Утверждено
приказом начальника
ШаройскогоРОО
от «11» 01.2018 № 24

Положение

о защите и обработке персональных данных работников ШаройскогоРОО

1. Общие положения

1.1. Положение о защите и обработке персональных данных в Шаройском районном отделе образования (далее - Положение) устанавливает требования к обеспечению безопасности персональных данных и определяет:

-порядок обработки персональных данных;

-мероприятия по обеспечению защиты прав и свобод граждан при обработке их персональных данных

- ответственность должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Положение разработано в соответствии с:

Конституцией РФ; Гражданским кодексом РФ;Трудовым кодексом РФ;Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;постановлением Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;приказом ФСТЭК России от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

1.3. Целью Положения является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания или по истечении 75 лет срока их хранения, или продлевается на основании заключения комиссии по защите персональных данных отдела образования, если иное не определено законом.

2. Основные понятия и состав персональных данных

2.1. Основные понятия, используемые в настоящем Положении:

-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, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

-оператор - физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

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

-распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на 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;

-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 затрагивающих 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;

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

2.2. Персональные данные, обрабатываемые в РОО, содержатся в документах:

- отдела образования;

- бухгалтерского учета и контроля.

2.2.1. В отделе образования создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.2.1.1. документы, содержащие персональные данные работников отдела (копия паспорта, копия страхового пенсионного свидетельства, копия ИНН, комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплект материалов по анкетированию, тестированию, проведению собеседований с кандидатами на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников, служебных проверок), подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству отдела.

2.2.1.2. документация по организации работы государственных образовательных учреждений (приказы, указания); документы по планированию, учету, анализу и отчетности в части работы с персоналом отдела.

2.2.2. В отделе бухгалтерского учета и контроля создаются и хранятся следующие документы, содержащие данные о работниках в единичном или сводном виде: карточка-справка, копия паспорта, копия страхового пенсионного свидетельства, копия ИНН, копия личного счета для зачисления заработной платы, копии приказов с расчетами, отчеты в органы статистики, отчеты в налоговые органы и другие организации.

3. Порядок сбора и обработки персональных данных

3.1. Порядок получения персональных данных о работниках отдела.

3.1.1. Все персональные данные работника РОО следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Ответственное лицо отдела 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.

3.1.2. Ответственные лица отдела не имеют права получать и обрабатывать персональные данные работника о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ ответственные лица отдела вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

Обработка указанных персональных данных работников возможна только с их согласия либо без их согласия в следующих случаях:

- персональные данные являются общедоступными;

- персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

- по требованию полномочных государственных органов в случаях, предусмотренных федеральными законами.

3.1.3. Письменное согласие работника на обработку своих персональных данных должно включать в себя:

-фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

-наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

-цель обработки персональных данных;

-перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

-перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

-срок, в течение которого действует согласие, а также порядок его отзыва.

Форма заявления о согласии работника на обработку персональных данных - согласно приложения к настоящему Положению.

3.1.4. Согласие работника не требуется в следующих случаях:

-обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

-обработка персональных данных осуществляется в целях исполнения трудового договора;

-обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

-обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

3.2. Порядок обработки, передачи и хранения персональных данных работников РОО.

3.2.1. Работник предоставляет ответственным работникам отдела кадров и отдела бухгалтерского учета достоверные сведения о себе. Ответственные работники указанных отделов проверяют достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами.

3.2.2. В соответствии со статьей 86 Трудового кодекса РФ в целях обеспечения прав и свобод человека и гражданина ответственные работники при обработке персональных данных работника должны соблюдать следующие общие требования:

3.2.2.1. обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

3.2.2.2. при определении объема и содержания, обрабатываемых персональных данных ответственные работники должны руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами;

3.2.2.3. при принятии решений, затрагивающих интересы работника, ответственные работники не имеют права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

3.2.2.4. защита персональных данных работника от неправомерного их использования или утраты обеспечивается ответственные работники и за счет средств отдела в порядке, установленном нормативными правовыми документами;

3.2.2.5. работники, осуществляющие обработку персональных данных, должны быть ознакомлены под расписку с документами РОО, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

3.2.2.6. во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен.

4. Обеспечение защиты персональных данных.

4.1. Безопасность персональных данных достигается путём исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

4.2. Безопасность персональных данных при их обработке обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-математических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

4.3. При обработке персональных данных должно быть обеспечено:

-проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

-своевременное обнаружение фактов несанкционированного доступа к персональным данным;

-недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

-возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

-постоянный контроль за обеспечением уровня защищённости персональных данных.

4.5. Мероприятия по обеспечению безопасности персональных данных включают в себя:

4.5.1. определение информационных систем, содержащих персональные данные;

4.5.2. классификацию информационных систем персональных данных в соответствии с совместным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;

4.5.3. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

4.5.4. использование средств защиты информации в соответствии с эксплуатационной и технической документацией;

4.5.5. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

4.5.6. учёт применяемых средств защиты информации.эксплуатационной и технической документации к ним, носителей персональных данных;

4.5.7. учёт лиц, допущенных к работе с персональными данными в информационной системе;

4.5.8. контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

4.5.9. составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут провести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных нарушений.

