

Администрация Петрозаводского городского округа
Муниципальное бюджетное дошкольное образовательное учреждение
Петрозаводского городского округа «Детский сад № 30 «Насто»
(МДОУ «Детский сад № 30 «Насто»)

УТВЕРЖДЕНО
приказом МДОУ
«Детский сад № 30 «Насто»
от 20.11.2025 № 159/1

ПОЛОЖЕНИЕ

о внутреннем контроле (аудите) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных МДОУ «Детский сад № 30 «Насто»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о внутреннем контроле (аудите) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных МДОУ «Детский сад № 30 «Насто» (далее — Положение) определяет процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок проведения внутреннего контроля (аудита) соответствия обработки персональных данных в МДОУ «Детский сад № 30 «Насто» (далее — МДОУ, Организация) требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных») и принятыми в соответствии с ним правовыми актами.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и принятыми в соответствии с ними нормативными правовыми актами.

1.3. В настоящем Положении используются основные понятия в значениях, определенных статьей 3 Федерального закона «О персональных данных».

II. ОБЩИЕ ТРЕБОВАНИЯ К ВНУТРЕННЕМУ АУДИТУ

2.1. Целями осуществления внутреннего аудита являются:

- оценка общего состояния выполнения в Организации требований по обработке и защите персональных данных, закрепленных законодательно, а также в локальных актах Организации;
- выявление и предотвращение нарушений законодательства в сфере персональных данных.

2.2. Внутренний аудит соответствия обработки персональных данных в Организации требованиям к защите персональных данных (далее — внутренний аудит) осуществляется путем проведения проверок лицом, ответственным за организацию обработки персональных данных в Организации (далее — ответственный за организацию обработки персональных данных), или комиссией по проведению внутреннего контроля соответствия обработки персональных данных в Организации требованиям к защите персональных данных (далее — комиссия).

2.3. Ответственный за организацию обработки персональных данных назначается приказом руководителя Организации (заведующего МДОУ).

2.4. Состав комиссии утверждается приказом руководителя Организации.

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

III. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО АУДИТА

3.1. Проверки соблюдения требований законодательства в сфере персональных данных разделяются на:

- плановые;
- внеплановые.

3.2. Плановые проверки соответствия обработки персональных данных установленным требованиям проводятся согласно Плану внутреннего контроля (аудита) (Приложение № 3).

3.3. Внеплановые внутренние проверки могут проводиться в следующих случаях:

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

3.4. Проведение внеплановой проверки организуется ответственным за организацию обработки персональных данных (председателем комиссии), а в его отсутствие — заместителем председателя комиссии в течение трех рабочих дней с даты поступления письменного заявления субъекта персональных данных о нарушении правил обработки персональных данных или с даты выявления нарушений установленных требований.

3.5. Проверка представляет собой комплекс мероприятий, который состоит из следующих этапов:

- подготовка к проведению проверки;
- сбор свидетельств проверки;
- анализ соответствия контрольным параметрам;
- подготовка акта по проверке (Приложение № 2).

3.6. В ходе подготовки к проведению проверки комиссия или ответственный за организацию обработки персональных данных определяет:

- перечень контрольных параметров;
- объекты контроля (процессы, подразделения, информационные системы персональных данных и т.п.);
- состав участников, привлекаемых для проведения проверки;
- сроки и этапы проведения проверки.

3.7. Типовой перечень контрольных параметров приведен в приложении к настоящему Положению (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. Проверки проводятся 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 сопоставляются с контрольными параметрами для формирования заключения по проверке.

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

IV. ПРАВА КОМИССИИ ПРИ ПРОВЕДЕНИИ ПРОВЕРКИ

4.1. Комиссия (ответственный за организацию обработки персональных данных) для реализации своих полномочий имеет право:

- привлекать к проведению проверок работников Организации;
- запрашивать у работников Организации информацию и (или) документы, необходимые для осуществления внутреннего аудита;
- принимать меры по устранению выявленных нарушений выполнения требований к защите персональных данных в Организации;
- требовать от сотрудников, допущенных к работе с персональными данными, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

4.2. Проверки могут проводиться с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

V. ПОРЯДОК ФИКСИРОВАНИЯ РЕЗУЛЬТАТОВ ПРОВЕРКИ

5.1. Результаты проведенных проверок оформляются в виде акта внутреннего аудита, составленного по форме согласно Приложению 2 к настоящему Положению, который подписывается ответственным за организацию обработки персональных данных или председателем комиссии, а в его отсутствие — заместителем председателя комиссии и членами комиссии в количестве не менее трех человек и утверждается руководителем Организации.

