



«Утверждено»

Заведующий МБДОУ «Детский сад
комбинированного вида № 17 «Василёк»
ЗМР РТ

С.В. Папилова
С.В. Папилова
ВВЕДЕНО В ДЕЙСТВИЕ

Приказом № 4/3 от 12.01.2023 г.

**Регламент выгрузки и передачи персональных данных
муниципального бюджетного дошкольного образовательного
учреждения
«Детский сад комбинированного вида № 17 «Василёк»
Зеленодольского муниципального района Республики Татарстан**

СОДЕРЖАНИЕ

	стр.
Используемые сокращения	3
Термины и определения	4
1 Общие положения	5
2 Права и обязанности работников	6
3 Обеспечение безопасности персональных данных при их выгрузке на носители и последующей передаче	7

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Сокращение	Полное наименование
Система	государственная информационная система Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений»,
ИБ	Информационная безопасность
Орган	Органы государственной власти / Органы местного самоуправления
ПДн	Персональные данные

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Закон	Федеральные законы от 27.07. 2006 г. № 152-ФЗ «О персональных данных», от 14.07. 2022 года № 266-ФЗ «О внесении изменений в Федеральный закон о персональных данных»
Обезличивание	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту ПДн
Обработка персональных данных (ПДн)	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 ПДн
Ответственный за обеспечение безопасности ПДн	Структурное подразделение Органа, ответственное за обеспечение безопасности ПДн
Передача ПДн	Доведение ПДн до уполномоченного представителя контрагента или третьего лица каким-либо образом (передача, пересылка, ознакомление, осуществление доступа)
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн)
Распространение персональных данных	Действия, направленные на раскрытие ПДн неопределенному кругу лиц
Уточнение персональных данных	Корректировка ПДн, обрабатываемых в организации, которая производится в случае недостоверности обрабатываемых данных или в случае их изменения

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящий документ устанавливает порядок обеспечения безопасности ПДн и выполнение положений Закона при осуществлении выгрузки ПДн из Системы.
- 1.2. Требования настоящего Регламента распространяются на Органы, в которых работают пользователи Системы.
- 1.3. При осуществлении выгрузки ПДн с целью обмена (передачи) ПДн между Органами и контрагентами/третьими лицами следует руководствоваться документом «Регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами».
- 1.4. Данный Регламент охватывает случаи осуществления выгрузки ПДн на бумажные носители.
- 1.5. Вывод ПДн на машинные носители (например, USB-флэш диски, DVD/CD диски) запрещен.

2. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКОВ

1.1 В рамках обеспечения ИБ при выгрузке и передаче ПДн выделяются следующие роли:

- руководители структурных подразделений, в которых работают пользователи;
- пользователи.

1.2 На руководителей структурных подразделений органов, осуществляющих обработку ПДн, возлагаются следующие обязанности:

1) проведение инструктажа пользователей Системы (под роспись в «Журнале проведения инструктажа»), для ознакомления со следующими документами:

– регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами;

– правила обеспечения безопасности персональных данных при их обработке;

– политика подсистемы разграничения доступа;

– настоящий регламент.

2) ознакомление пользователей Системы с перечнем обрабатываемых ими ПДн, на основании документа «Перечень персональных данных подлежащих защите»;

3) учет работников своего подразделения, допущенных к обработке ПДн Системы;

4) обеспечение выполнения пользователями Системы требований документов:

– регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами;

– правила обеспечения безопасности персональных данных при их обработке;

– политика подсистемы разграничения доступа;

– настоящий регламент.

1.3 На пользователей, обрабатывающих ПДн в рамках Системы, возлагаются обязанности по соблюдению положений организационно-распорядительной документации для обеспечения защиты ПДн в рамках Системы в части их касающейся.

3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ВЫГРУЗКЕ НА НОСИТЕЛИ И ПОСЛЕДУЮЩЕЙ ПЕРЕДАЧЕ

3.1. Обеспечение безопасности ПДн при их выгрузке на материальные носители достигается за счет реализации описанного ниже порядка.

3.2. Пользователь Системы осуществляет выгрузку ПДн на материальный носитель и передает полученные материальные носители на согласование руководителю соответствующего структурного подразделения Органа.

3.3. На передаваемых материальных носителях проставляется отметка «Конфиденциально», либо «Для служебного пользования» согласно действующим в Органе порядком конфиденциального делопроизводства.

3.4. При работе с материальными носителями ПДн пользователями Системы должны быть выполнены следующие условия:

3.5. Передача материальных носителей ПДн между пользователями одного структурного подразделения Органа осуществляется в соответствии с действующим в органе порядком конфиденциального делопроизводства.

3.6. Передача материальных носителей ПДн вручную (почтой, курьером или лично уполномоченным представителям контрагентов и третьих лиц), контрагентам или третьим лицам осуществляется только по поручению руководителя органа в соответствии документом «Регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами».

3.7. При необходимости уничтожения материальных носителей ПДн должны соблюдаться следующие условия:

3.8. Материальные носители ПДн, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

3.9. По истечении срока согласия субъекта на обработку его ПДн, ПДн уничтожаются.

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

3.11. Все материальные носители, содержащие ПДн, должны храниться в специально выделенных служебных помещениях или в запираемых и опечатываемых шкафах (хранилищах). При этом должны быть созданы необходимые условия, обеспечивающие их физическую сохранность.

3.12. При выходе пользователя из служебного помещения материальные носители должны быть убраны в хранилища.

3.13. Хранение материальных носителей ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки. По достижении целей обработки или в случае утраты необходимости в их достижении ПДн подлежат уничтожению за исключением случаев, предусмотренных законодательством РФ.

3.14. Все ПДн (материальные носители), обработка которых осуществляется в различных целях, должны храниться отдельно.

3.15. Хранение и выдачу носителей ПДн организывают руководители структурных подразделений органов, в которых работают пользователи.

3.16. Документы, содержащие ПДн субъектов ПДн, должны храниться в течение срока, определенного в согласии субъектов на обработку его ПДн.