ОТДЕЛ ОБРАЗОВАНИЯ
АДМИНИСТРАЦИИ ЗАВИТИНСКОГО РАЙОНА
АМУРСКОЙ ОБЛАСТИ

П Р И К А З

17.11.2020 № 222

г. Завитинск

Об утверждении Политики в отношении обработки персональных данных, обрабатываемых в информационных системах персональных данных отдела образования администрации Завитинского района Амурской области

В соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», во исполнение Постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

п р и к а з ы в а ю:

1.Утвердить «Политику в отношении обработки персональных данных, обрабатываемых в информационных системах персональных данных отдела образования администрации Завитинского района Амурской области» (Приложение).

2.Приказ довести до работников отдела образования под подпись.

3.Контроль за исполнением настоящего приказа оставляю за собой.

Начальник отдела образования Т.А.Доля

Приложение
к приказу начальника отдела
образования
от «17» 12 2020 № 227

Политика
в отношении обработки персональных данных, обрабатываемых в информационных системах персональных данных отдела образования администрации Завитинского района Амурской области

1. Введение

1.1.Политика в отношении обработки персональных данных, обрабатываемых в информационных системах персональных данных (далее – ИСПДн) отдела образования администрации Завитинского района Амурской области (далее – Политика) разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2.Политика разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки персональных данных, направленных на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, в частности, в целях защиты от несанкционированного доступа и неправомерного распространения персональных данных, обрабатываемых в информационных системах отдела образования администрации Завитинского района Амурской области (далее – Отдел).

1.3.Настоящая Политика раскрывает принципы, порядок и условия обработки персональных данных граждан Российской Федерации, иностранных граждан (далее – граждане) и лиц без гражданства Отделом.

2. Категории персональных данных

2.1. Перечень персональных данных, подлежащих защите в Отделе, формируется в соответствии с федеральным законодательством о персональных данных и утверждается приказом Отдела, устанавливающим принимаемые меры по защите персональных данных и ответственность должностных лиц. Персональные данные граждан и лиц без гражданства (любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) включены в Перечень сведений конфиденциального характера, утвержденный приказом Отдела.

2.2. Отдел обрабатывает персональные данные граждан и лиц без гражданства в связи с исполнением своих полномочий, установленных действующим законодательством.

3. Цели и задачи обеспечения безопасности персональных данных

3.1. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности персональных данных Отдела являются:

- Отдел, как собственник информационных ресурсов;
- руководство и сотрудники Отдела, в соответствии с возложенными на них функциями;
- физические лица, состоящие с Отделом в гражданско-правовых отношениях (граждане).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимым им персональным данным (их доступности);
- достоверности (полноты, точности, адекватности, целостности) персональных данных;
- конфиденциальности (сохранения в тайне) персональных данных;
- защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;
- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;
- защиты персональных данных от незаконного распространения.

3.2. Цели защиты.

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Отдела от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредствам обеспечения и постоянного поддержания следующих свойств персональных данных:

- доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем Отдела, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах Отдела и передаваемой по каналам связи;
- конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

3.3.Основные задачи системы обеспечения безопасности персональных данных.

Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности Отдела должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Отдела;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационных систем Отдела посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Отдела (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

- защиту от несанкционированной модификации используемых в информационных системах Отдела программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.4. Основные пути решения задач системы защиты.

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:
- строгим учетом всех подлежащих защите ресурсов информационных систем Отдела (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационной системы;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Отдела по вопросам обеспечения безопасности информации;
- подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;
- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Отдела;
- четким знанием и строгим соблюдением всеми пользователями информационных систем Отдела требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Отдела;
- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Отдела;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
-эффективным контролем над соблюдением пользователями информационных ресурсов Отдела требований по обеспечению безопасности информации;
- юридической защитой интересов Отдела при взаимодействии с внешними организациями (связанные с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

4. Обеспечение безопасности персональных данных

4.1. Отдел предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

4.2. В целях координации действий по обеспечению безопасности персональных данных в Отделе назначено лицо, ответственное за организацию обработки персональных данных.

5. Заключительные положения

5.1. Настоящая Политика является общедоступным документом и подлежит размещению на официальном сайте Отдела.

5.2. Настоящая Политика может быть изменена в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных или переутверждена при отсутствии изменений, но не реже одного раза в три года. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее утверждения приказом Отдела.

5.3.Контроль исполнения требований настоящей Политики осуществляется лицом, ответственным за организацию обработки персональных данных.

5.4.Ответственность должностных лиц Отдела, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Отдела.