Приложение 1
к приказу начальника
Управления по ФКС и Т
Администрации г. Челябинска

от _28.12.2015___ № _4/176____

Положение
об обработке персональных данных с использованием средств автоматизации в Управлении по физической культуре, спорту и туризму Администрации города Челябинска

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке персональных данных с использованием средств автоматизации (далее — Положение) в Управлении по физической культуре, спорту и туризму Администрации города Челябинска (далее – Управление) разработано в соответствии с Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 № 197-ФЗ, Гражданским кодексом Российской Федерации от 30.11.1994 № 51-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации.

1.2. Цели разработки Положения:

1.2.1. определение порядка обработки персональных данных сотрудников Управления, а также иных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий Управления;

1.2.2. обеспечение защиты прав и свобод человека и гражданина, в т.ч. сотрудников Управления, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

1.2.3. установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

1.3.1. обезличенных персональных данных;

1.3.2. общедоступных персональных данных.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, или продлевается на основании заключения экспертной комиссии Управления, если иное не определено законом Российской Федерации.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Доступ к информации – возможность получения информации и ее использования.

2.2. Информационная система персональных данных (далее ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.3. Информация – сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

2.5. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.6. 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 (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.7. 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 (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.8. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.9. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.10. Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

III. ПОРЯДОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Хранение 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.

3.2. 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.

3.3. Обработка персональных данных в Управлении осуществляется до утраты правовых оснований обработки персональных данных. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в Управлении определяются «Перечнем сведений, содержащих персональные данные и правовые основания обработки персональных данных».

3.4. По истечении срока хранения (30 дней, если иное не прописано в нормативно-правовых актах) для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ (например, «Safe Erase», «Eraser», «FDelete») без уничтожения материального носителя.

3.5. Обезличивания персональных данных в Управлении не предполагается.

IV. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка персональных данных может осуществляться исключительно в целях вида деятельности организации по уставным документам, принятия решения о трудоустройстве, кадрового планирования, осуществления трудовых отношений, и в случаях, установленных законодательством Российской Федерации.

4.2. При определении объема и содержания, обрабатываемых персональных данных Управления должен 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, а также настоящим Положением.

V. ПОРЯДОК ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

5.2. Предоставление персональных данных допускается в соответствии с законодательством Российской Федерации.

5.3. Не допускается распространение персональных данных субъекта.

VI. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

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

6.2.1. Проведение организационных мероприятий:

6.2.1.1. 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;

6.2.1.2. Ознакомление сотрудников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

6.2.1.3. Организация учёта носителей персональных данных;

6.2.1.4. Разработка модели угроз безопасности персональным данным;

6.2.1.5. Проведение обучения сотрудников вопросам защиты персональных данных.

6.2.2. Программно-аппаратная защита:

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

6.2.3. Инженерно-техническая защита:

6.2.3.1. Установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

6.2.3.2. Установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

6.3. 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 Управления.

6.4. Организацию и контроль защиты персональных данных в структурных подразделениях Управления осуществляют их непосредственные руководители.

VII. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

7.1. Допуск к персональным данным субъекта могут иметь только те сотрудники Управления, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких сотрудников утвержден приказом начальника Управления.

7.2. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

7.2.1. Ознакомление сотрудника с настоящим Положением, «Правилами обработки персональных данных» и другими локальными нормативно-правовыми актами Управления, касающимися обработки персональных данных;

7.2.2. Истребование с сотрудника «Обязательства о неразглашении информации ограниченного доступа»;

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

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

VIII. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

8.1. При обработке персональных данных в информационной системе должно быть обеспечено:

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

8.1.2. Своевременное обнаружение фактов несанкционированного доступа к персональным данным;

8.1.3. Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

8.1.4. Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8.1.5. Постоянный контроль над обеспечением уровня защищенности персональных данных.

8.2. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

8.2.1. Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

8.2.2. Разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

8.2.3. Проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

8.2.4. Установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

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

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

8.2.7. Учет лиц, допущенных к работе с персональными данными в информационной системе;

8.2.8. Контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

8.2.9. Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

8.2.10. Описание системы защиты персональных данных.

8.3. Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе уполномоченным лицом возлагается на старшего программиста Управления.

8.4. Список лиц, имеющих доступ к персональным данным, уполномоченных на обработку этих данных и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных, утверждается приказом начальника Управления.

8.5. При обнаружении нарушений порядка предоставления персональных данных уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

8.6. Иные требования по обеспечению безопасности информации и средств защиты информации в Управлении выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти субъекта РФ, в котором находится Оператор.

IX. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Состав информационных систем персональных данных Управления определяется «Перечнем информационных систем персональных данных».

9.2. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

9.3. Безопасность персональных данных достигается путем 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.

9.4. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

9.5. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

9.6. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

9.7. Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки персональных данных в ИСПДн (администратор безопасности ИСПДн).

9.8. При обработке персональных данных в информационной системе должно быть обеспечено:

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

9.8.2. Своевременное обнаружение фактов несанкционированного доступа к персональным данным;

9.8.3. Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

9.8.4. Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

9.8.5. Постоянный контроль над обеспечением уровня защищенности персональных данных.

9.9. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

9.9.1. Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

9.9.2. Разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

9.9.3. Проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

9.9.4. Установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

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

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

9.9.7. Учет лиц, допущенных к работе с персональными данными в информационной системе;

9.9.8. Контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

9.9.9. Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

9.9.10. Описание системы защиты персональных данных.

9.10. Иные требования по обеспечению безопасности информации и средств защиты информации в Управлении выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти субъекта РФ, в котором находится Оператор.

X. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на

пользователей ИСПДн, администратора безопасности ИСПДн и ответственного за организацию обработки персональных данных Управления.

10.2. Сотрудники Управления, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

10.2.1. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами Сокращенное наименование организации, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник Управления, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Управления (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

10.2.2. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях Российской Федерации.

10.2.3. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса Российской Федерации.

10.3. Начальник Управления за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

XI. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Все сотрудники Управления, участвующие в обработке персональных данных с использованием средств автоматизации, должны быть ознакомлены с настоящим Положением под подпись.

Приложение:
1. Инструкция пользователя информационной системы персональных данных на 3 л. в 1 экз.,
2. Лист ознакомления с «Положением о порядке обработки персональных данных с использования средств автоматизации» на 2 л. в 1 экз.

Приложение
к Положению о порядке
обработки персональных
данных с использования
средств автоматизации
от 28 декабря 2015 г.

ЛИСТ ОЗНАКОМЛЕНИЯ с
«Положением об обработке персональных данных с использованием средств автоматизации»

Дата ознакомления	ФИО сотрудника, ознакомившегося с документом	Должность сотрудника, ознакомившегося с документом	Подпись сотрудника, ознакомившегося с документом
1	2	3	4

1	2	3	4