

УТВЕРЖДАЮ

Директор МБОУ ДО ГДЮСШ МО

г. Краснодар

 В.Э. Шо:лухов

«

_____ 2017 г.

М.П.

**ПОЛИТИКА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

г. Краснодар

2017 г.

Содержание

1. Общие положения 3
2. Основные термины и понятия, используемые в локальных документах Организации, принимаемых по вопросу обработки персональных данных..... 5
3. Источники нормативного правового регулирования вопросов обработки персональных данных 7
4. Общие условия обработки персональных данных 10

1. Общие положения

1.1. Политика обработки персональных данных в ИС МБОУ ДО ГДЮСШ МО г. Краснодар (далее – Политика) детализирует положение Политики информационной безопасности МБОУ ДО ГДЮСШ МО г. Краснодар (далее – Организация) в области обработки и обеспечения безопасности персональных данных (далее – ПДн).

1.2. Политика обработки персональных данных:

- является основополагающим внутренним документом Организации, регулирующим вопросы обработки персональных данных;
- разработана в целях обеспечения соответствия с законодательством Российской Федерации обработки, хранения и защиты ПДн сотрудников, граждан.

1.3. Настоящей Политикой в своей работе должны руководствоваться все сотрудники Организации, осуществляющие обработку персональных данных.

1.4. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

- пересмотр положений настоящей Политики должен осуществляться не реже одного раза в 24 месяца;
- внеплановое внесение изменений в настоящую Политику может производиться в случае изменения действующего законодательства и иных нормативных актов в области обработки и обеспечения безопасности персональных данных, либо при существенном изменении процессов обработки персональных данных.

1.5. Ответственным за внесение изменений в настоящую Политику является начальник отдела информационной безопасности Организации.

1.6. Контроль за выполнением требований данной Политики осуществляет ответственный за обеспечение информационной безопасности и обработку персональных данных Организации.

2. Основные термины и понятия, используемые в локальных документах Организации, принимаемых по вопросу обработки персональных данных

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации, Перечнем ПДн, обрабатываемых в Организации, локальными актами Организации.

2.2. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

2.3. Распространение персональных данных – действия, направленные на раскрытие ПДн неопределенному кругу, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом.

2.4. Предоставление персональных данных – действия, направленные на раскрытие ПДн определенному кругу.

2.5. Использование персональных данных – действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом, затрагивающих права и свободы субъекта ПДн или других лиц.

2.6. Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

2.7. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе и (или) в результате которых уничтожаются материальные носители ПДн.

2.8. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

2.9. Информационная система персональных данных – информационная система, представляющая собой совокупность содержащихся в базе данных ПДн и их обработку, информационных технологий и технических средств.

2.10. Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем.

2.11. Общедоступные персональные данные – ПДн, доступ неограниченного круга лиц, к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.12. Трансграничная передача персональных данных – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Источники нормативного правового регулирования вопросов обработки персональных данных

3.1. Политика Организации в области обработки персональных данных определяется на основании следующих нормативных правовых актов РФ:

- Конституция Российской Федерации;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15 сентября 2008 г № 687;
- Указ Президента Российской Федерации от 30.05.2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;
- Постановление Правительства Российской Федерации от 06.06.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденное Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119;

– Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

– Указ Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера»;

– Трудовой кодекс Российской Федерации;

– Гражданский кодекс Российской Федерации;

– Налоговый кодекс Российской Федерации;

– Уголовный кодекс Российской Федерации;

– нормативные и методические документы ФСБ России, ФСТЭК России, Роскомнадзора.

3.2. Во исполнение настоящей Политики в Организации утверждаются следующие локальные нормативные правовые акты:

– Инструкция администратора информационной безопасности информационных систем;

– Инструкция администратора информационных систем;

– Инструкция по организации антивирусной защиты информационных систем;

– Перечень сведений конфиденциального характера, обрабатываемых в Организации;

– План мероприятий по защите персональных данных;

– Положение о порядке обработки и обеспечения безопасности персональных данных, обрабатываемых в государственных информационных системах Организации;

– Акт классификации государственных информационных систем Организации;

– Модель угроз и нарушителя безопасности информации Организации;

– иные локальные документы Организации, принимаемые во исполнение требований, действующих нормативных правовых актов

Российской Федерации в области обработки персональных данных.

4. Общие условия обработки персональных данных

4.1 Обработка ПДн в Организации осуществляется на основе следующих принципов:

4.1.1 Законности и справедливости обработки ПДн.

4.1.2 Законности целей и способов обработки ПДн и добросовестности.

4.1.3 Соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Организации.

4.1.4 Соответствия содержания и объема обрабатываемых ПДн целям обработки ПДн.

4.1.5 Достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн.

4.1.6 Недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.1.7 Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.1.8 Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.1.9 Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.1.10 Субъект ПДн является собственником своих ПДн и самостоятельно решает вопрос передачи Организации своих ПДн.

4.1.11 Держателем ПДн является Организация, которой субъект ПДн передает во владение свои ПДн. Организация выполняет функцию владения

этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

4.1.12 Комплекс мер по защите ПДн направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности ПДн и обеспечивает безопасность информации в процессе деятельности Организации.

4.1.13 Организация при обработке ПДн обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИСПДн.

4.1.14 Мероприятия по защите ПДн определяются частными политиками, приказами, инструкциями и другими внутренними документами Организации.

4.2 Для защиты ПДн в Организации применяются следующие принципы и правила:

4.2.1 Ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей ПДн.

4.2.2 Строгое избирательное и обоснованное распределение документов и информации между сотрудниками.

4.2.3 Рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации.

4.2.4 Знание сотрудниками требований нормативно-методических документов по защите ПДн.

4.2.5 Распределение персональной ответственности между сотрудниками, участвующими в обработке ПДн, за выполнение требований

по обеспечению безопасности ПДн.

4.2.6 Установление режима конфиденциальности в соответствии с требованиями по обеспечению безопасности ПДн при работе с конфиденциальными документами и базами данных.

4.2.7 Определение угроз безопасности персональных данных при их обработке в государственных информационных системах.

4.2.8 Исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка ПДн и находится соответствующая вычислительная техника.

4.2.9 Организация порядка уничтожения персональных данных.

4.2.10 Своевременное выявление нарушений требований разрешительной системы доступа.

4.2.11 Воспитательная и разъяснительная работа с сотрудниками отделов по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

4.2.12 Регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн.

4.2.13 Ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся ПДн.

4.2.14 Создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

4.2.15 Резервирование защищаемых данных (создание резервных копий).

4.3. Правовое основание обработки персональных данных:

4.3.1 Конституция Российской Федерации.

4.3.2 Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

4.3.3 Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите

информации».

4.3.4 Федеральный закон Российской Федерации от 27.07.2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации».

4.3.5 Указ Президента Российской Федерации от 30.05.2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

4.3.6 Указ Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера».

4.3.7 Трудовой кодекс Российской Федерации.

4.3.8 Гражданский кодекс Российской Федерации.

4.3.9 Налоговый кодекс Российской Федерации.

4.3.10 Уголовный кодекс Российской Федерации.