



Муниципальное бюджетное общеобразовательное учреждение  
«Средняя общеобразовательная школа № 14»  
(МБОУ «СОШ № 14»)

ПРИКАЗ

28.02.2023

№ 178

г. Нефтеюганск

Об утверждении регламентов

В целях соблюдения требований безопасности при обработке персональных данных и в соответствии со ст. 22.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в соответствии с приказом Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"», приказа Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных», на основе Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказом Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных» и других нормативных правовых актов, для определения единого и обязательного порядок проведения внутреннего расследования в связи с произошедшим инцидентом в области персональных данных, связанным с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлекшей нарушение прав субъектов персональных данных, в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №14»,

ПРИКАЗЫВАЮ:

1. Утвердить регламент оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» (приложению 1);
2. Утвердить регламент проведения внутреннего расследования в связи с произошедшим инцидентом в области персональных данных (приложение 2);
3. Утвердить регламент по проведению контрольных мероприятий и реагированию на инциденты, связанные с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных (приложение 3);
4. Утвердить регламент реагирования муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №14» на запросы/обращения уполномоченного органа по защите прав субъектов персональных данных и их представителей по поводу неточности персональных данных неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к своим персональным данным (приложение 4);
5. Утвердить регламент уничтожения персональных данных (приложение 5);

6. Утвердить регламент допуска работников муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №14» к обработке персональных данных (приложение 6).

7. Настоящие регламенты вступает в силу с 1 марта 2023 г.

8. Чижовой Наиле Наилловне, секретарю руководителя ознакомить работников МБОУ «СОШ№14 »под роспись с данным приказом.

9. Контроль за исполнением приказа возложить на ответственного за организацию обработки персональных данных Хамитулину Марину Владимировну.

Директор



А.Г.Фахрутдинова

С приказом от 28.02.2023 г. № 178 «Об утверждении регламентов», ознакомлены:

№ п/п	Фамилия, инициалы работника	Должность, профессия	Подпись	Дата
1.	Абубакиров А.А.	Заместитель директора		
2.	Аистова С.А.	Уборщик служебных помещений		
3.	Алиева А.Б.	Уборщик служебных помещений		
4.	Алиева Р.С.	Уборщик служебных помещений		
5.	Алмухамедова М.Ж.	Учитель		
6.	Аминова Р.Р.	Специалист по кадрам		
7.	Арканова К.М.	Учитель		
8.	Арсланова А.М.	Учитель		
9.	Ахмедханов А.А.	Сторож		
10.	Ахмедханова М.П.	Уборщик служебных помещений		
11.	Ахмедханова Ц.А.	Уборщик служебных помещений		
12.	Ахтямова Х.М.	Заместитель директора		
13.	Ашурбеков Ш.А.	Учитель		
14.	Багатова С.З.	Учитель		
15.	Баймурадова С.В.	Уборщик служебных помещений		
16.	Бастрикова Г.Р.	Учитель		
17.	Белобороова Н.С.	Гардеробщик		
18.	Березовская Н.В.	Учитель		
19.	Булатов В.В.	Учитель		
20.	Бусыгина И.З.	Учитель		
21.	Вагапова Д.И.	Воспитатель		
22.	Варфоломеева О.А.	Учитель		
23.	Васина С.В.	Учитель		
24.	Гаджиева Ш.М.	Уборщик служебных помещений		
25.	Галимова О.М.	Учитель		
26.	Дегтярь Л.П.	Уборщик служебных помещений		
27.	Джабаева А.Д.	Учитель		

28.	Джаббарова Р.М.	Уборщик служебных помещений		
29.	Донская О.Д.	Заместитель директора		
30.	Донскова К.В.	Учитель		
31.	Захарова Т.П.	Уборщик служебных помещений		
32.	Залибекова Ф.Р.	Педагог-организатор		
33.	Игнатенко Д.А.	Рабочий по КОРЗ		
34.	Котельникова Т.М.	Учитель		
35.	Ишимова З.А.	Педагог-психолог		
36.	Казеева Е.С.	Учитель		
37.	Казимова С.Г.	Дворник		
38.	Камашова Д.Н.	Воспитатель		
39.	Катаргулова В.В.	Учитель		
40.	Концевая С.А.	Уборщик служебных помещений		
41.	Кудрявцева И.В.	Лаборант		
42.	Курносова А.В.	Учитель		
43.	Кучерова А.Ю.	Учитель		
44.	Максименко Т.А.	Заместитель директора		
45.	Мамедова А.А.	Уборщик служебных помещений		
46.	Манзырова Д.М.	Учитель		
47.	Мелекесова Н.Н.	Учитель		
48.	Мельник Л.И.	Сторож		
49.	Мустафина А.Б.	Учитель		
50.	Мухалева Е.Н.	Учитель		
51.	Надина Т.И.	Учитель		
52.	Ниязова Д.Р.	Учитель		
53.	Нуртазинова Н.А.	Педагог-библиотекарь		
54.	Пантелеев С.В.	Учитель		
55.	Попова Е.В.	Гардеробщик		
56.	Проворова И.В.	Учитель-логопед		
57.	Робак О.Ф.	Воспитатель		
58.	Рыбакова Л.И.	Учитель		
59.	Сабитова Г.Х.	Учитель		

60.	Сабитова Г.Ш.	Гардеробщик		
61.	Салахова З.А.	Лаборант		
62.	Сараев А.Р.	Учитель		
63.	Сахаутдинов В.В.	Учитель		
64.	Сахаутдинова Ф.А.	Учитель		
65.	Сергеева Н.П.	Учитель		
66.	Серёдкина Л.А.	Учитель		
67.	Смолякова Н.И.	Учитель		
68.	Соболева О.В.	Заместитель директора		
69.	Столетов В.П.	Сторож		
70.	Тахиров Т.А.	Учитель		
71.	Тахирова В.Ф.	Уборщик служебных помещений		
72.	Трескова Н.В.	Учитель		
73.	Устюгова З.Т.	Учитель		
74.	Фаттахова Р.А.	Учитель		
75.	Федотов Е.А.	Учитель		
76.	Хабибуллина А.Р.	Учитель		
77.	Хамитулина М.В.	Заместитель директора		
78.	Хамуева Д.А.	Учитель		
79.	Хасанова Л.С.	Учитель		
80.	Чижкова А.Н.	Учитель		
81.	Чижова Н.Н.	Секретарь руководителя		
82.	Шарипова И.Ф.	Социальный педагог		
83.	Щеблова Е.А.	Учитель		
84.	Щеблова С.В.	Учитель		
85.	Щербина О.В.	Учитель		
86.	Юмагулова А.А.	Учитель		
87.	Юсупова Э.Н.	Уборщик служебных помещений		
88.	Яворская Л.Н.	Специалист по охране труда		



