СОГЛАСОВАНО
на заседании
Общего собрания работников
Протокол № 3
от «28» 08 2015 г.

УТВЕРЖДЕНО
Приказом директора МБУДО
«ДМШ № 2 г. Рубцовска»
№ 114.2-ос от 28.08.2015
Ефимец Л.Г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников МБУДО «ДМШ № 2 г. Рубцовска»

Подписано цифровой подписью: Ефимец Любовь Григорьевна
DN: cn=Ефимец Любовь Григорьевна, o=МБУДО "ДМШ № 2 г. Рубцовска", ou=директор, email=muz.schkola2@yandex.ru, c=RU
Дата: 2021.05.25 11:46:06 +07'00'

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных работников МБУДО «ДМШ № 2 г. Рубцовска» (далее – Учреждение) устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников Учреждения. Под работниками подразумеваются лица, заключившие трудовой договор с Учреждением.

1.2. Основанием для разработки настоящего Положения являются Конституция РФ, Трудовой кодекс РФ, Гражданский кодекс РФ, Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», Правила внутреннего трудового распорядка, Устав Учреждения.

1.3. Цель настоящего Положения – определение порядка обработки персональных данных работников Учреждения (штатных и привлеченных), защита персональных данных работников Учреждения от несанкционированного доступа и разглашения, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников.

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

1.5. Все работники Учреждения должны быть ознакомлены с настоящим Положением под роспись.

2. Основные понятия и состав персональных данных работников

2.1. В Положении используются следующие понятия:

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

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

2.1.3. 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.

2.1.4. 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.

2.1.5. 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.

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

2.1.7. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

2.1.9. 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.

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

2.1.11. Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу

Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

2.1.12. 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.

2.2. В состав персональных данных работников Учреждения входят:

- анкетные и биографические данные;
- данные о прохождении аттестации, повышения квалификации, результатов обучения и т.п.;
- образование, специальность, квалификация;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- данные обязательных предварительных и периодических осмотрах, медицинские заключения;
- занимаемая должность;
- наличие (отсутствие) судимости;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- личные дела и трудовые книжки сотрудников;
- запись с камер видеорегистратора.

2.3. 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 работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании и/или о квалификации;
- сведения о прохождении медицинских осмотров, медицинские заключения;
- свидетельство о присвоении ИНН (при его наличии у работника).

2.4. Информация, предоставляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму. При изменении своих персональных данных работник своевременно, либо в разумный срок, не превышающий пяти рабочих дней, обязан лично сообщить о происшедших изменениях ответственному за сбор информации.

2.4.1. Поверяется достоверность сведений, сверяя данные, представленные работником, с имеющимися документами, делаются копии представленных документов, подшиваются в личное дело работника, заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются анкетные и биографические данные работника.

2.4.2. В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации, повышении квалификации;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о месте жительства.

2.4.3. Документы, содержащие персональные данные работников, личные дела и трудовые книжки работников, копии отчетов, направляемые в государственные органы статистики, вышестоящие органы управления, хранятся у секретаря Учреждения.

2.4.4. Документация по организации работы (должностные инструкции, приказы, распоряжения, документы по планированию, учету, анализу и отчетности) с сотрудниками и персоналом хранятся у секретаря Учреждения.

2.4.5. Документы, содержащие персональные данные:

- сведения о заработной плате сотрудника;
- отчеты в налоговую инспекцию;
- отчеты в Пенсионный Фонд РФ;
- договоры о материальной ответственности;
- трудовые договоры;
- доверенности;
- кассовые документы (хранятся в бухгалтерии).

2.4.6. Учетные карточки работников, содержащие их персональные данные, хранятся у секретаря Учреждения.

2.4.7. Документы из пп. 2.4.3., 2.4.4., 2.4.5. и 2.4.6. хранятся в течение времени, предусмотренном номенклатурой дел Учреждения.

3. Сбор и обработка персональных данных

3.1. Обработка персональных данных работника – то получение, хранение, передача или любое другое использование данных работника.

