

<p><b>ПРИНЯТО:</b>          Протокол №5 от «15» мая 2017 г.          Собранием трудового коллектива          ГБФСУ КО          «СШОР по спортивной борьбе»</p>	<p style="text-align: right;"><b>УТВЕРЖДЕНО:</b>          Приказом № 101 § 5 от «01» сентября 2017г          Директор ГБФСУ КО «СШОР          по спортивной борьбе»</p> <p style="text-align: right;">           _____          А.С. Вертохвостов          Ф.И.О.</p>
--	---



## ПОЛОЖЕНИЕ

**О защите персональных данных работников  
 Государственного бюджетного физкультурно-спортивного  
 учреждения Кемеровской области «Спортивная школа  
 олимпийского резерва по спортивной борьбе»**

## 1. Основные положения

1.1. Настоящее положение о защите персональных данных занимающихся, поступающих и их родителей (законных представителей) (далее – Положение) разработано в соответствии с Конституцией РФ, Федеральным законом № 152-ФЗ от 27.07.2006 «О персональных данных», Федеральным законом №149-ФЗ от 27.07.2006 «Об информации, информатизации и защите информации», Федеральным законом №59-ФЗ от 02.05.2006 «О порядке рассмотрения граждан Российской Федерации», постановлением Правительства РФ №687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства РФ № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспертному контролю №21 от 18.02.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» в целях сохранения личной тайны и защиты персональных данных физического лица, вступившего в трудовые отношения (далее – Работник, Субъект персональных данных) с Государственным бюджетным физкультурно-спортивным учреждением Кемеровской области «Спортивная школа олимпийского резерва по спортивной борьбе» (далее – Учреждение, Оператор, Работодатель).

1.2. Положение определяет права и обязанности Учреждения и Работника, порядок использования информации, необходимых Работодателю в связи с трудовыми отношениями и касающейся конкретного работника в служебных целях, а также порядок взаимодействия по поводу сбора, документирования, хранения и уничтожения персональных данных Работников.

1.3. Основные понятия, используемые в настоящем положении:

*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;

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

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

*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 с помощью информационных технологий и технических средств;

*конфиденциальность персональных данных* – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным субъектов, требование не допускать их распространения без согласия субъекта или иного законного представителя.

## **2. Цели обработки персональных данных**

2.1. Обработка персональных данных в Учреждении осуществляется для достижения конкретных и законных целей.

2.2. Цели обработки, состав персональных данных и сроки их обработки утверждаются приказом руководителя Учреждения.

2.3. Не допускается обработка персональных данных, несовместимая с целями, для которых собирались персональные данные.

## **3. Сбор, обработка, хранение персональных данных работника и условия передачи третьим лицам**

3.1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных законодательством Российской Федерации. Обработка персональных данных допускается в следующих случаях:

а) обработка персональных данных осуществляется с согласия Работника на обработку его персональных данных;

б) обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

в) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

г) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

д) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

е) иных случаях, предусмотренных законодательством Российской Федерации.

3.2. Ответственный за организацию работы по защите персональных данных в учреждении, а также ответственные за обработку персональных данных работников назначаются приказом руководителя Учреждения.

3.3. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Оператором.

3.4. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии законных оснований.

3.5. В случаях, предусмотренных Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес Оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

3.6. Получение персональных данных Работника у третьих лиц возможно только при уведомлении работника об этом заранее и с его письменного согласия.

В уведомлении Работника о получении его персональных данных у третьих лиц должна содержаться следующая информация:

а) о целях получения персональных данных;

б) о предполагаемых источниках и способах получения персональных данных;

в) о характере подлежащих получению персональных данных;

г) о последствиях отказа Работника дать письменное согласие на их получение.

3.7. Работодатель не имеет права получать и обрабатывать персональные данные Работника о его политических, религиозных и иных убеждениях и частной жизни, а равно как персональные данные Работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации Работодатель вправе получать и обрабатывать данные о частной жизни Работника только с его письменного согласия.

3.8. 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.

3.9. Работники и их представители должны быть ознакомлены под расписку с документами Учреждения, устанавливающими порядок обработки персональных данных Работников, а также об их правах и обязанностях в этой области.

3.10. Сведения, содержащие персональные данные Работника, включаются в его личное дело, «Личную карточку работника» унифицированной формы Т-2, а также содержатся на электронных носителях информации, доступ к которым разрешен лицам, непосредственно использующим персональные данные работника в служебных целях. Перечень должностных лиц, доступ которых к персональным данным необходим для выполнения ими служебных (трудовых) обязанностей утверждается приказом руководителя Учреждения.

3.11. Должностные лица Учреждения имеют право получать только те персональные данные Работника, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц. Все остальные Работники имеют право на полную информацию только об их персональных данных и обработке этих данных.

3.12. Получение сведений о персональных данных Работников третьей стороной разрешается только при наличии заявления с указанием

конкретных персональных данных и целей, для которых они будут использованы, а также письменного согласия Работника, персональные данные которого затребованы.

3.13. Получение персональных данных Работника третьей стороной без его письменного согласия возможно в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровья Работника, а также в случаях, установленных законом.

3.14. Сообщение сведений о персональных данных Работников другим организациям и гражданам разрешается при наличии письменного согласия работника и заявления, подписанного руководителем организации либо гражданином, запросившим такие сведения.

3.15. Предоставление сведений о персональных данных Работников без соответствующего их согласия возможно в следующих случаях:

- а) в целях предупреждения угрозы жизни и здоровья Работника;
- б) при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях»;
- в) при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов.