5.2. По результатам проверки, при необходимости, проводится заседание. Решения, принятые на заседаниях комиссии, оформляются протоколом.

5.3. О результатах внутреннего аудита и мерах, необходимых для устранения выявленных нарушений, по мере необходимости ответственный за организацию обработки персональных данных или председатель комиссии докладывает руководителю Организации.

5.4. В целях контроля устранения выявленных нарушений может быть проведена повторная проверка.

VI. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Настоящее Положение является локальным нормативным актом и утверждается (либо вводится в действие) приказом заведующего МДОУ.

6.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.

6.3. Настоящее Положение принимается на неопределенный срок. Изменения и дополнения к Положению принимаются в порядке, предусмотренном п.6.1. настоящего Положения.

6.4. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

Положению о внутреннем контроле (аудите) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных
МДОУ «Детский сад № 30 «Насто»

ПЕРЕЧЕНЬ

контрольных параметров проверок соответствия обработки персональных данных установленным требованиям (типовой)

№ п/п	Контрольные параметры и объекты проверок
1.	Соответствие установленных в перечне персональных данных категорий персональных данных фактически обрабатываемым в Организации
2.	Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников
3.	Подтверждение факта ознакомления с локальными актами Организации в области обработки и обеспечения безопасности персональных данных
4.	Наличие в договорах с субъектом персональных данных положений, ограничивающих права и свободы субъекта персональных данных, устанавливающих случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положений, допускающих в качестве условия заключения договора бездействие субъекта персональных данных
6.	Наличие законных целей и оснований обработки всех категорий персональных данных
7.	Выборочные проверки работников на предмет знания организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных
8.	Соблюдение сроков хранения и порядка уничтожения персональных данных
9.	Соблюдение процедур и сроков подготовки ответов на обращения субъектов персональных данных
10.	Необходимость актуализации Уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, уполномоченного органа по защите прав субъектов персональных данных

Положению о внутреннем контроле (аудите) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных
МДОУ «Детский сад № 30 «Насто»

АКТ

внутреннего контроля (аудита) соответствия обработки персональных данных требованиям к защите персональных данных в МДОУ «Детский сад № 30 «Насто»

1. Настоящий Акт составлен в том, что «__» _____ 20__ г. ответственным за организацию обработки персональных данных (комиссией в составе: председатель - _____; члены комиссии: _____)

проведена проверка (внутренний аудит) соответствия обработки персональных данных требованиям к защите персональных данных в МДОУ «Детский сад № 30 «Насто».

2. Проверка осуществлялась в соответствии с требованиями:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Политики обработки и защиты персональных данных МДОУ «Детский сад № 30 «Насто»;
- Положения об обработке и защите персональных данных работников МДОУ «Детский сад № 30 «Насто»;
- Положения об обработке и защите персональных данных воспитанников, их родителей (законных представителей) и иных третьих лиц в МДОУ «Детский сад № 30 «Насто».

3. Результаты рассмотрения вопросов по предметам аудита:

Предмет аудита	Результат рассмотрения	Примечание

Выявленные нарушения:

Меры по устранению нарушений:

Срок устранения нарушений: _____

Ответственный за организацию обработки персональных данных _____

(Комиссия в составе:

- председатель - _____;

- члены комиссии: _____)

Положению о внутреннем контроле (аудите) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных
МДОУ «Детский сад № 30 «Настоя»

ПЛАН
внутреннего контроля (аудита) соответствия обработки персональных данных
установленным требованиям законодательства в сфере обработки персональных
данных МДОУ «Детский сад № 30 «Настоя»

п/п	Мероприятие	Периодичность	Исполнитель
1	Проведение внутренних проверок на предмет соответствия обработки персональных данных требованиям к защите персональных данных	Ежегодно	Ответственный за организацию обработки персональных данных, либо комиссия
2	Поддержание в актуальном состоянии документа «Перечень работников, доступ которым к персональным данным необходим для выполнения трудовых (служебных) обязанностей»	Ежемесячно	Ответственный за организацию обработки персональных данных
3	Контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения	Ежемесячно	Заведующий хозяйством
4	Контроль за соблюдением режима безопасности помещений в которых осуществляется обработка персональных данных	Ежеквартально	Заведующий хозяйством
5	Контроль за соблюдением режима безопасности помещений, в которых размещена информационная система	Ежеквартально	Ответственный за организацию обработки персональных данных
6	Контроль за соблюдением режима безопасности помещений, в которых размещена информационная система	Ежеквартально	Ответственный за организацию обработки персональных данных
7	Контроль сохранности защищаемой информации	Ежеквартально	Заведующий хозяйством