключить или исправить ПДн сотрудник имеет право заявить в письменной форме работодателю о своём несогласии, обосновав соответствующим образом такое несогласие. ПДн оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения. Сотрудник имеет право требовать от работодателя уведомления всех лиц, которым ранее были сообщены неверные или неполные ПДн сотрудника, обо всех произведённых в них изменениях или исключениях из них. Неправомерные действия или бездействие работодателя при обработке и защите ПДн сотрудника могут быть обжалованы в суд;
- получение подтверждения факта обработки ПДн оператором, а также сведений о цели и правовых основаниях такой обработки, способах обработки ПДн, применяемых оператором, сроках обработки ПДн (в том числе сроках их хранения), возможности трансграничной передачи ПДн; перечня обрабатываемых ПДн и сведений об источнике их получения; сведений о лице, обрабатывающем по поручению оператора ПДн сотрудника;
- получение сведений о лицах, которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора, заключенного с оператором, или федерального закона (за исключением сотрудников оператора).

11.2 В свою очередь, сотрудник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных ПДн, состав которых установлен трудовым законодательством и иными федеральными законами;
- своевременно сообщать работодателю об изменении своих ПДн.

12 Обязанности работодателя

12.1 В случае необходимости работодатель обязан разъяснить сотруднику порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов. Работодатель обязан рассмотреть возражение сотрудника в течение тридцати дней со дня его получения и уведомить его о результатах рассмотрения такого возражения.

12.2 Если обязанность предоставления ПДн сотрудником установлена федеральным законом, работодатель обязан разъяснить сотруднику юридические последствия отказа предоставить свои ПДн.

12.3 Если ПДн были получены не от сотрудника за исключением случаев, если ПДн были предоставлены оператору в связи с исполнением договора, на основании федерального закона или если ПДн сделаны общедоступными субъектом ПДн (либо получены из общедоступного источника), работодатель до начала обработки таких ПДн обязан предоставить сотруднику следующую информацию¹:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- права сотрудника в области защиты ПДн;
- источник получения ПДн.

12.4 Работодатель обязан безвозмездно предоставить сотруднику возможность ознакомления с ПДн, относящимися к соответствующему сотруднику, а также внести в них необходимые изменения, уничтожить или заблокировать соответствующие ПДн по предоставлению сотрудником сведений, подтверждающих, что ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах работодатель обязан уведомить сотрудника и принять меры по уведомлению третьих лиц, которым ПДн этого сотрудника были переданы.

12.5 В случае выявления неточных ПДн или неправомерной обработки ПДн работодатель обязан осуществить блокирование ПДн, относящихся к соответствующему сотруднику, с момента получения такой информации на период проверки.

12.6 В случае подтверждения факта неточности ПДн или неправомерной обработки ПДн работодатель на основании соответствующих документов обязан в течение семи рабочих дней обеспечить уточнение ПДн, снять их блокирование и принять меры по уведомлению об изменении ПДн тех лиц, которым ПДн сотрудника были переданы.

12.7 В случае выявления неправомерных действий с ПДн работодатель в срок, не превышающий трех рабочих дней с даты такого выявления, обязан прекратить неправомерную обработку ПДн. В случае если обеспечить правомерность обработки ПДн невозможно, работодатель в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить ПДн. Об устранении допущенных нарушений или об уничтожении ПДн работодатель обязан уведомить сотрудника.

¹ Если субъект ПДн не уведомлен об обработке его ПДн соответствующим оператором.

12.8 В случае достижения цели обработки ПДн работодатель обязан прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено федеральными законами (в частности, законодательством об архивном деле), договором, контрактом или соглашением, стороной которого является сотрудник.

13 Ответственность за нарушение установленных требований по защите ПДн сотрудников Учреждения

13.1 Руководитель, разрешающий доступ сотрудника к документам, файлам, базам данных или их частям, содержащим ПДн, несет персональную ответственность за данное разрешение.

13.2 Сотрудник, получающий доступ к документам, файлам, базам данных или их частям, содержащим ПДн, несет персональную ответственность за любые действия, совершаемые им с информацией или ее носителями.

13.3 Лица, виновные в нарушении установленных норм, регулирующих порядок обработки и мероприятия по защите ПДн сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

13.4 За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом Российской Федерации дисциплинарные взыскания.

13.5 Нарушение неприкосновенности частной жизни (в том числе незаконный сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения, наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с Уголовным Кодексом Российской Федерации.

14 Ознакомлены

С правилами ознакомлен, правила изучены и понятны.

№ п/п	Ф.И.О. сотрудника	Должность	Дата ознакомления	Личная подпись
1.	Жижина Е.А.	документовед		
2.	Иванова О.Г.	секретарь		
3.	Сутеева И.С.	зам.директора		
4.	Лепешова Т.Л.	зам.директора		
5.	Хомутова Ю.Д.	зам.директора		
6.	Кувалдина И.С.	зам.директора		
7.				
8.				
9.				
10.				