3.16. Работник, о котором запрашиваются сведения, должен быть уведомлён о передаче его персональных данных третьим лицам, за исключением случаев, когда такое уведомление невозможно в силу форс-мажорных обстоятельств, а именно: стихийных бедствий, аварий, катастроф.

3.17. Запрещается передача персональных данных Работника в коммерческих целях без его согласия.

#### **4. Требования к неавтоматизированной обработке персональных данных**

4.1. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемых без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

4.2. Дополнительно, при неавтоматизированной обработке персональных данных на бумажных носителях:

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, должны формироваться в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутреннюю опись документов с указанием цели обработки и категории персональных данных.

4.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, на случай необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должны быть составлена таким образом, чтобы каждый из субъектов персональных данных, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.4. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществить обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

- при необходимости использования, распространения или предоставления определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению, предоставлению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению, предоставлению и использованию применяется (распространяется, предоставляется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

4.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих данных, зафиксированных на материальном носителе (удаление, вымарывание).

## **5. Защита персональных данных работника**

5.1. Должностные лица Работодателя обязаны принимать или обеспечивать принятие необходимых правовых, организационных и

технических мер для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий с ними. Указанные меры принимаются с учетом возможного вреда субъекту персональных данных, объема и характера обрабатываемых персональных данных, условий обработки персональных данных, актуальности угроз безопасности персональных данных, а также возможностей технической реализации этих мер.

5.2. Целями защиты информации являются:

а) предотвращение утечки, хищения, утраты, искажения, подделки информации;

б) предотвращение угроз безопасности личности, общества, государства;

в) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

г) предотвращение других форм незаконного вмешательства в информационные ресурсы Учреждения;

д) защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в Учреждении;

е) сохранение конфиденциальности документированной информации в соответствии с законодательством Российской Федерации.

5.3. Меры по обеспечению безопасности персональных данных включают в себя, в частности:

а) определение угроз безопасности персональных данных при их обработке;

б) применение методов (способов) защиты информации и прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

в) оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы;

г) учет машинных носителей персональных данных;

д) обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

е) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

ж) установление правил доступа к персональным данным, обрабатываемым в Учреждении, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

з) контроль принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5.4. С целью организации работы по защите персональных данных в Учреждении приказом руководителя назначается ответственный за безопасность информационных систем персональных данных.



5.5. Контроль за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных организуется и проводится в учреждении не реже 1 раза в 3 года.

#### **6. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований**

6.1. Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований (например, утратившие практическое значение), подлежат уничтожению.

6.2. Решение об уничтожении персональных данных принимает руководитель Учреждения, на основании представления ответственного за обработку персональных данных.

6.3. Уничтожение документов производится комиссией по проведению внутреннего контроля соответствия обработки персональных данных в учреждении требованиям к защите персональных данных.

6.4. Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

6.5. После уничтожения материальных носителей членами комиссии подписывается акт (приложение №1), делается запись в журналах их учета и регистрации, а также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт № \_\_\_ (дата)».

6.6. Уничтожение информации на машинных носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на персональных компьютерах с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

#### **7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными работника**

7.1. В случае нарушения норм, регулирующих получение, обработку, хранение, передачу и защиту персональных данных Работника администрацией Работодателя и иными лицами, они несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

7.2. К лицам, виновным в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника могут быть применены следующие дисциплинарные взыскания:

- а) замечание;
- б) выговор;
- в) предупреждение о неполном должностном соответствии;
- г) освобождение от занимаемой должности;
- д) увольнение.

7.3. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

Приложение №1 к положению  
о защите персональных данных  
работников ГБФСУ КО «СШОР  
по спортивной борьбе»

от \_\_\_\_\_ № \_\_\_\_\_

Форма Акта

об уничтожении персональных данных (материальных носителей, информации с носителей, информации из информационной системы персональных данных)

**УТВЕРЖДАЮ**  
Директор ГБФСУ КО «СШОР  
по спортивной борьбе»

\_\_\_\_\_ А.С. Вертохвостов  
(подпись)  
« \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**АКТ № \_\_\_\_\_**

об уничтожении персональных данных  
субъекта(ов) персональных данных, обрабатываемых

в \_\_\_\_\_

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

составила настоящий Акт о том, что информация, зафиксированная на перечисленных в нем носителях информации (электронных, бумажных<sup>1</sup>), подлежат уничтожению.

Учетный номер материального носителя, номер дела и т.д.	Причина уничтожения носителя информации; стирания/обезличивания информации	Тип носителя информации	Производимая операция (стирание, уничтожение, обезличивание)	Дата
1	2	3	4	5

Всего подлежит уничтожению \_\_\_\_\_ носителей  
(цифрами и прописью)

Правильность произведенных записей в акте проверена.

Регистрационные данные на носителях информации перед уничтожением (стиранием с них информации) с записями в акте сверены, произведено уничтожение путем:

\_\_\_\_\_  
(стирания на устройстве гарантированного уничтожения информации, разрезания, сжигания, механического уничтожения, вымарывания и т.п.)

Отметки о стирании информации (уничтожении носителей информации) в учетных формах произведены.

Председатель комиссии: \_\_\_\_\_ / \_\_\_\_\_ /

Члены комиссии: \_\_\_\_\_ / \_\_\_\_\_ /

Примечание:

1. Акт составляется отдельно на каждый способ уничтожения носителей.
2. Все листы акта, а так же все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

<sup>1</sup> В случае, если объем уничтожаемых документов позволяет перечислять их в Акте.