Муниципальное бюджетное общеобразовательное учреждение  
«Средняя общеобразовательная школа № 14»  
(МБОУ «СОШ № 14»)

СОГЛАСОВАНО

Председатель первичной профсоюзной  
организации МБОУ «СОШ № 14»

\_\_\_\_\_ Д.М.Манзырова  
«\_\_» \_\_\_\_\_ 2023 г.

УТВЕРЖДАЮ

Директор МБОУ «СОШ № 14»

\_\_\_\_\_ А.Г.Фахрутдинова  
«\_\_» \_\_\_\_\_ 2023 г.

**РЕГЛАМЕНТ  
ОЦЕНКИ ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ  
ПЕРСОНАЛЬНЫХ ДАННЫХ В СЛУЧАЕ НАРУШЕНИЯ ФЕДЕРАЛЬНОГО ЗАКОНА  
«О ПЕРСОНАЛЬНЫХ ДАННЫХ»**

**1. Сокращения, термины и определения**

**Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Персональные данные, разрешенные субъектом персональных данных для распространения**, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О 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), совершаемые с персональными данными.

**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, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

## **2. Общие положения**

Регламент оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» (далее – Регламент) определяет единый и обязательный порядок и методику оценки вреда, который может быть причинён субъекту персональных в случае нарушения требований Федерального закона «О персональных данных» в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №14», (далее – Оператор, Организация).

Настоящий Регламент принят в целях обеспечения соответствия деятельности Оператора требованиям Федерального закона «О персональных данных».

Настоящий документ обязаны знать и использовать в работе члены комиссии по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

## **3. Порядок проведения оценки возможного вреда субъекту персональных данных**

Оценка возможного вреда субъекту персональных данных осуществляется комиссией по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», назначенной приказом руководителя Организации, в соответствии с методикой, описанной в разделе 4 настоящего Регламента.

По результатам оценки уровня возможного вреда субъекту персональных данных оформляется акт оценки возможного вреда субъекту персональных данных.

Допускается оформление одного акта на несколько категорий субъектов персональных данных.

## **4. Методика оценки возможного вреда субъекту персональных данных**

Субъекту персональных данных может быть причинён вред в форме:

а) убытков – расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

б) морального вреда – физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Оценка степени вреда, который может быть причинен субъекту персональных данных осуществляется в соответствии с приказом Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"».

Оператор для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Закона о персональных данных.

Высокая степень вреда устанавливается в случаях:

- обработки Оператором сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Оператором для установления личности субъекта персональных данных, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических персональных данных;

- обработки Оператором специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий персональных данных;

- обработки Оператором персональных данных несовершеннолетних для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является несовершеннолетний, а также для заключения договора по инициативе несовершеннолетнего или договора, по которому несовершеннолетний будет являться выгодоприобретателем или поручителем в случаях, не предусмотренных законодательством Российской Федерации;

- обезличивания персональных данных, в том числе с целью проведения оценочных (скоринговых) исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований, не предусмотренных пунктом 9 части 1 статьи 6 Закона о персональных данных;

Средняя степень вреда устанавливается в случаях:

- распространения персональных данных на официальном сайте Оператора в сети Интернет, а равно предоставление персональных данных неограниченному кругу лиц, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия такой обработки персональных данных;

- обработки персональных данных в дополнительных целях, отличных от первоначальной цели сбора;

- получения согласия на обработку персональных данных посредством реализации на официальном сайте в сети Интернет функционала, не предполагающего дальнейшую идентификацию и (или) аутентификацию субъекта персональных данных;



- осуществления деятельности по обработке персональных данных, предполагающей получение согласия на обработку персональных данных, содержащего положения о предоставлении права осуществлять обработку персональных данных определенному и (или) неопределенному кругу лиц в целях, несовместимых между собой.

## **5. Оформление результатов оценки вреда**

Результаты оценки вреда оформляются актом оценки вреда.

Акт оценки вреда должен содержать:

- а) наименование или фамилию, имя, отчество (при наличии) и адрес оператора;
- б) дату издания акта оценки вреда;
- в) дату проведения оценки вреда;
- г) фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии), проводивших оценку вреда, а также их (его) подпись;
- д) степень вреда, которая может быть причинена субъекту персональных данных, определенная в соответствии с методикой оценки вреда, указанной в разделе 4 настоящего Регламента.

Акт оценки вреда в электронной форме, подписанный в соответствии с федеральным законом электронной подписью, признается электронным документом, равнозначным акту оценки вреда на бумажном носителе, подписанному собственноручной подписью.

В случае если по итогам проведенной оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии с методикой оценки вреда могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

## **6. Пересмотр регламента**

Пересмотр настоящего Регламента должен осуществляться в следующих случаях, но не реже одного раза в три года:

- при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;
- при существенном изменении процессов обработки персональных данных Организации.



Муниципальное бюджетное общеобразовательное учреждение  
«Средняя общеобразовательная школа № 14»  
(МБОУ «СОШ № 14»)

СОГЛАСОВАНО

Председатель первичной профсоюзной  
организации МБОУ «СОШ № 14»

\_\_\_\_\_ Д.М.Манзырова  
«\_\_» \_\_\_\_\_ 2023 г.

УТВЕРЖДАЮ

Директор МБОУ «СОШ № 14»

\_\_\_\_\_ А.Г.Фахрутдинова  
«\_\_» \_\_\_\_\_ 2023 г.

