

УТВЕРЖДАЮ

Председатель

Ассоциации родителей по развитию и
поддержке образования «Содействие»



Е.В. Смирнова

« 27



2024 г.

ПОЛИТИКА

**в отношении обработки персональных данных
в Ассоциации родителей по развитию и
поддержке образования «Содействие»**

г. Йошкар-Ола
2024

Содержание

I.	Общие положения	3
II.	Термины и определения	3
III.	Правовые основания обработки персональных данных	6
IV.	Принципы обработки персональных данных	6
V.	Цели обработки персональных данных	8
VI.	Категории и перечень обрабатываемых персональных данных. Субъекты персональных данных	8
VII.	Порядок и способы обработки персональных данных	9
VIII.	Сроки обработки и хранения персональных данных, порядок их уничтожения	11
IX.	Меры обеспечения конфиденциальности и безопасности персональных данных. 12	
X.	Права субъектов персональных данных	13
XI.	Права и обязанности оператора персональных данных	14
XII.	Ответственность	16
XIII.	Актуализация документа	16
XIV.	 Нормативные и правовые акты, в соответствии с которыми определяется Политика обработки персональных данных	16

I. Общие положения

Настоящая Политика в отношении обработки персональных данных в Ассоциации родителей по развитию и поддержке образования «Содействие» (далее – Политика), является официальным документом и разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных в Ассоциации родителей по развитию и поддержке образования «Содействие» (далее – Ассоциация).

В Политике определены требования к работникам Ассоциации, степень ответственности работников, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных Ассоциации.

Действие Политики распространяется на все процессы Ассоциации, в которых осуществляется обработка персональных данных и обязательна для ознакомления и исполнения всеми работниками Ассоциации, осуществляющими обработку персональных данных в процессе выполнения должностных обязанностей.

Политика является основой для организации обработки и защиты персональных данных, в том числе для разработки дополнительных документов, развивающих положения настоящей Политики в части организации обработки и защиты персональных данных.

Политика определяет:

- ▣ правовые основания обработки персональных данных;
- ▣ принципы обработки персональных данных, которыми руководствуется Ассоциация;
- ▣ цели обработки персональных данных;
- ▣ категории и перечень обрабатываемых персональных данных;
- ▣ категории субъектов персональных данных, персональные данные которых обрабатываются;
- ▣ порядок и способы обработки персональных данных;
- ▣ сроки обработки и хранения персональных данных, порядок их уничтожения;
- ▣ меры обеспечения конфиденциальности и безопасности персональных данных;
- ▣ права и обязанности Ассоциации, как оператора персональных данных, и субъектов персональных данных.

Ознакомление с положениями настоящей Политики осуществляется под подпись всеми работниками Ассоциации.

Настоящая Политика является общедоступным документом и подлежит размещению на официальном ресурсе Ассоциации, размещенном в информационно-телекоммуникационной сети «Интернет» (далее – сайт).

Доступ к Политике не может быть ограничен.

II. Термины и определения

В настоящей Политике используются следующие термины и определения:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и до-

ступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Доступ к информации – возможность получения информации и её использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Источник угрозы безопасности персональных данных – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности персональных данных.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не распространять их без согласия субъекта персональных данных или наличия иного законного основания.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному 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.

Объект вычислительной техники – стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации. К объектам вычислительной техники относятся автоматизированные системы, автоматизированные рабочие места, информационно-вычислительные центры и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть

отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

Оператор персональных данных – 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. В настоящей Политике оператором является Ассоциация.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты персональных данных.

Субъекты персональных данных – работники, обучающиеся и другие лица.

Технические средства информационной системы персональных данных – 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.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через

физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

В случае отсутствия используемого далее по тексту Политики термина, толкование и применение данного термина осуществляется в соответствии с положениями применимых нормативных правовых актов РФ.

III. Правовые основания обработки персональных данных

Правовыми основаниями обработки персональных данных в Ассоциации в зависимости от целей процесса обработки являются:

- Конституция Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Гражданский Кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Федеральный закон от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ;
- Устав Ассоциации;
- согласие субъекта (представителя субъекта) на обработку персональных данных;

Целью настоящей Политики является обеспечение безопасности персональных данных Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

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.

Информация и связанные с ней ресурсы должны быть доступны только для авторизованных пользователей. В информационных системах персональных данных должно осуществляться своевременное обнаружение угроз и реагирование на угрозы безопасности персональных данных.

В информационных системах персональных данных необходимо исключить возможность преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Перечень персональных данных, подлежащих защите, определен в Положении об обработке персональных данных в ГАОУ Республики Марий Эл «Лицей Бауманский».

