УТВЕРЖДЕНО:
Приказом МАОУ ДО
ЦТР и ГО «Гармония»
от 07.06.2017 № 224

ПОЛОЖЕНИЕ
о недопущении оператором вреда при обработке персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об обработке персональных данных издано и применяется Муниципальным автономным образовательным учреждением дополнительного образования Центр творческого развития и гуманитарного образования «Гармония» (далее "Оператор") в соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных".

1.2. Настоящее Положение устанавливает процедуры, направленные на выявление причин, которые могут повлечь причинение вреда субъекту персональных данных и/или оператору и их предотвращение, а также на устранение последствий такого вреда при обработке персональных данных.

1.3. Под вредом для целей настоящего Положения понимается моральный вред и/или материальный ущерб субъекта персональных данных и/или оператора, который реально причинен или может быть причинен в случае нарушения оператором требований Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - "вред"). Размер вреда определяется в соответствии со ст. ст. 15, 151, 152, 1101 Гражданского кодекса Российской Федерации. Соотношение вреда и принимаемых оператором мер, направленных на предупреждение, недопущение и/или устранение его последствий, установлены настоящим Положением.

1.4. Недопущение вреда является одним из направлений обеспечения общей безопасности оператора и представляет собой комплекс правовых, организационных и технических мер. Правовые меры состоят из изучения и применения законодательства по вопросам недопущения вреда, разработки локальных актов и их применения в данной сфере деятельности оператора. Организационные меры включают тщательный отбор, обучение и расстановку кадров, повышение их мотивации в вопросах недопущения вреда. Технические меры объединяют создание условий и реализацию мероприятий по недопущению вреда, в том числе:

1.4.1. Обеспечение сохранности собственности оператора, в том числе материальных носителей информации, путем установления и поддержания соответствующих режимов безопасности.

1.4.2. Недопущение попадания конфиденциальной информации оператора, в том числе информации, составляющей коммерческую и служебную тайны, неуполномоченным лицам путем выделения специальных помещений для обработки и хранения персональных данных.

1.4.3. Обеспечение информационной безопасности оператора, бесперебойного функционирования технических средств обработки персональных данных. 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 (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

1.4.4. Обеспечение физической защиты объектов, находящихся на балансе оператора, путем установления внутриобъектового и пропускного режимов и режима взрыво- и пожаробезопасности.

1.4.5. Обеспечение физической защиты работников оператора при исполнении ими служебных обязанностей, комфортного морально-психологического климата и обстановки делового сотрудничества среди работников оператора.

1.4.6. Обеспечение личной безопасности руководителей оператора.

1.4.7. Незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.4.8. Постоянный контроль за обеспечением уровня защищенности персональных данных.

1.5. В целях недопущения вреда оператор до начала обработки персональных данных назначает ответственного за организацию обработки персональных данных в должности не ниже начальника структурного подразделения (или: заместителя руководителя оператора), именуемого далее "куратор ОПД".

1.5.1. Куратор ОПД получает указания непосредственно от исполнительного органа оператора и подотчетен ему.

1.5.2. Куратор ОПД осуществляет внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

1.5.3. Куратор ОПД проводит ориентировочную оценку размера вреда, устанавливает, какие меры были приняты в целях недопущения вреда, и их соотношение.

1.6. Руководящими документами при обработке персональных данных в первую очередь являются ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Постановление Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15.09.2008 N 687, Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная Заместителем директора ФСТЭК России 14.02.2008, Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные руководством 8 Центра Федеральной службы безопасности Российской Федерации от 21.02.2008 N 149/54-144.

1.7. Настоящее Положение и изменения к нему утверждаются руководителем оператора и вводятся приказом оператора.

1.8. Сотрудники оператора, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены под роспись до начала работы с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, с данным Положением и изменениями к нему. Обучение указанных работников организуется структурным подразделением по повышению квалификации в соответствии с утвержденными оператором графиками.

1.9. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного руководителем Оператора.

1.10. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в п. 1.9 настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется

соответствующими должностными лицами (работниками) оператора.

1.11. В целях предотвращения и уменьшения вреда при обнаружении нарушений порядка предоставления персональных данных оператор незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

1.12. Режим конфиденциальности персональных данных оператор обеспечивает в соответствии с Положением оператора о конфиденциальности.

1.13. Контроль за соблюдением сотрудниками оператора требований законодательства и положений локальных нормативных актов оператора организован в соответствии с Положением о внутреннем контроле оператора при обработке персональных данных.

1.14. Аудит соблюдения оператором требований законодательства и положений локальных нормативных актов оператора организован в соответствии с Положением оператора об аудите при обработке персональных данных.