3.2. Все персональные данные работника 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.

3.3. Должностное лицо работодателя 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.

3.4. Работник предоставляет работодателю достоверные сведения о себе. Должностное лицо работодателя проверяет достоверность сведений, сверяя данные, предоставленные работником с имеющимися у него документами. Предоставление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

3.5. Обработка указанных персональных данных работников работодателем возможна только с их согласия.

3.6. 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 целей;
- обработка данных необходима для защиты жизни, здоровья и иных жизненно важных интересов работника, если получение его согласия невозможно.

3.7. Личное дело ведется на протяжении всей трудовой деятельности работника. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

3.8. В случае выявления неправомерных действий с персональными данными работника:

- работник либо уполномоченный орган по защите прав субъектов персональных данных обращается к руководителю с заявлением;
- руководитель издает распоряжение о блокировании персональных данных, относящихся к соответствующему работнику, с момента такового обращения или получения запроса на период проверки, и назначает ответственного за проведение служебного расследования;
- если в ходе служебного расследования подтвердился факт использования недостоверных персональных данных, то работник, ответственный за обработку персональных данных и допустивший подобные действия, в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений данные работник в срок, не превышающий трех рабочих дней с даты такого выявления, обязан уничтожить персональные данные. Об устранении нарушений либо об

уничтожении персональных данных работник, ответственный за сбор персональных данных, обязан уведомить работника, в случае если запрос или обращение были направлены уполномоченным органом по защите прав субъектов персональных данных, – также указанный орган.

4. Передача и хранение персональных данных

4.1. При передаче персональных данных должностные лица должны соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья работника, а также в случаях, установленных федеральным законом;
- предупредить лица, получившие персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц того, что это правило соблюдено;
- разрешить доступ к персональным данным только специально уполномоченным лицам и только к тем данным, которые необходимы для выполнения конкретной функции;
- не запрашивать информацию о состоянии здоровья работника за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

4.2. Персональные данные обрабатываются и хранятся у секретаря Учреждения и в бухгалтерии в установленном порядке.

5. Защита персональных данных

5.1. 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.

5.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

5.3. Защита персональных данных представляет собой жестко регламентированный и динамически-технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

5.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральными законами.

5.5. Внутренняя защита:

5.5.1. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

5.5.2. Защита персональных данных сотрудника на электронных носителях – все папки, содержащие персональные данные сотрудника, должны быть защищены паролем.

5.6. Внешняя защита:

5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

5.6.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

– порядок приема, учета и контроля деятельности посетителей;
– пропускной режим организации;
– учет и порядок выдачи удостоверений;
– технические средства охраны, сигнализации;
– порядок охраны помещения.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

5.8. По возможности персональные данные обезличиваются.

5.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. Доступ к персональным данным работников

6.1. Внутренний доступ к персональным данным работника имеют:
– руководитель Учреждения;
– заместитель директора по учебно-воспитательной работе;
– секретарь (в обязанности которого входит работа с кадрами);
– работники бухгалтерии к тем данным, которые необходимы при выполнении обязанностей;
– другие сотрудники учреждения при выполнении ими своих служебных обязанностей;
– сам работник, носитель данных.

6.2. Внешний доступ.

Персональные данные вне организации могут предоставляться в государственные и негосударственные функциональные структуры:
– налоговые инспекции;
– правоохранительные органы;
– органы статистики;
– страховые агентства;
– военкоматы;
– органы социального страхования;
– пенсионные фонды;
– подразделения муниципальных органов управления.

6.3. Другие организации.

Сведения о работнике (в том числе уволенном) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

6.4. Родственники и члены семей.

Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

7. Ответственность за обработку и защиту персональных данных

7.1. Личные дела и документы, содержащие персональные данные работников, хранятся в закрывающихся шкафах, сейфах, обеспечивающих защиту от несанкционированного доступа.

7.2. Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

7.3. Передача информации, содержащей сведения о персональных данных работников, по телефону, факсу, электронной почте без письменного согласия работника запрещается.

7.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.