IV. Принципы обработки персональных данных

Система защиты персональных данных строится на основании:

- Перечня персональных данных, подлежащих защите;
- Перечня информационных систем персональных данных;
- Акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных;

- Частной модели угроз и нарушителя безопасности персональных данных;
- Положения о разграничении прав доступа к обрабатываемым персональным данным;

На основании этих документов определяется необходимый уровень защищенности персональных данных в каждой информационной системе персональных данных Учреждения. Для каждой информационной системы персональных данных должен быть составлен список используемых технических средств, а также программного обеспечения участвующего в обработке персональных данных, подлежащих защите.

В зависимости от уровня защищенности персональных данных в информационной системе персональных данных и актуальных угроз, система защиты персональных данных может включать следующие технические и программные средства:

- антивирусные средства для объектов вычислительной техники;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами информационной системы персональных данных и операционных систем, прикладным программным обеспечением и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление доступом и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений.

Список используемых средств должен поддерживаться в актуальном состоянии. Все изменения состава системы защиты персональных данных или элементов информационных систем персональных данных должны быть согласованы с Администратором информационной безопасности.

Обработка персональных данных в Ассоциации осуществляется на основе следующих принципов:

- обработка осуществляется на законной и справедливой основе;
- ограничивается достижением конкретных, заранее определенных и законных целей. Обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается;
- объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой, не допускается;
- обработке подлежат только те персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям их обработки и не является избыточным;
- при обработке персональных данных обеспечивается их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки;
- принимаются необходимые меры (либо обеспечивается их принятие) по удалению или уточнению неполных, или неточных данных;
- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом, обрабатываемые персональные данные уничтожаются либо обезличиваются.

V. Цели обработки персональных данных

Обработка персональных данных осуществляется на основе принципа соответствия объема и категории обрабатываемых персональных данных, а также способов их обработки заявленным целям.

Цели обработки персональных данных определяются исходя из анализа правовых актов, регламентирующих деятельность Ассоциации, целей фактически осуществляемой Ассоциацией деятельности, а также деятельности, которая предусмотрена учредительными документами.

Ассоциация осуществляет обработку персональных данных в следующих целях:

- организация, обеспечение и регулирование трудовых и непосредственно связанных с ними отношений в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, а также Уставом и внутренними документами Ассоциации, обеспечения личной безопасности работников, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам;
- привлечение и отбор кандидатов для трудоустройства, принятие решения о возможности заключения трудового договора с соискателями должностей;
- обеспечение и осуществление взаимодействия с третьими лицами/членами Ассоциации по вопросам заключения договоров и в рамках исполнения обязательств по договорам;
- выполнение действий (обязательств) по поступившим обращениям субъектов персональных данных, отправка почтовых и/или курьерских отправок;
- исполнение запросов надзорных/контролирующих органов, подлежащих исполнению в соответствии с законодательством Российской Федерации;
- выполнение иных целей, предусмотренных уставом Ассоциации.

VI. Категории и перечень обрабатываемых персональных данных. Субъекты персональных данных

Категории и перечень обрабатываемых персональных данных соответствует заявленным целям обработки. Обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки.

Ассоциация обрабатывает персональные данные, относящиеся к следующим категориям:

- персональные данные, разрешенные субъектом для обработки;
- иные персональные данные.

Обработка биометрических персональных данных не осуществляется.

Ассоциация обрабатывает персональные данные следующих категорий субъектов персональных данных:

- кандидаты на соискание вакантных должностей;
- работники Ассоциации, в том числе бывшие работники Ассоциации;
- представители контрагентов;
- члены Ассоциации.

Перечень обрабатываемых персональных данных по категориям субъектов персональных данных содержится в соглашениях субъектов персональных данных на обработку их персональных данных.

VII. Порядок и способы обработки персональных данных

Обработка персональных данных осуществляется в соответствии с требованиями законодательства Российской Федерации и с соблюдением требований конфиденциальности, установленных ст. 7 152-ФЗ.

К обработке персональных данных допускаются работники Ассоциации, в чьи должностные обязанности входит обработка персональных данных.

Ассоциация осуществляет обработку персональных данных с использованием средств автоматизации и без использования средств автоматизации. При этом исключается принятие решений на основании исключительно автоматизированной обработки персональных данных, которые порождают юридические последствия в отношении субъекта персональных данных, или иным образом затрагивают его права и законные интересы.

Обработка персональных данных включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Обработка персональных данных осуществляется с согласия субъекта персональных данных, а также в случаях, установленных законодательством Российской Федерации (если предоставление персональных данных является обязательным соответствии с федеральными законами). Обработка персональных данных осуществляется в соответствии с принципами обработки, приведенными в настоящей Политике.

Если предоставление персональных данных субъектом является обязательным в целях исполнения законодательства Российской Федерации, но от субъекта получен отказ в предоставлении его персональных данных, Ассоциация разъясняет субъекту юридические последствия такого отказа и информирует о невозможности предоставления услуги, сервиса и т.д.

