

Принято
на заседании педагогического совета
Протокол №1 от 30 августа 2022 года

«УТВЕРЖДАЮ»
Директор школы
Ильинская И.В.Балукина
Приказ № 500-ПД от 31 августа 2022
года



ПОРЯДОК
уничтожения, блокировании персональных данных
муниципального бюджетного
общеобразовательного учреждения –
Хотынецкой средней общеобразовательной
школы имени Сергея Геннадьевича Поматилова
Хотынецкого района Орловской области

1. Общие положения

Настоящий Порядок определяет условия и способы:

- уничтожения бумажных носителей (документов), содержащих персональные данные по достижению цели обработки этих персональных данных;
- персональных данных в машинных носителях информации, в том числе персональных данных, и при необходимости самих машинных носителей информации,

2. Блокирование и уничтожение персональных данных, содержащих на машинных носителях информации

2.1. Блокирование информации, содержащей персональные данные субъекта персональных данных, производится в случаях:

- если персональные данные являются неполными, устаревшими, недостоверными;
- если сведения являются незаконно полученными или не являются необходимыми для заявленной оператором персональных данных цели обработки,

2.2. В случае подтверждения факта недостоверности персональных данных уполномоченное Оператором лицо на основании документов, представленных субъектом персональных данных, уполномоченным органом по защите прав субъектов персональных данных или полученных в ходе самостоятельной проверки, обязано уточнить персональные данные и снять их блокирование,

2.3. В случае выявления неправомерных действий с персональными данными уполномоченное Оператором лицо обязало устранить (организовать устранение) допущенные нарушения. В случае невозможности устранения допущенных нарушений необходимо в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожить персональные данные.

2.4. Об устраниении допущенных нарушений или об уничтожении персональных данных, уполномоченное Оператором лицо обязано уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган,

2.5. Уполномоченное Оператором лицо обязано уничтожить персональные данные субъекта персональных данных в случаях:

- достижения цели обработки персональных данных оператор;
- отзыва субъектом согласия на обработку своих персональных данных,

2.6. Уничтожение персональных данных должно быть осуществлено в течение трех дней с указанных моментов, в согласии субъекта персональных данных на обработку его персональных данных могут быть установлены иные сроки уничтожения персональных

данных при достижении цели обработки персональных данных, Уполномоченное Оператором лицо должно направить уведомление о факте уничтожения персональных данных субъекту персональных данных,

3. Работа с бумажными носителями (Документами)

3.1. Виды и периоды уничтожения бумажных носителей, содержащих персональные данные, представлены в таблице :

Таблица

№/пп	Документ	Срок хранения	действия по окончании срока хранения	Виды и периоды уничтожения бумажных носителей, содержащих персональные данные
1.	Документы (сведения, содержащие персональные данные о работниках Оператора), переданные и Сформированные при трудоустройстве работника,	75 лет		Уничтожение
2	Документы об обучающихся (сведения, содержащие персональные данные обучающихся)	установленные для данных документов сроки хранения		Уничтожение
3	Другие документы с грифом «Конфиденциально» и «Для служебного пользования» (Журналы учета, списки доступа, эксплуатационная документация ит.п.)	хранятся до замены на новые, если не указан конкретный срок		Уничтожение

3.2 Документы, указанные в 3.1. должны находиться в сейфах, опечатываемых печатями сотрудника отдела кадров или учебной части. Исключение составляют документы, обрабатываемые на настоящий момент на рабочем месте.

3.3. По окончании срока хранения документы, указанные в 3.1 уничтожаются путём измельчения на мелкие части (или иным способом), исключающие возможность последующего восстановления информации или сжигаются.

4. Работа с машинными носителями информации

4.1. Виды и периоды уничтожения персональных данных, хранимых в электронном виде («файлах») на жестком диске компьютера (далее — НЖМД) и машинных носителях: компакт дисках (далее — DVD,R,'RW в зависимости от формата), дискетах 3,5"1,4 МБ(далее — FDD),FLASH-накопителях

Пример видов и периодов уничтожения персональных данных, хранимых в электронном виде на НЖМД, представлен в таблице 2,

Таблица 2

Виды и периоды уничтожения персональных данных, хранимых в электронном виде на жестком диске компьютера

	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
	база данных автоматизированной информационной системы Оператора. Носитель; файлы на НЖМД сервера	До создания 60леे актуальной копки	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности уничтожение носителя; удаление архивных файлов НЖМД
2	База данных автоматизированной информационной системы «1С Предприятие-Кадры», Носитель: файлы на НЖМД се са	До создания 60лее актуальной копии	Повторное использование носителя для записи очередной резервной ко пий БД, в случае невозможности уничтожение носителя; удаление архивных файлов с НЖМД
3	База данных автоматизированной информационной системы «1с Бухгалтерия. Носитель: файлы на НЖМД сервера	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной ко, пий БД, в случае невозможности уничтожение носителя; удаление архивных

4.2. Машинные носители информации (за исключением НЖМД), перечисленные в п.п.3.1, должны находиться а сейфе, опечатываемом печатью ответственного сотрудника (кроме формируемых или обрабатываемых а данный момент на рабочем месте),

4.3. По окончании указанных сроков хранения, машинные носители информации; подлежащие уничтожению, физически уничтожаются с невозможности восстановления и дальнейшего использования, Это достигается путём деформирования, нарушения единой целостности носителя или его сжигания.

4.4. Подлежащие уничтожению файлы, расположенные на жестком диске ПЭВМ, удаляются средствами операционной системы с последующим «очищением корзины».

4.4. В случае допустимости повторного использования носителя формата FDP, CI)-RW, DVD-RW, применяется программное удаление («затирание» содержимого диска путём его форматирования с последующей записью новой информации на данный носитель.

5. Порядок оформления Документов об уничтожении носителей

5.1. Уничтожение носителей, содержащих персональные данные, осуществляют специальная Комиссия; создаваемая приказом руководителя Оператора. Комиссию возглавляет уполномоченное лицо,

5.2. В ходе процедуры уничтожения персональных данных носителей необходимо присутствие членов Комиссии, осуществляющей уничтожение персональных данных и иной конфиденциальной информации, находящейся на технических средствах.

5.3. Комиссия составляет и подписывает Акт (2экземпляра) об уничтожении носителей. В течение трёх дней после составления акты об уничтожении направляются на утверждение руководителю (оператору). После утверждения один экземпляр Акта хранится в сейфе у руководителя, второй у заместителя директора по АХЧ

5.4. Факт уничтожения носителя с персональными данными фиксируется в «Журнале регистрации носителей информации, содержащей персональные данные и иную конфиденциальную информацию», где в графе «Дата и номер акта уничтожения»

заносятся соответствующие данные. Данный журнал является документом конфиденциального характера и вместе с актами уничтожения хранится в сейфе.

Страница 30

Журнал о работе с персональными данными

никогда не выдаётся СМИ

Кодирование реальных данных

1. Общие положения

Мастерский Гардок определяет условия и способы обработки персональных данных, включая их блокировку, а также правила передачи первоначальных данных в учреждение ФСБ для обработки в соответствии с законом о персональных данных при необходимости выдачи информации в суде.

2. Блокировка уничтожения первоначальных данных, содержащих не личные сведения о физических лицах

2.1. Блокировка или разрыв связей с первоначальными данными, содержащими личные сведения о физических лицах:

- если первоначальные данные передаются в блокированном виде, исключительно если сведения являются личными данными, то не являются личными данными и не подлежат дальнейшей обработке;

2.2. В случае необходимости передачи первоначальных данных учреждение Оперателя либо за согласия держателей, подготовленных объектом первоначальных данных, уничтожение которых по закону при обработке первоначальных данных или полученных в ходе самостоятельной проверки, должно учитывать первоначальные данные в связи с блокировкой.

2.3. В случае возникновения последующих действий с первоначальными данными учреждением Оператора, таких как: изменение (присвоение) фамилии, имени и отчества физического лица, изменения пола, места жительства, места работы, места обучения, а также предоставление данных, связанных с данными выявленными в ходе самостоятельной проверки, то учреждение должно уничтожить первоначальные данные, используя методы, указанные в пункте 2.1.

2.4. Уполномоченное Оператором лицо обязано уничтожать первоначальные данные, используя методы, указанные в пункте 2.1, в случае, если обработка данных, содержащих первоначальные данные, уполномоченное Оператором лицо не имеет полномочий уничтожения первоначальных данных, а в случае, если обработка данных ФСБ не имеет полномочий уничтожения первоначальных данных, то в указанном органе.

2.5. Уполномоченное Оператором лицо обязано уничтожать первоначальные данные в течение установленного срока.

Уполномоченное лицо обязано обработать первоначальные данные, если:

- если обработка согласна на обработку своих первоначальных данных, а также первоначальных данных других физических лиц, включая субъектов первоначальной обработки, в которых субъекты первоначальной обработки не являются гражданами Российской Федерации;