

Правила
осуществления внутреннего контроля соответствия обработки персональных данных
требованиям к защите персональных данных, установленным Федеральным законом «О
персональных данных», принятыми в соответствии с ним нормативными правовыми
актами и приказами МБДОУ «Детство» «ЦРР» г. Калуги

1. Общие положения

1.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и приказами МБДОУ «Детство» «ЦРР» г. Калуги (далее – Правила) разработаны в соответствии с Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства РФ от 01.11.2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", постановлением Правительства Российской Федерации от 21.03.2012г. № 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».

1.2. Настоящие Правила устанавливают основания, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных требованиям, установленным в муниципальном бюджетном дошкольном образовательном учреждении «Детство» «Центр развития ребенка» города Калуги.

2. Цели внутреннего контроля

2.1. Целями осуществления внутреннего контроля являются:

- оценка общего состояния выполнения в процессах МБДОУ «Детство» «ЦРР» г. Калуги требований по обработке и защите персональных данных, закрепленных законодательно, а также в локальных актах МБДОУ «Детство» «ЦРР» г. Калуги;

- выявление и предотвращение нарушений законодательства в сфере персональных данных.

2.2. Внутренний контроль осуществляется Комиссией по обеспечению безопасности персональных данных, создаваемой приказом МБДОУ «Детство» «ЦРР» г. Калуги (далее – Комиссией).

2.3. В состав Комиссии входят работники МБДОУ «Детство» «ЦРР» г. Калуги.

2.4. В составе комиссии не может участвовать работник, прямо или косвенно заинтересованный в ее результатах.

2.5. Члены комиссии, получивший доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных субъектов персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.

3. Организация внутреннего контроля

3.1. Внутренний контроль соответствия обработки персональных данных установленным

требованиям (далее – внутренний контроль) осуществляется путём проведения проверок соблюдения требований законодательства в сфере персональных данных.

3.2. Внутренний контроль делится на:

- плановый;
- внеплановый.

3.3. Плановый внутренний контроль проводят 1 раз в квартал.

3.4. Непосредственно перед началом проведения планового внутреннего контроля за 10 (десять) рабочих дней, ответственным за организацию обработки персональных данных направляется уведомление руководителю необособленного структурного подразделения, другие подразделения МБДОУ «Детство» «ЦРР» г. Калуги, в которых планируется проведение внутреннего контроля.

3.5. Внеплановые внутренние проверки могут проводиться в следующих случаях:

- по результатам расследования выявленных нарушений требования законодательства в сфере персональных данных;
- по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов персональных данных.

3.6. Внутренний контроль представляет собой комплекс мероприятий, который состоит из следующих этапов:

- подготовка к проведению проверки;
- сбор свидетельств проверки;
- анализ соответствия контрольным параметрам;
- подготовка заключения по внутреннему контролю.

3.7. В ходе подготовки к проведению проверки Комиссия определяет:

- границы и описание области, подвергающейся внутреннему контролю;
- перечень контрольных параметров;
- объекты контроля (процессы, необособленные структурные подразделения, информационные системы и т.п.);
- состав участников, привлекаемых для проведения контроля;
- сроки и этапы проведения внутреннего контроля.

Перечень контрольных параметров в МБДОУ «Детство» «ЦРР» г.Калуги приведен в приложении к настоящим Правилам (приложение 1).

3.8. Сбор свидетельств проверки включает:

- анализ организационно-распорядительных и регламентирующих документов по обработке и защите персональных данных;
- опрос персонала, участвующего в процессах обработки персональных данных, обслуживании и эксплуатации информационных систем персональных данных.

3.9. Внутренний контроль проводится Комиссией непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

3.10. Свидетельства проверки сопоставляют с контрольными параметрами для формирования заключения по внутреннему контролю.

3.11. Общий срок внутреннего контроля не может превышать 20 (двадцати) рабочих дней. При необходимости срок может быть продлен, но не более чем на 10(десять) рабочих дней.

4. Права Комиссии при проведении внутреннего контроля.

4.1. Комиссия для реализации своих полномочий имеет право:

- привлекать для проведения внутреннего контроля работников МБДОУ «Детство» «ЦРР» г. Калуги;
- запрашивать у сотрудников дошкольного образовательного учреждения необходимую информацию;
- принимать меры по устранению выявленных нарушений выполнения требований к защите персональных данных;

- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить предложение о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

5. Порядок оформления результатов внутреннего контроля

5.1. Факт проведения внутреннего контроля и результаты фиксируются в журнале проверок (приложение 2).

5.2. Журнал проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных прошивается, а листы нумеруются.

5.3. По результатам внутреннего контроля Комиссией, при необходимости, проводится заседание. Решение, принятое на заседании Комиссии, оформляется протоколом.

5.4. В целях контроля устранения выявленных нарушений Комиссия проводит повторный внутренний контроль.

К Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и приказами МБДОУ «Детство» «ЦРР» г. Калуги

ПЕРЕЧЕНЬ

Контрольных параметров проверок в области обработки и обеспечения безопасности персональных данных в МБДОУ «Детство» «ЦРР» г. Калуги

№ п/п	Контрольные параметры и объекты проверок
1	Соответствие установленных в перечне персональных данных категорий персональных данных фактически обрабатываемым в МБДОУ «Детство» «ЦРР» г. Калуги (необособленных структурных подразделениях)
2	Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников
3	Подтверждение факта ознакомления с локальными актами в области обработки и обеспечения безопасности персональных данных
4	Наличие законных целей и оснований обработки всех категорий персональных данных
5	Выборочные проверки сотрудников на предмет знания организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных
6	Соблюдение сроков хранения и порядка уничтожения персональных данных
7	Соблюдение процедур и сроков подготовки ответов на обращение субъектов персональных данных
8	Необходимость актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных

