Приложение № 3

к приказу от 01.03.2021г. № 23

**Правила**

**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБУ «Верхнеуральский центр помощи детям, оставшимся без попечения родителей»**

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в МБУ «Верхнеуральский центр помощи детям, оставшимся без попечения родителей» (далее - Учреждение) разработаны в целях выявления и предотвращения нарушений законодательства Российской Федерации в сфере персональных данных.

2. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее - внутренний контроль) осуществляется в соответствии с Федеральным [законом](consultantplus://offline/ref=166FD1F20230E30F5FE30753AF055D1AF93B680521DC32C6CFFAF2B5A8w6qAE) от 27 июля 2006 года N 152-ФЗ "О персональных данных", [постановлением](consultantplus://offline/ref=166FD1F20230E30F5FE30753AF055D1AFA3C63002BD932C6CFFAF2B5A8w6qAE) Правительства Российской Федерации от 21 марта 2012 года N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" и локальными актами оператора.

3. Настоящие Правила определяют порядок осуществления внутреннего контроля в Учреждении и действуют постоянно.

4. В целях осуществления внутреннего контроля в Учреждении организовывается проведение проверок условий обработки персональных данных.

Тематика проверок внутреннего контроля:

1) с использованием средств автоматизации: соответствие полномочий матрице доступа;

* соблюдение пользователями информационных систем персональных данных службы парольной политики;
* соблюдение пользователями информационных систем персональных данных службы антивирусной политики;
* соблюдение пользователями информационных систем персональных данных службы правил работы со съемными носителями персональных данных;
* соблюдение порядка доступа в помещения службы, где расположены элементы информационных систем персональных данных;
* соблюдение порядка резервирования баз данных и хранения резервных копий;

2) без использования средств автоматизации:

* хранение бумажных носителей с персональными данными;
* доступ к бумажным носителям с персональными данными;
* доступ в помещения, где обрабатываются и хранятся бумажные носителя с персональными данными.

5. Проверки условий обработки персональных данных на соответствие требованиям к защите персональных данных (далее - проверки) осуществляются комиссией, создаваемой приказом директора Учреждения.

6. Проверки внутреннего контроля проводятся по поручению директора Учреждения не реже 1 раза в три года либо в связи с поступившим в Учреждение обращением субъекта персональных данных о нарушениях правил обработки персональных данных.

7. В течение трех рабочих дней с момента поступления в Учреждение заявления о нарушениях правил обработки персональных данных принимается решение о проведении проверки, которое оформляется приказом директора Учреждения.

8. Проведение проверки организуется в течение трех рабочих дней с момента оформления приказа о проведении проверки внутреннего контроля.

9. При проведении проверки комиссией устанавливается соблюдение или нарушение правил обработки персональных данных установленным требованиям.

10. Срок проведения внеплановой проверки не должен превышать 30 календарных дней со дня регистрации обращения субъекта персональных данных.

11. При проведении проверки комиссия имеет право:

1) запрашивать у сотрудников Учреждения информацию, необходимую для проведения проверки;

2) вносить директору Учреждения предложения о принятии мер (правовых, организационных, технических) по обеспечению безопасности персональных данных при их обработке;

3) вносить директору Учреждения предложения о привлечении к дисциплинарной ответственности лиц, нарушивших правила обработки персональных данных.

12. Для каждой проверки оформляется акт проверки внутреннего контроля. Решение комиссии оформляется протоколом проведения проверки. Форма [акта](#Par67) и [протокола](#Par129) приведены в приложении к настоящим Правилам.

13. О результатах проведенной проверки и мерах, необходимых для устранения нарушений (в случае их выявления), директору Учреждения докладывает ответственный за организацию обработки персональных данных.

14. Членами комиссии обеспечивается конфиденциальность персональных данных, ставших известными им при проведении проверки.

15. Контроль за своевременностью и правильностью проведения назначенных проверок осуществляется директором Учреждения.

Приложение 1

к Правилам

осуществления внутреннего контроля

соответствия обработки персональных данных

требованиям к защите персональных данных

АКТ

ПРОВЕДЕНИЯ ПРОВЕРКИ СООТВЕТСТВИЯ ОБРАБОТКИ

ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

ОТ "\_\_" \_\_\_\_\_\_\_\_\_ 20\_\_ ГОДА

Членами комиссии внутреннего контроля в МБУ «Верхнеуральский центр помощи детям, оставшимся без попечения родителей» проведена проверка соответствия обработки персональных данных требованиям к защите персональных данных.

Тема проверки:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В ходе проведения проверки установлено:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Возможные нарушения требований к защите персональных данных (ПДн) | Наличие нарушения |
| Соблюдение пользователями информационных систем ПДн антивирусной политики (работа с ПДн на рабочем месте, не защищенном антивирусной программой) |  |
| Обработка ПДн сотрудниками, не включенными в перечень допущенных в обработке ПДн |  |
| Отсутствие или неактуальность перечня сотрудников, допущенных к обработке ПДн |  |
| Обработка ПДн после достижения цели обработки ПДн |  |
| Отсутствие записей в журнале учета электронных носителей ПДн при использовании самих носителей |  |
| Отсутствие подписанных обязательств о неразглашении ПДн |  |
| Хранение файлов на рабочей станции сотрудника, содержащих ПДн |  |
| Соблюдение пользователями информационных систем персональных данных парольной политики (доступность логина, пароля для доступа в информационные системы ПДн для посторонних) |  |
| Возможность считывания информации с экрана монитора для посторонних |  |
| Соблюдение порядка доступа в помещение, в котором ведется обработка ПДн |  |
| Отсутствие записей в журнале учета уничтожения ПДн |  |

Рекомендации по устранению выявленных нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Председатель комиссии: / /

Члены комиссии: / /

/ /

/ /

Приложение 2

к Правилам

осуществления внутреннего контроля

соответствия обработки персональных данных

требованиям к защите персональных данных

ПРОТОКОЛ

ПРОВЕДЕНИЯ ПРОВЕРКИ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ

ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящий Протокол составлен в том, что комиссией по внутреннему контролю проведена проверка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(указывается тема проверки)

По результатам проверки составлен акт от "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Проверка осуществлялась в соответствии с требованиями Федерального [закона](consultantplus://offline/ref=166FD1F20230E30F5FE30753AF055D1AF93B680521DC32C6CFFAF2B5A8w6qAE) от 27 июля 2006 года N 152-ФЗ "О персональных данных", [постановления](consultantplus://offline/ref=166FD1F20230E30F5FE30753AF055D1AFA3C63002BD932C6CFFAF2B5A8w6qAE) Правительства Российской Федерации от 21 марта 2012 года N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным [законом](consultantplus://offline/ref=166FD1F20230E30F5FE30753AF055D1AF93B680521DC32C6CFFAF2B5A8w6qAE) "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора".

В ходе проверки проверено:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Выявленные нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок устранения нарушений: до "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года.

Председатель комиссии:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

Члены комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/