1.15. Опубликование или обеспечение иным образом неограниченного доступа к настоящему Положению, иным документам, определяющим политику оператора в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных оператор проводит в соответствии с Положением оператора о раскрытии информации.

2. СТРУКТУРНЫЕ ПОДРАЗДЕЛЕНИЯ ОПЕРАТОРА ПО НЕДОПУЩЕНИЮ ВРЕДА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработку персональных данных, в том числе реализацию общих мер по недопущению вреда, организует Комиссия по организации работы с персональными данными (далее - "Комиссия").

2.2. Реализация специальных мер по недопущению вреда возложена на Комиссию.

2.4. Комиссия находится в непосредственном подчинении директора Оператора.

2.5. Состав, уровень квалификации сотрудников Комиссии, их, функции установлены Приказом о создании комиссии.

2.6.Комиссия:

1) координирует действия всех подразделений и работников оператора по вопросам недопущения вреда;

2) организует правовое, методическое и техническое сопровождение обработки персональных данных сотрудниками оператора с целью недопущения вреда;

3) рассматривает обращения и запросы субъектов персональных данных, которым причинен вред, принимает меры по устранению его последствий.

2.7. Контроль за деятельностью возложен на руководителя Оператора.

3. ПРОЦЕДУРЫ ПО НЕДОПУЩЕНИЮ ВРЕДА И ПО УСТРАНЕНИЮ ЕГО ПОСЛЕДСТВИЙ

3.1. Процедуры, направленные на предупреждение вреда:

3.1.1. Соблюдение должностными лицами и сотрудниками оператора установленных законодательством и локальными актами оператора регламентов получения, обработки, хранения, предоставления и распространения персональных данных (далее - "регламент").

3.1.2. Выявление нарушений со стороны сотрудников и/или субъектов персональных данных установленных регламентов и доведение информации о нарушениях до комиссии по организации работы с персональными данными.

3.1.3. Разработка и утверждение оператором правил определения возможных форм причинения вреда и оценки его размера.

3.1.4. Ознакомление сотрудников оператора с правилами определения возможных форм причинения вреда и оценки его размера.

3.1.5. Предупреждение субъектов персональных данных о рисках причинения вреда

в ходе обработки персональных данных.

3.1.6. Внеочередной инструктаж всех сотрудников оператора по вопросам недопущения вреда в случае обнаружения факта причинения вреда.

3.2. Процедуры, направленные на устранение вреда:

3.2.1. Своевременное обнаружение допущенных нарушений регламентов и незамедлительное пресечение таких нарушений.

3.2.2. Оценка уже причиненного вреда, фиксация мер, принятых оператором по недопущению вреда, и их сопоставление.

3.2.3. Информирование субъектов персональных данных о допущенных нарушениях, о рисках и о подлежащих принятию мерах.

3.2.4. Компенсация причиненного вреда на основе определенных оператором форм причинения вреда и оценки его размера.

3.2.5. Привлечение к ответственности сотрудников оператора, допустивших причинение вреда.

3.3. Процедуры, направленные на устранение последствий вреда:

3.3.1. Восстановление деловой репутации оператора.

3.3.2. Корректировка регламентов и программ обучения сотрудников.

4. ОБЯЗАННОСТИ РУКОВОДИТЕЛЯ И РАБОТНИКОВ ОПЕРАТОРА

4.1. Руководитель оператора:

- оказывает содействие комиссии в выполнении им своих обязанностей;
- организует устранение выявленных нарушений законодательства Российской Федерации, нормативных правовых актов уполномоченного федерального органа исполнительной власти, внутренних документов оператора, а также причин и условий, способствовавших совершению нарушения;
- организует рассмотрение случаев причинения вреда и выплату компенсаций.

4.2. Сотрудники оператора:

- оказывают содействие комиссии в выполнении им своих обязанностей;
- незамедлительно доводят до сведения своего непосредственного руководителя и комиссию (в части их компетенции) сведения обо всех случаях причинения вреда другими сотрудниками оператора или контрагентами оператора.

5. КОНТРОЛЬ, ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ИЛИ НЕИСПОЛНЕНИЕ ПОЛОЖЕНИЯ

5.1. Контроль за исполнением Положения возложен на Комиссию по организации работы с персональными данными.

5.2. Лица, нарушающие или не исполняющие требования Положения, привлекаются к дисциплинарной, административной (ст. ст. 5.39, 13.11, 13.14 Кодекса Российской Федерации об административных правонарушениях) или уголовной ответственности (ст. ст. 137, 272, 274 Уголовного кодекса Российской Федерации).

5.3. Руководители структурных подразделений оператора несут персональную ответственность за исполнение обязанностей их подчиненными.