**РЕГЛАМЕНТ  
ПРОВЕДЕНИЯ ВНУТРЕННЕГО РАССЛЕДОВАНИЯ В СВЯЗИ С ПРОИЗОШЕДШИМ  
ИНЦИДЕНТОМ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**1. Сокращения, термины и определения**

**Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Персональные данные, разрешенные субъектом персональных данных для распространения**, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О 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), совершаемые с персональными данными.

**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, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Типовая информационная система** – информационная система, в которой требуется обеспечение только конфиденциальности персональных данных.

**Специальная информационная система** – информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

## 2. Общие положения

Настоящий Регламент определяет единый и обязательный порядок проведения внутреннего расследования в связи с произошедшим инцидентом в области персональных данных, связанным с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлекшей нарушение прав субъектов персональных данных, в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №14» (далее – МБОУ «СОШ№14»).

## 3. Проведение внутреннего расследования инцидента

Проведение внутреннего расследования и составление заключений в обязательном порядке должны проводиться в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;
- выявление факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных;
- халатность и несоблюдение требований по обеспечению безопасности персональных данных;
- несоблюдение условий хранения носителей персональных данных;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

Задачами внутреннего расследования являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

Проведение внутреннего расследования возлагается приказом руководителя на комиссию в области персональных данных (далее – Комиссия). Комиссия должна приступить к работе по расследованию не позднее следующего дня после даты выявления нарушения.

Общая продолжительность внутреннего расследования не должна превышать 72 часов с момента выявления нарушения или инцидента в области персональных данных.

#### **4. Права и обязанности комиссии**

Права и обязанности Комиссии:

- опрос работников, допустивших нарушение конфиденциальности информации, а также лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента в области персональных данных;

- проведение осмотров объектов и предметов, которые могут иметь отношение к факту нарушения;

- привлечение (с разрешения соответствующего руководителя) других работников к проведению отдельных действий в рамках внутреннего расследования.

Работник, в отношении которого проводится расследование, должен быть ознакомлен с приказом руководителя о проведении расследования.

Все действия членов Комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (актами, справками и т. п.).

Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами Комиссии (не менее чем за двумя подписями).

В целях исключения возможности какого-либо воздействия на процесс расследования члены Комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения руководителя МБОУ «СОШ№14».

Для организованного и оперативного проведения внутреннего расследования Администратор безопасности разрабатывает версии причин и составляет план проведения необходимых мероприятий по каждой из этих версий. В ходе расследования могут выдвигаться и отрабатываться дополнительные версии, в этом случае план действий уточняется.

Одновременно с проведением внутреннего расследования, руководитель МБОУ «СОШ№14» может поручить Комиссии определить актуальность утраченной (разглашенной) конфиденциальной информации, оценить вред, который возможно был причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных", а также определить (подсчитать) ущерб (убытки) по расследуемому факту. В отдельных случаях такая оценка может быть осуществлена специализированной организацией.

#### **5. Оформление результатов расследования**

По окончании внутреннего расследования Комиссия представляет директору МБОУ «СОШ№14» заключение, в котором излагаются:

- основания и время проведения расследования;
- проделанная работа (кратко);
- время, место и обстоятельства факта нарушения;
- причины и условия совершения нарушения;
- виновные лица и степень их вины;
- наличие умысла в действиях виновных лиц;
- степень вреда, который был причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"
- предложения по возмещению ущерба;
- предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;

- рекомендации по исключению подобных нарушений;
- другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т.д.).

К заключению прилагаются:

- письменные объяснения лиц, которых опрашивали члены Комиссии;
- акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т.д.;
- другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба (убытков), оценке вреда.

Заключение должно быть подписано всеми членами Комиссии. При несогласии с выводами или содержанием отдельных положений член Комиссии, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде).

Заключение по результатам расследования подлежит утверждению руководителя МБОУ «СОШ№14».

Работник, в отношении которого проводится расследование, или его уполномоченный представитель, имеют право знакомиться с материалами расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов.

Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с заключением по результатам расследования.

Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом.

При наличии в действиях лица признаков административного правонарушения или уголовного преступления руководитель обязан обращаться в правоохранительные органы для привлечения виновного к ответственности в соответствии с законодательством Российской Федерации.

В соответствии с Трудовым кодексом возмещение ущерба проводится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нарушение режима конфиденциальности.

Первый экземпляр заключения с резолюцией руководителя, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дело о внутренних расследованиях вносится в номенклатуру дел МБОУ «СОШ№14».



Муниципальное бюджетное общеобразовательное учреждение  
«Средняя общеобразовательная школа № 14»  
(МБОУ «СОШ № 14»)

СОГЛАСОВАНО

Председатель первичной профсоюзной  
организации МБОУ «СОШ № 14»

\_\_\_\_\_ Д.М.Манзырова  
« \_\_\_ » \_\_\_\_\_ 2023 г.

УТВЕРЖДАЮ

Директор МБОУ «СОШ № 14»

\_\_\_\_\_ А.Г.Фахрутдинова  
« \_\_\_ » \_\_\_\_\_ 2023 г.

**РЕГЛАМЕНТ  
ПО ПРОВЕДЕНИЮ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ И РЕАГИРОВАНИЮ  
НА ИНЦИДЕНТЫ, СВЯЗАННЫЕ С НЕПРАВОМЕРНОЙ ИЛИ СЛУЧАЙНОЙ ПЕРЕДАЧЕЙ  
(ПРЕДОСТАВЛЕНИЕМ, РАСПРОСТРАНЕНИЕМ, ДОСТУПОМ)  
ПЕРСОНАЛЬНЫХ ДАННЫХ**

**1. Сокращения, термины и определения**

**Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Персональные данные, разрешенные субъектом персональных данных для распространения**, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О 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), совершаемые с персональными данными.

**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, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Типовая информационная система** – информационная система, в которой требуется обеспечение только конфиденциальности персональных данных.

**Специальная информационная система** – информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

## 2. Общие положения

Настоящий Регламент определяет единый и обязательный порядок реагированию на инциденты, связанные с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлекшей нарушение прав субъектов персональных данных, а также порядок проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №14»\_ (далее – МБОУ «СОШ№14» ).

