

Правила осуществления внутреннего контроля соответствия обработки персональных данных и требования к защите персональных данных

Термины и определения :

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, блокирование, уничтожение персональных данных.

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), совершаемых с персональными данными

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

1. Общие положения :

1.1 Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных», далее – Правила) определяют процедуру, направление и предотвращение нарушения законодательства Российской Федерации в сфере персональных данных, формы, а также основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ д/с №49 (далее – Утверждение)

1.2 Настоящие правила разработаны в соответствии с постановлением Правительства Российской Федерации от 21.03.2012 года № 211 «Об утверждении перечня мер, направленных на обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 года № 52 – ФЗ «О персональных данных» и принятыми в соответствии с ними нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.3. Внутренний контроль состояния защиты информации включает в себя:
- Контроль организации защиты информации;
- Контроль эффективности защиты информации.

2. Порядок осуществления внутреннего контроля.

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организовывается проведение периодической проверки условий обработки персональных данных.

2.2. Проверки осуществляются ответственным за организацию обработки персональных данных либо комиссией, созданной на основании приказа руководителя.

2.3. В проведении проверки не может участвовать сотрудник, прямо или косвенно заинтересованный в ее результатах.

2.4. Проверка соответствия обработки персональных данных установленными

требованиям проводится не реже одного раза в год на основании утвержденного руководителем «Плана осуществления внутреннего соответствия обработки персональных данных установленным требованиям» или на основании письменного заявления о нарушении правил обработки.

2.5. Проведение внеплановой проверки организуется в течение 3 рабочих дней с момента поступления соответствующего заявления.

2.6. При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям полностью, объективной и всесторонне проводится проверка:

- соблюдение принципов обработки персональных данных;
- соответствия локальных актов в области персональных данных действующему законодательству Российской Федерации;
- выполнения сотрудниками требований и правил обработки персональных данных;
- актуальности информации о законности целей обработки персональных и оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований обработки и обеспечения безопасности персональных данных;
- правильности осуществления сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных;
- актуальности перечня лиц имеющих доступ к персональным данным;
- соблюдение прав субъектов персональных данных;
- порядка взаимодействия с субъектами персональных данных, в том числе соблюдения сроков, требований по уведомлению, порядка разъяснения субъектам необходимой информации, порядка реагирования на запросы субъектов персональных данных, порядка действий при достижении целей обработки и отзыве согласия субъекта персональных данных, наличия необходимых согласий субъектов персональных данных;
- актуальности сведений, содержащихся в уведомлении об обработке персональных данных;
- актуальности перечня информационных систем персональных данных;
- знания и соблюдения сотрудниками положений действующего законодательства Российской Федерации в области персональных данных, локальных актов Учреждения;
- соблюдения условий сотрудниками конфиденциальности персональных данных;
- соблюдения сотрудниками требований по обеспечению безопасности персональных данных.

2.7. Контроль осуществляется непосредственно на месте обработки персональных данных путем опроса сотрудников и осмотра рабочих мест, участвующих в процессе обработки персональных данных.

2.8. По результатам проведения внутреннего контроля составляется протокол проведения проверки.

2.9. При выявлении нарушений в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

2.10. О результатах проведения проверки и мерах, необходимых для устранения нарушений, руководителю Учреждения докладывает ответственный за организацию обработки персональных данных.