

Приложение № 3

УТВЕРЖДЕНЫ
приказом ГБОУ школы № 15
г. Краснодара
от «01» сентября 2023 г № 357-О

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных
данных в государственном бюджетном общеобразовательном учреждении
Краснодарского края специальной (коррекционной) школе № 15
г. Краснодара

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном общеобразовательном учреждении Краснодарского края специальной (коррекционной) школе № 15 г. Краснодара (далее – Правила) устанавливают основания, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных (далее - ПД) требованиям, установленным в государственном бюджетном общеобразовательном учреждении Краснодарского края специальной (коррекционной) школе № 15 г. Краснодара (далее – ГБОУ школа № 15 г. Краснодара).

Настоящие Правила разработаны в соответствии с законодательством Российской Федерации в области обработки и защиты ПД и иными правовыми актами, принимаемыми в соответствии с данным законодательством (далее – законодательство в сфере персональных данных).

Целями осуществления внутреннего контроля являются:

- оценка общего состояния выполнения в процессах ГБОУ школы № 15 г. Краснодара требований по обработке и защите ПД, закрепленных законодательно, а также в локальных актах ГБОУ школы № 15 г. Краснодара;
выявление и предотвращение нарушений законодательства в сфере персональных данных.

Проверки проводятся Комиссией по обеспечению безопасности ПД, создаваемой приказом ГБОУ школы № 15 г. Краснодара далее – Комиссией).

Члены Комиссии, получившие доступ к ПД субъектов ПД в ходе проведения проверки, обеспечивают конфиденциальность ПД субъектов ПД, не раскрывают третьим лицам и не распространяют ПД без согласия субъекта ПД.

2. Порядок осуществления внутреннего контроля

Внутренний контроль соответствия обработки ПД установленным требованиям (далее – внутренний контроль) осуществляется ГБОУ школой № 15 г. Краснодара путем проведения проверок соблюдения требований законодательства в сфере ПД.

Проверки разделяются на:

- плановые;
- внеплановые.

Плановые проверки проводятся не реже одного раза в год.

Непосредственно перед началом проведения плановой проверки, за 10 (десять) рабочих дней, ответственным за организацию обработки ПД направляются уведомления руководителям структурных подразделений, в которых планируется проведение внутреннего контроля.

Внеплановые внутренние проверки могут проводиться в следующих случаях:

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

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

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

В ходе подготовки к проведению проверки Комиссия определяет:

- границы и описание области, подвергающейся проверке;
- перечень контрольных параметров;
- объекты контроля (процессы, подразделения, информационные системы ПД и т.п.);
- состав участников, привлекаемых для проведения проверки;
- сроки и этапы проведения проверки.

Типовой перечень контрольных параметров приведен в приложении к настоящим Правилам (Приложение 1).

Сбор свидетельств проверки включает:

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

Проверки проводятся Комиссией непосредственно на месте обработки ПД путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки ПД.

Свидетельства проверки сопоставляются с контрольными параметрами для формирования заключения по проверке.

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.

3. Права Комиссии при проведении проверки

Комиссия для реализации своих полномочий имеет право:

- привлекать к проведению проверок сотрудников ГБОУ школы № 15 г. Краснодара;
- запрашивать у сотрудников ГБОУ школы № 15 г. Краснодара; необходимую информацию;
- принимать меры по устранению выявленных нарушений выполнения требований к защите ПД в ГБОУ школе № 15 г. Краснодара;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПД при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПД.

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

4. Порядок фиксирования результатов проверки

Факт проведения проверок и результаты проверки фиксируются в Акте проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных (Приложение 2).

По результатам проверки Комиссией, при необходимости, проводится заседание. Решения, принятые на заседаниях Комиссии, оформляются протоколом.

В целях контроля устранения выявленных нарушений Комиссия проводит повторную проверку.

ПЕРЕЧЕНЬ
контрольных параметров проверок в области обработки и
обеспечения безопасности персональных данных

№ п/п	Контрольные параметры и объекты проверок
1.	Соответствие установленных в перечне персональных данных категорий персональных данных фактически обрабатываемым в ГБОУ школе № 15 г. Краснодара;
2.	Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников
3.	Подтверждение факта ознакомления с локальными актами ГБОУ школы № 15 г. Краснодара в области обработки и обеспечения безопасности персональных данных
4.	Наличие в договорах с третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных
5.	Наличие законных целей и оснований обработки всех категорий персональных данных
6.	Выборочные проверки сотрудников на предмет знания организационно- распорядительных документов в области обработки и обеспечения безопасности персональных данных
7.	Соблюдение сроков хранения и порядка уничтожения персональных данных
8.	Соблюдение процедур и сроков подготовки ответов на обращения субъектов персональных данных
9.	Необходимость актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных

АКТ
проведения внутренней проверки соответствия обработки персональных
данных требованиям к защите персональных данных

« ___ » _____ 202__ .

№ _____

Краснодар

Комиссия в составе:

Председатель:

Члены комиссии:

1. _____

2. _____

3. _____

составила настоящий акт о том, что комиссией были проведены мероприятия по контролю соответствия обработки персональных данных в ГБОУ школы № 15 г. Краснодара требованиям к защите персональных данных. Результат проведенного внутреннего контроля отражен в Таблице 1.

№ п/п	Мероприятие	Выявленные недостатки	Мероприятия по устранению недостатков	Срок проведения мероприятий	Ответственное лицо

Внутренний контроль проводился в соответствии с «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном общеобразовательном учреждении Краснодарского края специальной (коррекционной) школе № 15 г. Краснодара».

Председатель:

Члены комиссии:

**План проведения
внутреннего контроля обработки персональных данных
в государственном бюджетном общеобразовательном учреждении
Краснодарского края специальной (коррекционной) школе № 15
г. Краснодара**

№ п/п	Мероприятие	Срок проведения
1	Проверка полноты, качества и актуальности внутренних распорядительных документов, регламентирующих обработку и обеспечение безопасности персональных данных	Ежегодно
2	Контроль выполнения требований по режиму доступа в помещение, где ведется обработка персональных данных	Ежегодно
3	Проверка порядка использования технических средств защиты	Ежегодно
4	Соблюдение порядка уточнения, блокирования и уничтожения персональных данных	Ежегодно
5	Работа с обращениями субъектов персональных данных	Ежегодно
6	Проверка актуальности сведений в Реестре операторов персональных данных Роскомнадзора	Ежегодно
7	Подведение итогов	Ежегодно
8	Устранение недостатков	Ежегодно
9	Составление акта внутреннего контроля	Ежегодно
10	Доклад директору ГБОУ школы № 15 г. Краснодара	Ежегодно