Ассоциация получает персональные данные из следующих источников:

- непосредственно от субъекта персональных данных;
- от третьей стороны, в целях исполнения договорных обязательств, заключения договоров или исполнения требований законодательства Российской Федерации, при условии предоставления Оператору подтверждения наличия оснований;
- от другого субъекта персональных данных, в целях реализации его законных прав;
- общедоступных источников.

При этом:

- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется на основании согласия, оформляемого отдельно от иных согласий субъекта персональных данных, в котором субъект имеет право: определить перечень персональных данных по каждой категории персональных данных, указанных в согласии на обработку персональных данных, разрешенных субъектом для распространения; установить запреты на передачу (кроме предоставления доступа) этих персональных данных неограниченному кругу лиц; установить запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц;

- обработка персональных данных субъектов, не достигших совершеннолетия, осуществляется при наличии согласия законного представителя такого субъекта;

Ассоциация вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

Поручение обработки персональных данных другому лицу возможно на основании заключаемого с этим лицом договора, обязательным условием которого являются:

- соблюдение этим лицом принципов и правил обработки персональных данных, предусмотренных действующим законодательством Российской Федерации;
- обеспечение конфиденциальности персональных данных;
- обеспечение безопасности персональных данных при их обработке в соответствии с законодательством Российской Федерации.

Лицо, осуществляющее обработку персональных данных по поручению Ассоциации, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные 152-ФЗ.

В случае, если Ассоциация поручает обработку персональных данных другому лицу, ответственность перед субъектом за действия указанного лица несет Ассоциация.

Персональные данные не раскрываются третьим лицам и не распространяются иным образом без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

Представители органов государственной власти (в том числе, контролирующих, надзорных, правоохранительных, дознания и следствия и иных уполномоченных органов по основаниям, предусмотренным действующим законодательством Российской Федерации) получают доступ к персональным данным, обрабатываемым Ассоциацией, в объеме и порядке, установленном законодательством Российской Федерации.

Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Персональные данные (материальные носители персональных данных), обработка которых осуществляется в различных целях, хранятся отдельно друг от друга.

Хранение персональных данных осуществляется на учтенных носителях, не дольше, чем этого требуют цели обработки персональных данных, хранение персональных данных на неучтенных носителях (даже в зашифрованном виде) не допускается.

Лицо, ответственное за обработку персональных данных, несет ответственность за исполнение сроков обработки, хранения и уничтожения персональных данных.

Использование веб-ресурсов:

Ассоциация обрабатывает персональные данные, получаемые при заполнении членами Ассоциации формы доступа в личный кабинет. Персональные данные, собираемые посредством заполнения формы на сайте Ассоциации, используются для осуществления доступа к личному кабинету члена Ассоциации.

VIII. Сроки обработки и хранения персональных данных, порядок их уничтожения

Хранение персональных данных осуществляется не дольше, чем того требуют цели их обработки, если срок хранения обрабатываемых данных не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Персональные данные подлежат уничтожению:

- при достижении целей обработки или утраты необходимости в их достижении;
- при получении требования от субъекта персональных данных о прекращении обработки его персональных данных или истечении срока действия его согласия на обработку персональных данных;
- при получении от субъекта персональных данных отзыва согласия на обработку своих персональных данных (если отзыв согласия влечет за собой уничтожение персональных данных);
- при получении требования от уполномоченного органа по защите прав субъектов персональных данных;
- при невозможности устранения допущенных нарушений при обработке персональных данных.

При наступлении условий, при которых обработка персональных данных должна быть прекращена, персональные данные подлежат уничтожению/обезличиванию, в установленные законодательством Российской Федерации сроки, с учетом требований Роскомнадзора в части уничтожения и обезличивания персональных данных.

При получении от субъекта персональных данных требования о прекращении обработки его персональных данных и/или отзыва согласия на обработку персональных данных, Ассоциация вправе продолжить их обработку при наличии следующих оснований:

- обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;
- обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;
- обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Уничтожение и обезличивание персональных данных осуществляются в соответствии с требованиями нормативных правовых актов Роскомнадзора.

IX. Меры обеспечения конфиденциальности и безопасности персональных данных

При обработке персональных данных Ассоциация принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении персональных данных.

