Приложение 1

к распоряжению администрации Бобровского муниципального района

Воронежской области

от 01.11.2013 г. № 372-р

**Правила**

**осуществления в администрации Бобровского муниципального района Воронежской области внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных**

1. Настоящие Правила устанавливают процедуры проведения в администрации Бобровского муниципального района Воронежской области (далее - администрация) внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральным законодательством о персональных данных.

2. Настоящие Правила разработаны с учетом требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21.03.2012 № 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».

3. Целью настоящих Правил является выявление и предотвращение нарушений законодательства Российской Федерации в сфере защиты персональных данных.

4. Для осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в администрации организуется проведение проверок условий обработки персональных данных.

5. Тематика проверок обработки персональных данных с использованием средств автоматизации:

- соответствие полномочий пользователя разрешенной системе доступа;

- соблюдение пользователями информационных систем персональных данных парольной политики;

- соблюдение пользователями информационных систем персональных данных антивирусной политики;

- соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных;

- соблюдение ответственными за криптографические средства защиты информации правил работы с ними;

- соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;

- соблюдение порядка резервирования баз данных и хранения резервных копий;

- соблюдение порядка работы со средствами защиты информации;

- знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях.

6. Тематика проверок обработки персональных данных 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 носители с персональными данными.

7. Проверки условий обработки персональных данных на соответствие требованиям к защите персональных данных, установленных в администрации (далее - проверки), осуществляются ответственным за организацию обработки персональных данных и ответственным за обеспечение безопасности персональных данных - администратором безопасности информационных систем персональных данных в администрации.

8. Проверки могут быть плановыми и внеплановыми, документарными и проводимыми в помещениях администрации, в которых ведется обработка персональных данных.

9. Плановые проверки проводятся в соответствии с ежегодным планом проведения проверок, не менее двух раз в год.

10. План проведения проверок разрабатывается лицом, ответственным за организацию обработки персональных данных в администрации.

11. Внеплановые проверки проводятся на основании поступившего в администрацию письменного заявления физического лица (субъекта персональных данных) о нарушениях правил обработки персональных данных.

12. Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления в администрацию соответствующего заявления.

13. При проведении проверок должен быть полностью, объективно и всесторонне исследован порядок обработки персональных данных и его соответствие требованиям обработки персональных данных, установленным в администрации, а именно:

- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора персональных данных;

- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

- достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;

- отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

14. В случае выявления нарушений обязательных требований соответствия обработки персональных данных требованиям к защите персональных данных, установленных федеральным законодательством, ответственный за организацию обработки персональных данных в администрации, проводящий плановую проверку, обязан сообщить главе администрации о выявленных нарушениях в течение пяти рабочих дней со дня окончания проведения плановой проверки.

15. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных - администратор безопасности информационных систем персональных данных в администрации при проведении проверки имеют право:

- запрашивать у работников администрации информацию, необходимую для реализации полномочий;

- требовать от уполномоченных на обработку персональных данных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить главе администрации предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить главе администрации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

16. В процессе проведения внутреннего контроля (проверок) соответствия обработки персональных данных требованиям к защите персональных данных разрабатываются меры, направленные на предотвращение негативных последствий выявленных нарушений.

17. В случаях выявления нарушений обработки персональных данных, требующих немедленного устранения, принимаются меры оперативного реагирования.

18. Плановая проверка должна быть завершена не позднее чем через двадцать рабочих дней со дня ее начала.

19. Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении к настоящим Правилам.

20. При выявлении в ходе проверки нарушений, ответственным за организацию обработки персональных данных в администрации в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения. Устранение выявленных нарушений проводится не позднее 30 дней с момента подписания Протокола, если в нем не определено иное.

21. Заключение о результатах проведенной проверки и принятых по устранению выявленных нарушений мерах, а также мерах, необходимых для устранения нарушений, направляется ответственным за организацию обработки персональных данных в администрации главе администрации.

22. Протоколы хранятся у ответственного за организацию обработки персональных данных в администрации в течение текущего года.

23. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в администрации в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться их конфиденциальность.

Приложение

к Правилам осуществления в администрации Бобровского муниципального района Воронежской области внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

**Форма Протокола**

**проведения внутренней проверки условий обработки персональных данных**

**в администрации Бобровского муниципального района Воронежской области**

Настоящий Протокол составлен в том, что \_\_.\_\_.20\_\_ ответственным за организацию обработки персональных данных в администрации и ответственным за обеспечение безопасности персональных данных - администратором безопасности информационных систем персональных данных в администрации проведена проверка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 (тема проверки)

Проверка осуществлялась в соответствии с требованиями \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(название документа)

 В ходе проверки проверено: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 Выявленные нарушения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 Меры по устранению нарушений: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 Срок устранения нарушений: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(должность ответственного)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(должность ответственного) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_(Ф.И.О.)\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Ф.И.О.) |