

## **ПОРЯДОК уничтожения, блокирования персональных данных**

### **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, содержащихся в 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 обязано 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 устранении 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 оператором;
- 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 1:

Таблица 1

Виды и периоды уничтожения бумажных носителей, содержащих персональные данные

| № п/п | Документ   | Срок хранения   | Действия по окончании срока хранения |
|-------|--|---|--------------------------------------|
| 1.    | Документы (сведения, содержащие персональные данные о работниках Оператора), переданные и сформированные при трудоустройстве работника.          | 75 лет  | Уничтожение                          |
| 2.    | Документы о воспитанниках (сведения, содержащие персональные данные воспитанников).  | установленные для данных документов сроки хранения          | Уничтожение                          |
| 3.    | Другие документы с грифом «Конфиденциально» и «Для служебного пользования» (Журналы учёта, списки доступа, эксплуатационная документация и т.п.) | хранятся до замены на новые, если не указан конкретный срок | Уничтожение                          |

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

3.3. По окончании срока хранения документы, указанные в п. 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 – CD-R/RW, DVD-R/RW в зависимости от формата), дискетах 3,5“ 1.4Mb (далее – FDD), FLASH-накопителях.

Таблица 2

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

| № п/п | Информация, вид носителя   | Срок хранения                      | Действия по окончании срока хранения   |
|-------|--|------------------------------------|--|
| 1.    | База данных автоматизированной информационной системы Оператора.<br>Носитель: файлы на НЖМД сервера              | До создания более актуальной копии | Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности – уничтожение носителя; удаление архивных файлов с НЖМД |
| 2.    | База данных автоматизированной информационной системы «1С Предприятие-Кадры».<br>Носитель: файлы на НЖМД сервера | До создания более актуальной копии | Повторное использование носителя для записи очередной резервной копии 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 копии БД, в случае невозможности – уничтожение носителя; удаление архивных файлов с НЖМД |
|----|---|------------------------------------|--|

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

4.3. По окончании указанных сроков хранения, машинные носители информации, подлежащие уничтожению, физически уничтожаются с целью 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 FDD, CD-RW, DVD-RW, FLASH 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, осуществляет специальная Комиссия, создаваемая приказом руководителя Оператора. Комиссию возглавляет руководитель службы информационной безопасности Оператора (*или иное уполномоченное лицо*). В состав Комиссии должен входить сотрудник отдела автоматизированных информационных систем и руководитель соответствующего подразделения Оператора.

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 Оператора. После утверждения один экземпляр Акта хранится в сейфе у руководителя соответствующего подразделения Оператора, второй экземпляр Акта хранится у руководителя службы информационной безопасности Оператора.

5.4. Факт уничтожения носителя с персональными данными фиксируется в «Журнале регистрации носителей информации, содержащих 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.

УТВЕРЖДАЮ

\_\_\_\_\_ (Ф.И.О., подпись)

« \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**А К Т №**

уничтожения персональных данных и иной конфиденциальной информации,  
находящейся на технических средствах информационных систем

\_\_\_\_\_ « \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.  
(место уничтожения) (дата уничтожения)

Комиссия, в составе:

Председатель:

\_\_\_\_\_  
(должность, фамилия, имя, отчество)

Члены:

\_\_\_\_\_  
(должность, фамилия, имя, отчество)

\_\_\_\_\_  
(должность, фамилия, имя, отчество)

составили настоящий акт в том, что « \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г. произведено уничтожение персональных данных или иной конфиденциальной информации, находящейся

на \_\_\_\_\_

\_\_\_\_\_ (наименование АРМ по утвержденной конфигурации, ФИО ответственного Пользователя АРМ, заводской или учетный номер системного блока ПЭВМ)

| № | Информация | Вид носите- | Коли- | Примечание |
|---|------------|-------------|-------|------------|
|---|------------|-------------|-------|------------|

| п/п | (наименование документа) | ля,<br>учетный но-<br>мер | чество |  |
|-----|--------------------------|---------------------------|--------|--|
|     |                          |                           |        |  |
|     |                          |                           |        |  |

Перечисленные съемные носители уничтожены путем

---

(механического уничтожения, сжигания, разрезания, демонтажа и т.п.)

---

Подписи членов комиссии:

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(Ф. И. О.)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(Ф. И. О.)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(Ф. И. О.)