## 3. Определение инцидента информационной безопасности в ИСПДн

К инцидентам, связанным с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных (далее – инциденты информационной безопасности, инциденты ИБ) относятся:

- нарушение конфиденциальности, целостности или доступности ПДн;
- отказ оборудования, сервисов, средств обработки и (или) защиты ПДн;
- несоблюдение требований внутренней организационно-распорядительной документации и действующего законодательства Российской Федерации в области защиты и обработки персональных данных;
- заражение вредоносными программами информационных систем персональных данных, в случае если эти события привели к неправомерной или случайной передаче (предоставлению, распространению, доступу) персональных данных, повлекшей нарушение прав субъектов персональных данных.

К инцидентам информационной безопасности в ИСПДн также относятся попытки и факты получения несанкционированного доступа к информационным системам персональных данных:

- сеансы работы в ИСПДн незарегистрированных пользователей;
- сеансы работы Пользователей ИСПДн с нарушением установленного времени доступа;

- сеансы работы Пользователей ИСПДн, срок действия полномочий которых истек либо в состав полномочий которых не входят выявленные действия с ПДн;
  - действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой личной выгоды методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи;
  - совершение попыток несанкционированного доступа к персональной рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);
  - несанкционированное внесение изменений в конфигурации программных или аппаратных средств обработки или защиты ПДн.
- Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для наступления случаев, описанных выше.

## **4. Порядок реагирования на инциденты информационной безопасности**

### **4.1 Оповещение об инциденте информационной безопасности**

Последовательность действий работника Оператора в случае выявления инцидента ИБ:

- прекратить работу с ресурсом, в котором выявлен инцидент ИБ;
- оповестить непосредственного руководителя о факте выявления инцидента ИБ;
- непосредственный руководитель работника должен оповестить ответственного по безопасности персональных данных о факте выявления инцидента;
- после извещения ответственных сотрудников по их решению представить всю необходимую информацию.

Ответственный по безопасности персональных данных проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его наступлению, и составляет краткую справку, в которой описываются произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ.

### **4.2 Мероприятия при наступлении инцидента информационной безопасности, ставшего причиной негативных последствий для субъекта ПДн**

В случае если инцидент ИБ может стать (или уже стал) причиной негативных последствий для субъектов ПДн, персональные данные этих субъектов необходимо немедленно блокировать до устранения причин, повлекших наступление инцидента ИБ и его последствий. Решение о блокировании персональных данных принимает ответственный по безопасности персональных данных. Для этой цели ответственный по безопасности персональных данных блокирует персональные данные.

Должностные лица по обработке ПДн уведомляет субъекта о блокировании его персональных данных.

Персональные данные остаются заблокированными до устранения причин, повлекших наступление инцидента ИБ.

Если причины возникновения инцидента ИБ невозможно устранить, то персональные данные должны быть уничтожены. Должностное лицо обработки ПДн и ответственный по безопасности персональных данных обеспечивают немедленное уничтожение персональных данных.

Должностное лицо по обработке ПДн оповещает субъекта ПДн о прекращении и уничтожении его персональных данных.

### **4.3 Устранение последствий и причин инцидента информационной безопасности**

Обязанности по устранению последствий и причин инцидента информационной безопасности возлагаются на ответственного по безопасности персональных данных. Не позднее 24



часов с момента наступления инцидента Администратор безопасности составляет План устранения последствий и причин наступления инцидента информационной безопасности. В данный план целесообразно включить:

- общую информацию о произошедшем инциденте;
- анализ ситуации, оперативные контрмеры, которые можно применить для локализации инцидента;
- определение лиц, ответственных за расследование и установление причин, по которым стало возможным наступление инцидента;
- определение лиц, ответственных за проведение профилактических мероприятий, разработку и внедрение мер по недопущению повторного наступления инцидента.

#### **4.4 Проведение расследования инцидента информационной безопасности**

Разбирательство и составление заключений в обязательном порядке должны проводиться в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;
- выявление факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных;
- халатность и несоблюдение требований по обеспечению безопасности персональных данных;
- несоблюдение условий хранения носителей персональных данных;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

Внутреннее расследование проводится в соответствии с Регламентом проведения внутреннего расследования в связи с произошедшим инцидентом в области персональных данных.

Результаты внутреннего расследования оформляются в виде заключения.

Заключение с резолюцией руководителя, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле.

Дело о внутренних расследованиях вносится в номенклатуру дел МБОУ «СОШ№14».

#### **4.5 Превентивные меры по недопущению повторного возникновения инцидентов информационной безопасности**

Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение в зависимости от произошедшего инцидента ИБ включают в себя:

- мониторинг событий в информационной системе персональных данных;
- восстановление операционной системы рабочей станции, на которой произошел инцидент ИБ, на заводские настройки;
- своевременное удаление неиспользуемых учетных записей;
- контроль и мониторинг действий пользователей в информационной системе персональных данных;
- контроль над действиями системных администраторов;
- проведение обучения (повторного обучения) пользователей правилам обработки и защиты персональных данных;
- ознакомление пользователей с мерами ответственности, установленными законодательством Российской Федерации за нарушение норм и правил обработки персональных данных, а также за разглашение полученных данных;

– пересмотр организационно-распорядительной документации, устанавливающей правила обработки и обеспечения безопасности при работе с персональными данными.

## **5. Оценка эффективности реализованных мер в рамках системы защиты персональных данных**

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится комиссией по проведению в соответствии с требованиями законодательства Российской Федерации в области персональных данных.

Контроль за выполнением требований защиты персональных данных в информационных системах персональных данных МБОУ «СОШ№14» организуется и проводится администратором безопасности информационных систем персональных данных.

Оценка эффективности реализованных в рамках системы защиты персональных данных мер и контроль за выполнением требований защиты персональных данных в информационных системах персональных данных проводится администратором безопасности информационных систем персональных и менеджером обработки персональных данных не реже 1 раза в 12 месяцев. Итоги проведенных мероприятий по проверке состояния защиты персональных данных вносятся в План внутренних проверок состояния защиты персональных данных (Приложение 1).

## **6. Уведомление уполномоченного органа по защите прав субъектов персональных данных об инциденте**

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор обязан с момента выявления такого инцидента Оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение 24 часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом (первичное уведомление);

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии) (дополнительное уведомление).

Взаимодействие МБОУ «СОШ№14» с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций в рамках ведения реестра учета инцидентов в области персональных данных осуществляется в рамках приказа Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».

Первичное уведомление должно содержать:

1) Сведения:

- о произошедшем инциденте (дату и время выявления инцидента, характеристику (характеристики) персональных данных (содержание базы данных, ставшей доступной неограниченному кругу лиц в результате неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных (далее – скомпрометированная база данных), количество содержащихся в ней записей. Дополнительно оператор может представить информацию об актуальности скомпрометированной базы данных, а также о периоде, в течение которого собраны персональные данные);

- о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных (предварительные причины неправомерного распространения персональных данных, повлекшего нарушение прав субъектов персональных данных);

- о предполагаемом вреде, нанесенном правам субъектов персональных данных (результаты предварительной оценки вреда, который может быть нанесен субъектам персональных данных, в связи с неправомерным распространением персональных данных, а также последствия такого вреда, проведенной в соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона «О персональных данных»);

- о принятых мерах по устранению последствий соответствующего инцидента (перечень принятых оператором организационных и технических мер по устранению последствий инцидента в соответствии со статьями 18.1, 19 Федерального закона «О персональных данных»);

- о лице, уполномоченном оператором на взаимодействие с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, по вопросам, связанным с выявленным инцидентом.

2) Данные оператора, направившего уведомление:

- фамилию, имя и отчество (при наличии) гражданина, индивидуального предпринимателя;

- полное и сокращенное (при наличии) наименование юридического лица;

- идентификационный номер налогоплательщика юридического лица, индивидуального предпринимателя, физического лица;

- адрес регистрации по месту жительства (пребывания) физического лица, индивидуального предпринимателя;

- адрес юридического лица в пределах места нахождения юридического лица;

- адрес электронной почты (при наличии).

3) Иные сведения и материалы, находящиеся в распоряжении оператора, в том числе об источнике получения информации об инциденте, а также подтверждающие принятие мер по устранению последствий инцидента (при наличии).

Дополнительное уведомление должно содержать сведения:

- о результатах внутреннего расследования выявленного инцидента (информация о причинах, повлекших нарушение прав субъектов персональных данных, и вреде, нанесенном правам субъектов персональных данных, о дополнительно принятых мерах по устранению последствий соответствующего инцидента (при наличии), а также о решении оператора о проведении внутреннего расследования с указанием его реквизитов);

- о лицах, действия которых стали причиной выявленного инцидента (при наличии) (фамилия, имя, отчество (при наличии) должностного лица оператора с указанием должности (если причиной инцидента стали действия сотрудника оператора), фамилия, имя, отчество (при наличии) физического лица, индивидуального предпринимателя или полное наименование юридического лица, действия которых стали причиной выявленного инцидента, IP-адрес компьютера или устройства, предполагаемое местонахождение таких лиц и (или) устройств (если причиной инцидента стали действия сторонних лиц) и иные сведения о выявленном инциденте, имеющиеся в распоряжении оператора).

В случае если оператор на момент направления первичного уведомления располагает сведениями о результатах внутреннего расследования выявленного инцидента, то он вправе указать такие сведения в первичном уведомлении.

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа.

Уведомление в виде документа на бумажном носителе направляется по адресу Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Уведомление в форме электронного документа направляется оператором посредством заполнения специализированной формы, размещенной на Портале персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в информационно-телекоммуникационной сети "Интернет" (далее – Портал персональных данных), после прохождения процедуры идентификации и аутентификации

посредством федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (далее – ЕСИА) и подписывается электронной подписью.

МБОУ «СОШ№14» с момента поступления уведомления в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу электронной почты, указанному в первичном уведомлении, направляется информационное письмо, содержащее сведения о дате и времени передачи уведомления в информационную систему Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также номер и ключ уведомления.

При направлении дополнительного уведомления посредством Портала персональных данных оператор должен указать номер и ключ уведомления.

В случае направления неполных или некорректных сведений Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу электронной почты, указанному в первичном уведомлении, не позднее трех рабочих дней со дня получения первичного или дополнительного уведомления направляет запрос оператору о предоставлении недостающих сведений и (или) пояснений относительно некорректности представленных в уведомлении сведений.

Недостающие сведения и (или) пояснения относительно некорректности представленных в уведомлении сведений предоставляются в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение трех рабочих дней со дня получения запроса.

#### **6. Пересмотр и внесение изменений в документы оператора**

Пересмотр положений настоящего и иных локальных документов МБОУ «СОШ№14», касающихся вопросов обработки и обеспечения безопасности персональных данных, проводится в следующих случаях, если иное не установлено в пересматриваемых документах:

- на регулярной основе, но не реже одного раза в полгода;
- при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти РФ;
- по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности персональных данных;
- по результатам внутреннего контроля (аудита) системы защиты персональных данных в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности персональных данных и выявивших недостатки в правилах предоставления доступа к персональным данным.

Ответственным за пересмотр настоящего Регламента является ответственный по безопасности персональных данных.

Внесение изменений производится на основании соответствующего приказа руководителя МБОУ «СОШ№14».

**План внутренних проверок  
состояния защиты персональных данных**

<b>Наименование мероприятий</b>	<b>Срок/периодичность</b>	<b>Ответственный/исполнитель</b>
Контроль за выполнением требований защиты персональных данных в информационных системах персональных данных	1 раз в 12 месяцев	Ответственный по организации обработки ПДн
Оценка эффективности реализованных в рамках системы защиты персональных данных мер	1 раз в 12 месяцев	Ответственный по организации обработки ПДн



Муниципальное бюджетное общеобразовательное учреждение  
«Средняя общеобразовательная школа № 14»  
(МБОУ «СОШ № 14»)

СОГЛАСОВАНО

Председатель первичной профсоюзной  
организации МБОУ «СОШ № 14»

\_\_\_\_\_ Д.М.Манзырова  
« \_\_\_\_ » \_\_\_\_\_ 2023 г.

УТВЕРЖДАЮ

Директор МБОУ «СОШ № 14»

\_\_\_\_\_ А.Г.Фахрутдинова  
« \_\_\_\_ » \_\_\_\_\_ 2023 г.

**РЕГЛАМЕНТ  
РЕАГИРОВАНИЯ ОПЕРАТОРА НА ЗАПРОСЫ/ОБРАЩЕНИЯ  
УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ  
ПЕРСОНАЛЬНЫХ ДАННЫХ, СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ  
ПРЕДСТАВИТЕЛЕЙ ПО ПОВОДУ НЕТОЧНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ,  
НЕПРАВОМЕРНОСТИ ИХ ОБРАБОТКИ, ОТЗЫВА СОГЛАСИЯ И ДОСТУПА  
СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ К СВОИМ ПЕРСОНАЛЬНЫМ  
ДАНЫМ**

**1. Общие положения**

1.1. Регламент реагирования муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №14» на запросы/обращения уполномоченного органа по защите прав субъектов персональных данных, субъектов персональных данных и их представителей по поводу неточности персональных данных, неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к своим данным (далее – Регламент) определяет последовательность действий при рассмотрении запросов/обращений уполномоченного органа по защите прав субъектов персональных данных, субъектов персональных данных или их представителей, поданных в соответствии с частью 1 статьи 14 Федерального закона «О персональных данных», правила ведения делопроизводства по Запросам, поступающим в адрес муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №14» (далее – МБОУ «СОШ №14»), а также осуществление контроля за соблюдением Регламента.

1.2. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных

мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

1.3. Запрос субъекта персональных данных (далее – Запрос) – требование субъекта персональных данных и/или их представителей от МБОУ «СОШ№14» уточнения персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

1.4. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

1.5. Рассмотрение Запросов в МБОУ «СОШ№14», являющейся в соответствии со статьей 3 Федерального закона «О персональных данных» Оператором, осуществляющим обработку персональных данных, выполняется с соблюдением прав субъектов персональных данных или их представителей и в соответствии с обязанностями оператора, определенными Федеральным законом «О персональных данных».

## **2. Прием и регистрация Запросов**

2.1. Запросы могут быть доставлены лично, через представителей, почтовым отправлением, по электронным каналам связи в форме электронного документа, подписанного электронной подписью, в соответствии с законодательством Российской Федерации.

2.2. Запросы в МБОУ «СОШ№14», поступающие непосредственно от субъектов персональных данных (далее – субъект), принимаются и регистрируются в приемной руководителя МБОУ «СОШ№14».

2.3. Если к Запросу прилагаются подлинные документы, удостоверяющие личность (паспорт, свидетельство, удостоверение и другие документы), с них снимаются копии, оригиналы возвращаются непосредственно субъекту или отправляются заказным письмом по указанному в Запросе адресу.

2.4. Работник МБОУ «СОШ№14», при прочтении Запроса проверяет правильность адресования Запроса, проверяет историю Запросов субъекта на повторность.

2.5. В Запросах, поступивших повторно и удовлетворяющих требованиям частей 4 и 5 статьи 14 Федерального закона «О персональных данных», делается отметка о повторном поступлении Запроса, и к нему приобщаются копии материалов предыдущих Запросов. МБОУ «СОШ№14» вправе отказать субъекту персональных данных или его представителю в рассмотрении повторного Запроса, не соответствующего требованиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона «О персональных данных». Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного Запроса лежит на МБОУ «СОШ№14».

2.6. Работник МБОУ «СОШ№14», заносит необходимую информацию о Запросе в журнал учета обращений субъектов персональных данных.

2.7. Регистрация Запросов производится путем присвоения порядкового номера каждому поступившему Запросу в течение трех календарных дней с даты их поступления,

информация о запросе вносится в журнал (типовая форма журнала приведена в Приложении 1 к настоящему Регламенту). На лицевой стороне первого листа в правом нижнем углу письменного Запроса проставляется регистрационный штамп. В случае если место, предназначенное для регистрационного штампа, занято текстом, штамп может быть проставлен в ином месте, обеспечивающем его прочтение.

2.8. Запрос, ошибочно поступивший в адрес МБОУ «СОШ№14», направляется исполнителем по указанному в Запросе адресу с сопроводительным письмом с уведомлением субъекта персональных данных или его представителя, направившего Запрос, о переадресации Запроса.

### **3. Направление Запроса на рассмотрение**

3.1. После регистрации, в тот же день, Запрос, поступивший в адрес МБОУ «СОШ№14», вместе с карточкой передается руководителю Организации, для рассмотрения, определения исполнителя (ответственное лицо) и формирования поручения по Запросу.

3.2. Срок для определения исполнителей и дачи поручений по Запросу не может превышать пять календарных дней, которые входят в основной (десять рабочих дней) срок рассмотрения Запроса со дня его регистрации.

3.3. В случае если Запрос, поступивший в адрес МБОУ «СОШ№14», содержит требование уточнить персональные данные, заблокировать их или уничтожить в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, руководитель в тот же день определяет исполнителей и дает поручение осуществить блокирование неправомерно обрабатываемых либо неточных персональных данных, относящихся к этому субъекту персональных данных с даты получения указанного Запроса на период проверки.

3.4. В поручении указываются фамилии, инициалы исполнителей, содержание поручения (при необходимости), срок исполнения, дата и подпись.

### **4. Порядок рассмотрения Запросов**

4.1. Ответственное лицо при рассмотрении Запроса обеспечивает объективное, всестороннее и своевременное рассмотрение Запроса, запрашивает необходимые для рассмотрения Запроса документы и материалы у работников МБОУ «СОШ№14», по компетенции.

4.2. Запрос рассматривается не более десяти рабочих дней со дня его получения, если статьями 20, 21 Федерального закона «О персональных данных» не установлен более короткий срок рассмотрения Запроса.

4.3. В установленный срок (десять рабочих дней) входит время на визирование (определение исполнителей и нанесение поручений), рассмотрение Запроса по существу, подготовку текста ответа, его возможное согласование, подписание и направление ответа субъекту персональных данных.