5. Передача персональных данных

5.1. Передача персональных данных работников РОО.

5.1.1. Управление не вправе предоставлять персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законодательством.

5.1.2. В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных работника или отсутствует письменное согласие работника на предоставление его персональных сведений, отдел обязан отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

5.1.3. Персональные данные работника могут быть переданы представителям третьей стороны в том объёме, в каком это необходимо для выполнения указанными представителями их функций.

5.1.4. Отдел бухгалтерского учёта и контроля отдела обрабатывает персональные данные работников отдела с целью формирования необходимой электронной отчетности, направляемой в отдел пенсионного фонда, налоговой службы по защищенным каналам связи.

5.2. При передаче персональных данных работника внутри структурного подразделения или в другое структурное подразделение Управления, информация ограничивается только теми персональными данными работника, которые необходимы для выполнения должностными лицами их функции.

5.3. Порядок приостановки предоставления персональных данных в случае обнаружения нарушений порядка их предоставления.

5.3.1. При обнаружении нарушений порядка предоставления персональных данных работник Управления должен немедленно приостановить предоставление персональных данных.

5.3.2. Начальник (либо лицо, исполняющее его обязанности) отдела назначает служебное расследование для выявления причин нарушения.

5.3.3. После устранения нарушений предоставление персональных данных возобновляется.

6. Хранение персональных данных

6.1. Персональные данные работников отдела обрабатываются и хранятся в отделе как на бумажных носителях, так и в электронном виде в локальных информационных системах.

7. Доступ к персональным данным

7.1. Доступ работников отдела к персональным данным ограничен. В отделе вводится разрешительная система доступа к персональным данным, согласно которой разрешается доступ только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

8. Порядок действий должностных лиц в случае обнаружения нарушений, угрожающих конфиденциальности обрабатываемых персональных данных

8.1. В случае обнаружения фактов несоблюдения условий хранения носителей персональных данных, неисправности средств защиты информации, нарушения порядка предоставления персональных данных или иных нарушений, угрожающих конфиденциальности обрабатываемых персональных данных (далее - инцидент информационной безопасности), обнаружившие инцидент работники отдела, осуществляющие обработку персональных данных, обязаны немедленно информировать о нем администратору информационной безопасности информационных систем персональных данных отдела.

8.9. Администратором информационной безопасности информационных систем персональных данных отдела составляется заключение по факту инцидента информационной безопасности, включающее в себя:исходное протоколирование инцидента;причины и следствия возникновения инцидента;меры, предпринятые для ликвидации инцидента и его последствий;предложения по внесению изменений в систему обеспечения безопасности информации.

9. Обязанности должностных лиц по обеспечению безопасности персональных данных

9.1. Ответственный за организацию работ по защите персональных данных в РОО назначается приказом начальника отдела.

9.2. Безопасность персональных данных при их обработке обеспечивают должностные лица отдела, определенные приказом отдела ответственными за осуществление мероприятий по защите персональных данных;

9.3. Работники РОО, осуществляющие обработку персональных данных в информационных системах, обязаны:

9.3.1. строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами информационных систем;

9.3.2. хранить в тайне свой пароль (пароли). В соответствии с разделом 11 настоящего Положения с установленной периодичностью менять свой пароль (пароли);

9.3.3. выполнять требования раздела 12 настоящего Положения в части касающейся действий пользователей рабочих станций информационной системы.

10. Правила учета средств защиты информации и носителей персональных данных.

10.1. Средства защиты информации, используемые в информационной системе персональных данных, подлежат учёту в журнале учёта средств защиты информации, в котором отражается:

наименования средств защиты; серийные (заводские) номера; наименование организаций, установивших средства защиты;место установки средств защиты информации.

11. Работники отдела, имеющие доступ к персональным данным, 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.

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

12. Правила антивирусной защиты:

12.1. В отделе допускаются к использованию только лицензионные антивирусные средства.

12.2. Установка и настройка параметров средств антивирусного контроля на компьютерах отдела осуществляется работниками отдела по обслуживанию рабочих мест

12.3. Ежедневно после включения компьютера (для серверов - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютера.

12.4. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, текстовые файлы любых форматов), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после её приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

12.6. 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 отдела самостоятельно или (при необходимости) вместе с работником отдела по обслуживанию рабочих мествнеочередной антивирусный контроль компьютера.

12.7. Ежедневно в автоматическом режиме должно проводиться обновление антивирусных баз

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

Работники отдела, виновные в нарушении норм настоящего Положения, а также законодательства Российской Федерации, регулирующего получение, обработку и защиту персональных данных работника, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.