ОБСУЖДЕНО
на общем собрании МБДОУ
детского сада № 45 «Радуга»
протокол № 1 от «09» января 2019 г.

«УТВЕРЖДАЮ»
Заведующий МБДОУ
детским садом № 45 «Радуга»
_____ Калонова Н.Н.
приказ № 54 от «09» января 2019 г.

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ детского сада № 45 «Радуга»

г. Пятигорск

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в МБДОУ детском саду № 45 «Радуга» (далее - учреждение), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее - ПД), основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПД, необходимой для предоставления муниципальных услуг и выполнение требований к защите ПД.

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «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», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211.

1.3. Для обработки ПД, необходимых для предоставления муниципальных услуг, используется информационная система персональных данных «ИАС «Аверс: ДОО».

1.4. Обработка ПД работников, необходимых для обеспечения кадровой и бухгалтерской деятельности осуществляется без использования средств автоматизации.

1.5. Пользователем информационной системы персональных данных «ИАС «Аверс: ДОО» является работник, участвующий в процессе автоматизированной обработки ПД и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее - СЗИ) информационной системы персональных данных «ИАС «Аверс: ДОО».

1.6. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационной системе персональных данных «ИАС «Аверс: ДОО» проводятся в следующих целях:

проверка выполнения требований организационно-распорядительной документации по защите информации в информационной системе персональных данных «ИАС «Аверс: ДОО» и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

оценка уровня осведомленности и знаний работников в области обработки и защиты персональных данных;

оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля

2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

а) соответствие полномочий пользователя матрице доступа;

б) соблюдение пользователем информационных систем персональных данных правил использования паролей;

в) соблюдение пользователем информационных систем персональных данных требований федерального законодательства по использованию антивирусной защиты;

г) соблюдение пользователем информационных систем персональных данных требований федерального законодательства по работе со съемными носителями персональных данных;

д) соблюдение пользователем требований федерального законодательства за криптографические средства защиты информации и правил работы с ними;

е) соблюдение требований федерального законодательства по порядку резервирования баз данных и хранения резервных копий;

ж) знание пользователем информационных систем персональных данных порядка своих действий во внештатных ситуациях.

2.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

а) соблюдение правил хранения бумажных носителей с персональными данными;

б) соблюдение порядка доступа к бумажным носителям с персональными данными.

3. Планирование контрольных мероприятий

3.1. План проведения контрольных мероприятий включает следующие сведения по каждому из мероприятий:

цели проведения контрольных мероприятий;

задачи проведения контрольных мероприятий;

объекты контроля (процессы, подразделения, информационные системы и т.п.);

состав участников, привлекаемых для проведения контрольных мероприятий;

сроки и этапы проведения контрольных мероприятий.

3.2. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Порядок проведения плановых и внеплановых контрольных мероприятий

4.1. Плановые и внеплановые контрольные мероприятия проводятся должностным лицом, ответственным за организацию обработки персональных данных, либо комиссией, создаваемой заведующим учреждением.

4.2. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

соответствие полномочий пользователя правилам доступа;

соблюдение пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПД.

соблюдение пользователями инструкций и регламентов по обеспечению безопасности информации в информационной системе персональных данных «ИАС «Аверс: ДОО»;

знание Инструкции по обеспечению безопасности обработки ПД при возникновении внештатных ситуаций;

порядок и условия применения средств защиты информации;

состояние учета машинных носителей персональных данных;

наличие (отсутствие) фактов несанкционированного доступа к ПД и принятие необходимых мер;

проведенные мероприятия по восстановлению ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

технические мероприятия, связанные со штатным и нештатным функционированием средств защиты;

технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты информации.

4.3. Внеплановые проверки проводятся по необходимости в соответствии с поручением заведующего учреждением, но не реже одного раза в год.

4.4. Внеплановые проверки осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных.

4.5. По результатам каждой проверки составляется Протокол проведения внутренней проверки (приложение 2).

4.6. При выявлении в ходе проверки нарушений в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

4.7. Протоколы хранятся у ответственного за организацию обработки персональных данных в течение текущего года. Уничтожение протоколов проводится в первом квартале года, следующего за отчетным.