4.4. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления МБОУ «СОШ№14» в адрес субъекта мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.5. В случае обращения субъекта персональных данных к МБОУ «СОШ№14» с требованием о прекращении обработки персональных данных МБОУ «СОШ№14» обязан в срок, не превышающий десяти рабочих дней с даты получения соответствующего



требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона «О персональных данных».

4.6. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.7. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных МБОУ «СОШ№14» обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.

4.8. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

## **5. Оформление ответов на Запросы**

5.1. Ответы на Запросы, поступившие в адрес МБОУ «СОШ№14», подписываются руководителем.

5.2. Подготовку ответа обеспечивает руководитель структурного подразделения Организации, в соответствии с поручением по Запросу. В случае если в поручении указано несколько исполнителей, ответственным исполнителем считается лицо, указанное первым в поручении по Запросу. Ответ на Запрос готовит основной исполнитель, указанный в поручении первым, при этом другие исполнители визируют данный ответ.

5.3. Ответ на Запрос, поступивший по информационным системам общего пользования, направляется по почтовому адресу, указанному в Запросе.

5.4. Текст ответа должен излагаться четко, последовательно, кратко, исчерпывающе давать пояснения на все поставленные вопросы.

5.5. Запрос считается исполненным, если по существу поставленных вопросов субъекту персональных данных или его представителю в представлении сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», или приняты меры, предусмотренные частью 3 статьи 20 и частями 1-3 статьи 21 Федерального закона «О персональных данных».

5.6. МБОУ «СОШ№14» предоставляет сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

5.7. Ответы на письменные Запросы оформляются в соответствии с порядком, установленным Инструкцией по делопроизводству в Организации, и должны содержать дату и регистрационный номер документа, фамилию и инициалы гражданина, его почтовый адрес, текст документа (ответ на Запрос), наименование должности лица, подписавшего документ, его инициалы, фамилию, подпись, а также инициалы, фамилию и номер телефона исполнителя.

## **6. Контроль соблюдения регламента**

6.1. Контроль соблюдения Регламента возлагается на заместителя руководителя Организации ответственного за организацию обработки персональных данных в МБОУ «СОШ№14».

6.2. Организация делопроизводства по Запросам и контролю за своевременным, объективным и полным рассмотрением Запросов, поступивших в адрес МБОУ «СОШ№14», осуществляется работником ответственным за прием и регистрацию входящих документов в МБОУ «СОШ№14».



Муниципальное бюджетное общеобразовательное учреждение  
«Средняя общеобразовательная школа № 14»  
(МБОУ «СОШ № 14»)

СОГЛАСОВАНО

Председатель первичной профсоюзной  
организации МБОУ «СОШ № 14»

\_\_\_\_\_ Д.М.Манзырова  
«\_\_» \_\_\_\_\_ 2023 г.

УТВЕРЖДАЮ

Директор МБОУ «СОШ № 14»

\_\_\_\_\_ А.Г.Фахрутдинова  
«\_\_» \_\_\_\_\_ 2023 г.

**РЕГЛАМЕНТ  
УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**1. Сокращения, термины и определения**

**Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Персональные данные, разрешенные субъектом персональных данных для распространения**, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О 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), совершаемые с персональными данными.

**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, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

## **2. Общие положения**

2.1. Регламент уничтожения персональных данных (далее – Регламент) определяет единый и обязательный порядок, условия и способы уничтожения персональных данных субъектов персональных данных, которые обрабатываются в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №14» (далее – МБОУ «СОШ№14», Организация), а также устанавливает формы подтверждения уничтожения персональных данных.

2.2. Настоящий Регламент принят в целях обеспечения защиты прав и свобод обучающихся и работников при обработке их персональных данных и обеспечения соответствия деятельности МБОУ «СОШ№14» требованиям Федерального закона «О персональных данных».

2.3. Настоящий Регламент разработан на основе Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказа Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных» и других нормативных правовых актов.

2.4. Настоящий Регламент обязаны знать и использовать в работе члены комиссии по уничтожению персональных данных.

## **3. Порядок уничтожения носителей, содержащих персональные данные**

3.1. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, должно соответствовать следующим правилам:

- быть конфиденциальным, исключая возможность последующего восстановления;
- подтверждаться юридически, в частности, оформлением соответствующих документов, установленных законодательством;
- должно проводиться комиссией по уничтожению персональных данных, утвержденной приказом директора МБОУ «СОШ№14» (далее – Комиссия);
- уничтожение должно касаться только тех носителей, содержащих персональные данные субъектов персональных данных, которые подлежат уничтожению в связи с истечением срока хранения, достижением цели обработки указанных персональных

данных либо утратой необходимости в их достижении, не допуская случайного или преднамеренного уничтожения актуальных носителей.

3.2. Персональные данные субъектов персональных данных хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении.

3.3. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются в специально отведенном для этих целей помещении Комиссией.

3.4. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются Комиссией в срок, не превышающий 30 дней с даты достижения целей обработки персональных данных либо утраты необходимости в их достижении, а также в случае, если истек срок их хранения.

3.5. Комиссия производит отбор бумажных носителей персональных данных, подлежащих уничтожению, с указанием оснований для уничтожения.

3.6. На все отобранные к уничтожению документы составляется акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению.

3.7. В актах о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению и актах об уничтожении персональных данных субъектов персональных данных, исправления не допускаются.

3.8. Комиссия проверяет наличие всех документов, включенных в акт о выделении носителей, содержащих персональные данные субъектов персональных данных, к уничтожению.

3.9. По окончании сверки акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению подписывается всеми членами Комиссии и утверждается руководителем МБОУ «СОШ№14».

3.10. Носители, содержащие персональные данные субъектов персональных данных, отобранные для уничтожения и включенные в акт, после проверки их Комиссией передаются ответственному за уничтожение документов в помещение отдела кадров.

3.11. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, производится после утверждения акта в присутствии всех членов Комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте носителей.

3.12. Уничтожение персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.13. Уничтожение персональных данных, осуществляется в следующем порядке:

- уничтожение персональных данных, содержащихся на бумажных носителях, осуществляется путем измельчения на мелкие части, исключающие возможность последующего восстановления информации. Измельчение осуществляется с использованием shreddera (уничтожителя документов), установленного в помещении отдела кадров, либо документы передаются на переработку (утилизацию) организациям, собирающим вторсырье (пункты приема макулатуры);

- уничтожение персональных данных, содержащихся на машиночитаемых носителях, осуществляется путем нанесения им неустраняемого физического повреждения, исключающего возможность их использования, а также восстановления данных.