Обеспечение безопасности персональных данных достигается применением необходимых и достаточных мер, в частности следующих:

- назначается ответственный за организацию обработки персональных данных;
- издаются Политика, локальные акты Ассоциации по вопросам обработки персональных данных,

- а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на Ассоциацию не предусмотренные законодательством Российской Федерации полномочия и обязанности;

- применяются правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со статьей 19 152-ФЗ, в частности: определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных; применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных; применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации; проведение оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных; учет машинных носителей персональных данных; обнаружение фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них; восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных; контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

- осуществляется внутренний контроль и (или) аудит соответствия обработки персональных данных 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, Политике, локальным актам;

- проводится оценка вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который

может быть причинен субъектам персональных данных в случае нарушения 152-ФЗ, соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ;

- осуществляется ознакомление работников Ассоциации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, Политикой, локальными актами Ассоциации по вопросам обработки персональных данных, и (или) обучение указанных работников;

Х. Права субъектов персональных данных

Субъект персональных данных имеет право:

- на получение информации, касающейся обработки его персональных данных, в том числе содержащей: подтверждение факта обработки персональных данных; правовые основания и цели обработки персональных данных; цели и применяемые способы обработки персональных данных; наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона; обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом; сроки обработки персональных данных, в том числе сроки их хранения; порядок осуществления субъектом персональных данных прав, предусмотренных 152-ФЗ; наименование или фамилию, имя, отчество (при наличии) и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу; информацию о способах исполнения Оператором обязанностей, установленных статьей 18.1 152-ФЗ; иные сведения, предусмотренные 152-ФЗ или другими федеральными законами.

Указанные выше сведения предоставляются субъекту персональных данных (или его представителю) в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе, в сроки, установленные 152-ФЗ.

Субъект персональных данных имеет право обратиться повторно или направить повторный запрос, в целях получения сведений: не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных; ранее чем через тридцать дней в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

Повторный запрос наряду со сведениями, определенными в ч.3 ст.14 152-ФЗ, должен содержать обоснование направления повторного запроса.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

- иных случаях, установленных ч.8 ст.14 152-ФЗ.

Субъект персональных данных также имеет право:

- на уточнение его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- отозвать свое согласие на обработку персональных данных и потребовать удалить свои персональные данные, если персональные данные больше не требуются для целей, в которых они были получены и/или отсутствуют законные основания для продолжения обработки его данных;
- обратиться к оператору с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения;
- на иные права, установленные законодательством Российской Федерации.

XI. Права и обязанности оператора персональных данных

Ассоциация как оператор персональных данных имеет право:

- самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательными и нормативными актами Российской Федерации;
- поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора;
- продолжить обработку персональных данных в случае отзыва субъектом персональных данных согласия на обработку персональных данных без согласия при наличии иных законных оснований.

Ассоциация как оператор персональных данных обязан:

- обеспечить при сборе персональных данных (в том числе посредством сети «Интернет») запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных 152-ФЗ;
- при получении соответствующего запроса от субъекта персональных данных (его представителя) предоставить субъекту персональных данных (или его представителю) информацию, предусмотренную главой X настоящей Политики, в доступной форме и сроки, определенные 152-ФЗ; в случае отказа в предоставлении информации дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя;
- безвозмездно предоставить субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;
- внести необходимые изменения в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными;
- уничтожить персональные данные в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем

сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

- уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

- устранить нарушения законодательства и осуществить соответствующие действия в порядке и сроки, установленные ст. 21 152-ФЗ, в случае выявления неправомерной обработки персональных данных, выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных;

- обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных, в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности: в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, с момента выявления такого инцидента Ассоциацией, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных: в течение 24 часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом; в течение 72 часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии);

- провести оценку вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных;

Права и обязанности Ассоциации также определяются действующим законодательством, договорами и внутренними документами.

XII. Ответственность

Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных Ассоциации, в пределах его полномочий. Ответственность лиц, участвующих в обработке персональных данных на основании поручений Ассоциации, за неправомерное использование персональных данных устанавливается в соответствии с условиями заключенного между Ассоциацией и контрагентом гражданско-правового договора или соглашения о конфиденциальности информации. Лица, виновные в нарушении положений, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами, локальными актами, договорами Ассоциации.

XIII. Актуализация документа

Настоящая Политика пересматривается при изменении законодательства Российской Федерации, нормативных правовых актов, регулирующих вопросы обработки персональных данных и обеспечения информационной безопасности, по результатам внутренних и внешних аудитов, а также по инициативе руководителя Ассоциации. В случае изменения законодательства Российской Федерации, внесения изменений во внутренние документы Ассоциации, Политика действует в части, не противоречащей законодательству и внутренним документам Ассоциации до приведения ее в соответствие с такими изменениями.

XIV. Список использованных источников

1. Конституция Российской Федерации;
2. Конституция Республики Марий Эл;
3. Трудовой кодекс Российской Федерации;
4. Семейный кодекс Российской Федерации;
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
6. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
7. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
8. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008 г.;
10. Методика оценки угроз безопасности информации, утвержденная ФСТЭК России 05 февраля 2021 г.

Лист внесения изменений

[illegible]

Лист ознакомления

[illegible]