

ПРАВИЛА

обработки персональных данных в государственном бюджетном учреждении Ставропольского края «Спортивная школа олимпийского резерва по художественной гимнастике»

1. Общие положения

1.1. Обработка персональных данных может осуществляться исключительно в целях принятия решения о трудоустройстве, кадрового планирования, осуществления трудовых отношений, зачисления воспитанников для прохождения спортивной подготовки, присвоения воспитанникам спортивных разрядов, участия воспитанников в соревнованиях, и в случаях, установленных законодательством Российской Федерации.

1.2. При определении объема и содержания обрабатываемых персональных данных в государственном бюджетном учреждении Ставропольского края «Спортивная школа олимпийского резерва по художественной гимнастике» (далее – Учреждение) необходимо руководствоваться Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами Российской Федерации.

2. Порядок хранения персональных данных

2.1. Хранение электронных носителей (дискет, дисков и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

2.2. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

2.3. Обработка персональных данных в Учреждении осуществляется до утраты правовых оснований обработки персональных данных. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в Учреждении определяются Перечнем персональных данных в государственном бюджетном учреждении Ставропольского края «Спортивная школа олимпийского резерва по художественной гимнастике».

2.4. По истечении срока хранения документы, либо иные материальные носители персональных данных должны быть уничтожены без возможности восстановления (например, в бумагорезательных машинах) с составлением акта. Для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ без уничтожения материального носителя.

2.5. Обезличивания персональных данных в Учреждении не предполагается.

3. Порядок работы со сведениями, содержащими персональные данные

3.1. При обработке персональных данных на бумажных документах, съёмных носителях (дискетах, дисках, флеш-носителях и т.п.), компьютерах и других технических средствах, работники Учреждения обязаны следить как за сохранностью самих бумажных документов, съёмных носителей и компьютеров, и других технических средств, так и за сохранностью содержащейся в них информации, а именно не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с персональными данными.

3.2. Допуск к персональным данным субъекта могут иметь только те работники Учреждения, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких сотрудников отражен в Приказе об утверждении списка должностных лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей.

3.3. Процедура оформления допуска к персональным данным представляет собой истребование с сотрудника Обязательства о неразглашении конфиденциальной информации.

3.4. Каждый сотрудник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

3.5. Сотрудникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

3.6. Запрещается хранение или оставление бумажных документов и съёмных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий. Напечатанные документы, содержащие персональные данные, должны изыматься из принтеров немедленно. Хранение бумажных документов и съёмных носителей, содержащих персональные данные, допускается только в специальных закрытых шкафах, сейфах и помещениях, к которым исключён доступ лиц, не допущенных к обработке соответствующих персональных данных.

3.7. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съёмные носители.

3.8. Запрещается использовать для передачи персональных данных съёмные носители, не учтённые в Журнале учета носителей персональных данных в государственном бюджетном учреждении Ставропольского края «Спортивная школа олимпийского резерва по художественной гимнастике».

3.9. Запрещается выносить документы, съёмные носители или переносные компьютеры, содержащие персональные данные, за пределы служебных помещений Учреждения, если это не требуется для выполнения служебных (трудовых) обязанностей и если на это не дано разрешение руководителя Учреждения или ответственного за организацию обработки персональных данных.

3.10. Бумажные документы с персональными данными, у которых истёк срок хранения, лишние или испорченные копии документов с персональными данными,

должны быть уничтожены без возможности их восстановления (например, в shredders).

3.11. Большие объёмы бумажных документов с персональными данными, съёмные носители с персональными данными, а также встроенные в компьютеры носители с персональными данными должны уничтожаться под контролем ответственного за организацию обработки персональных данных, способом, исключающим дальнейшее восстановление информации.

3.12. Мониторы компьютеров, использующихся для обработки персональных данных, должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуск к обработке персональных данных.

3.13. Категорически запрещается упоминать в разговоре с третьими лицами сведения, содержащие персональные данные.

3.14. Запрещается в нерабочее время или за пределами служебных помещений упоминать в разговоре с кем-либо, включая любых работников Учреждения, сведения, содержащие персональные данные.

3.15. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки персональных данных, администратора безопасности информации, руководства, или лица, уполномоченного руководством на обсуждение данных вопросов.

3.16. Передавать персональные данные субъектов допускается только тем сотрудникам, которые имеют допуск к обработке персональных данных.

3.17. Предоставление персональных данных допускается в случаях передачи Федеральной налоговой службе, Фонду социального страхования России, Пенсионному фонду России, Банку с целью перечисления заработной платы, а также в иных случаях, установленных законодательством РФ.

3.18. Не допускается распространение персональных данных субъекта.

4. Уничтожение документов, содержащих персональные данные

4.1. Уничтожение документов, содержащих персональные данные, в том числе черновиков, бракованных листов и испорченных копий, производится назначенной комиссией с обязательной простановкой отметок об уничтожении в соответствующих учетных документах.

4.2. Порядок уничтожения черновиков, испорченных листов, неподписанных проектов документов, содержащих персональные данные:

а) черновики документов, испорченные листы, варианты и неподписанные проекты документов надрываются (возможно использование автоматических уничтожителей бумаги) и помещаются в урну (мешок).

б) по мере накопления содержимое урны (мешка) изымается работниками и уничтожается;

в) уничтожение документов, содержащих персональные данные, производится в строгом соответствии со сроками хранения;

г) разрешение на уничтожение дает комиссия;

д) при проведении экспертизы ценности документов перед их передачей на архивное состояние, отбор документов на уничтожение производит комиссия;

е) отобранные для уничтожения документы, содержащие персональные данные, вносятся в акт установленной формы, сверяются перед уничтожением работниками с учетными данными и уничтожаются;

ж) после уничтожения в учетных данных производятся отметки с указанием номера акта, даты уничтожения и подписи сотрудников, производивших уничтожение;

з) уничтожение документов, содержащих персональные данные, производится путем их сожжения или измельчения или другим путем исключающим восстановление текста документов.

5. Организация защиты персональных данных

5.1. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Учреждением за счет своих средств.

5.2. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

5.2.1. Проведение организационных мероприятий:

– разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

– организация учёта носителей персональных данных;

– проведение обучения сотрудников вопросам защиты персональных данных.

5.2.2. Программно-аппаратная защита:

– внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом №184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия.

5.2.3. Инженерно-техническая защита:

– установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

– установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

5.3. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами Учреждения.

6. Заключительные положения

6.1. Настоящие Правила утверждаются руководителем и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

6.2. Все сотрудники Учреждения, участвующие в обработке персональных данных с использованием средств автоматизации, должны быть ознакомлены с настоящими Правилами под роспись.