Вышеуказанное достигается путем деформирования, нарушения единой целостности носителя;

- подлежащие уничтожению файлы с персональными данными субъектов персональных данных, расположенные на жестком диске средств автоматизации или в базах данных ИСПДн, удаляются средствами операционной системы компьютера и/или с использованием специального программного обеспечения;

- в случае допустимости повторного использования носителя флэш, CD-RW, DVD-RW применяется программное удаление («затирание») содержимого диска путем его форматирования с последующей записью новой информации на данный носитель.

#### **4. порядок подтверждения уничтожения персональных данных**

4.1. В случае если обработка персональных данных осуществляется МБОУ «СОШ№14» без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

4.2. В случае если обработка персональных данных осуществляется МБОУ «СОШ№14» с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в ИСПДн (далее – выгрузка из журнала).

4.3. Акт об уничтожении персональных данных составляется и подписывается всеми членами Комиссии и утверждается руководителем МБОУ «СОШ№14».

4.4. Акт об уничтожении персональных данных должен содержать:

а) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица) и адрес Оператора;

б) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица), адрес лица (лиц), осуществляющего (осуществляющих) обработку персональных данных субъекта (субъектов) персональных данных по поручению МБОУ «СОШ№14» (если обработка была поручена такому (таким) лицу (лицам));

в) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

г) фамилию, имя, отчество (при наличии), должность лиц (лица), уничтоживших персональные данные субъекта персональных данных, а также их (его) подпись;

д) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

е) наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

ж) наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

з) способ уничтожения персональных данных;

и) причину уничтожения персональных данных;

к) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

4.5. Акт об уничтожении персональных данных в электронной форме, подписанный в соответствии с законодательством Российской Федерации, признается электронным документом, равнозначным акту об уничтожении персональных данных на бумажном носителе, подписанному собственноручной подписью лиц, указанных в подпункте "г" пункта 4.4 настоящего Регламента.

4.6. Выгрузка из журнала должна содержать:

а) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

б) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

в) наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;

г) причину уничтожения персональных данных;

д) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

4.7. В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные пунктом 5 настоящих Требований, недостающие сведения вносятся в акт об уничтожении персональных данных.

4.8. В случае если обработка персональных данных осуществляется оператором одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала.

4.9. Факт уничтожения персональных данных субъектов персональных данных, фиксируется в журнале регистрации уничтожения ПДн субъектов ПДн. Данный документ является документом конфиденциального характера и вместе с актами о выделении документов, содержащих персональные данные субъектов персональных данных, актами об уничтожении персональных данных и выгрузками из журнала регистрации событий хранится в помещении отдела кадров в течение 3 лет с момента уничтожения персональных данных. По истечении срока указанные документы передаются в архив Организации на хранение.

## **6. Пересмотр регламента**

Пересмотр настоящего Регламента должен осуществляться в следующих случаях, но не реже одного раза в три года:

– при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;

– при существенном изменении процессов обработки персональных данных МБОУ «СОШ№14».



Муниципальное бюджетное общеобразовательное учреждение  
«Средняя общеобразовательная школа № 14»  
(МБОУ «СОШ № 14»)

СОГЛАСОВАНО

Председатель первичной профсоюзной  
организации МБОУ «СОШ № 14»

\_\_\_\_\_ Д.М.Манзырова  
« \_\_\_\_ » \_\_\_\_\_ 2023 г.

УТВЕРЖДАЮ

Директор МБОУ «СОШ № 14»

\_\_\_\_\_ А.Г.Фахрутдинова  
« \_\_\_\_ » \_\_\_\_\_ 2023 г.

**РЕГЛАМЕНТ  
ДОПУСКА РАБОТНИКОВ МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО  
ОБЩЕОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ «СРЕДНЯЯ  
ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №14»  
К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**1. Общие положения**

1.1. Регламент допуска работников муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №14» (далее – Организация, Оператор) к обработке персональных данных (далее – Регламент) разработан в соответствии с Трудовым кодексом РФ, Законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами в области обработки и защиты персональных данных, действующими на территории РФ.

1.2. Настоящий Регламент определяет порядок допуска работников Организации к обработке персональных данных других работников Организации и гарантии конфиденциальности сведений о работнике, предоставленных работником работодателю.

**2. Виды допуска к обработке персональных данных работников**

2.1. Допуск работников Организации к обработке персональных данных других работников Организации подразделяется на полный и частичный согласно приказу директора.

**3. Порядок допуска работников к обработке персональных данных**

3.1. Лица, указанные в п. 2.2, 2.3 настоящего Регламента, допускаются к обработке персональных данных других работников Организации с соблюдением общей процедуры оформления работы с персональными данными, предусмотренной действующим законодательством и локальными актами Организации, без дополнительного оформления.



3.2. Лица, указанные в п. 2.4 настоящего Регламента, заинтересованные в частичном допуске к обработке персональных данных других работников, направляют директору Организации мотивированное ходатайство, в котором излагают:

- цель допуска к обработке персональных данных других работников Организации;
- перечень персональных данных, допуск к обработке которых необходим;
- обоснование необходимости и целесообразности допуска к обработке персональных данных других работников Организации.

3.3. Ходатайство подлежит рассмотрению в течение трех рабочих дней. По результатам рассмотрения ходатайства директор Организации издает приказ о допуске работника к обработке персональных данных других работников либо принимает решение об отказе в допуске с указанием причин отказа.

#### **4. Порядок прекращения допуска работников Организации к обработке персональных данных**

4.1. Допуск к обработке персональных данных работников Организации прекращается:

- при увольнении работника, имеющего допуск;
- при переводе работника, имеющего допуск, на должность, выполнение работ по которой уже не требует допуска к обработке персональных данных.

4.2. Допуск к обработке персональных данных у лиц, указанных в п. 2.4 настоящего Регламента, может быть дополнительно прекращен по письменному решению директора Организации или его заместителей.