**АДМИНИСТРАЦИЯ ЖИРЯТИНСКОГО РАЙОНА**

П ОС Т А Н О В Л Е Н И Е

от 10.12.2019 года № 415

с. Жирятино

Об утверждении Правил осуществления внутреннего

контроля соответствия обработки персональных данных

требованиям к защите персональных данных

в администрации Жирятинского района

В соответствии с  Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»; Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Постановлением Правительства Российской Федерации  от 17.11.2007 №  781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»; Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»; Постановлением 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 и муниципальными органами»

**ПОСТАНОВЛЯЮ:**

 1. Утвердить  Правила  осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных  в администрации Жирятинского района (приложение).

2. Настоящее постановление подлежит опубликованию на официальном сайте администрации Жирятинского района в течение 10 дней после его принятия.

 3. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации Жирятинского района Пожарскую В.П..

Глава администрации района Л.А. Антюхов

*И.А. Елисеева*

*8/848344/3-06-11*

Приложение

к постановлению администрации

Жирятинского района

от 10.12.2019 года № 415

**Правила**

**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных  в администрации Жирятинского района**

**1.  Общие положения**

1.1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации муниципального образования Жирятинского района (далее - Правила)  устанавливаются процедуры (основания, порядок и формы) проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. Настоящие Правила разработаны в соответствии с  Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»; Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Постановлением Правительства Российской Федерации  от 17.11.2007 №  781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»; Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»; Постановлением 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 и муниципальными органами»; Приказом ФСТЭК РФ от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» и другими нормативными правовыми актами.

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

1.4. В Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

**2. Тематика внутреннего контроля**

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

соответствие полномочий пользователя правилам доступа;

соблюдение пользователями информационных систем персональных данных департамента парольной политики;

соблюдение пользователями информационных систем персональных данных

департамента антивирусной политики;

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

соблюдение порядка доступа в помещения департамента, 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.

2.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

организация хранения бумажных носителей с персональными данными;

доступ к бумажным носителям с персональными данными;

доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

**3.** **Процедуры, направленные на выявление и предотвращение нарушений** **законодательства Российской Федерации**

**в сфере персональных данных**

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в администрации Жирятинского района (далее - Администрация) организовывается проведение проверок условий обработки персональных данных.

3.2. Проверки условий обработки персональных данных на соответствие требованиям к защите персональных данных, установленных в Администрации и ее отраслевых органах (далее - проверки) осуществляются комиссией, утвержденной распоряжением  Администрации (далее - Комиссия по персональным данным).

3.3.  Проверки условий обработки персональных данных могут быть плановыми и внеплановыми, документарными и проводимыми в помещениях Администрации, в которых ведется обработка персональных данных.

3.4. Плановые проверки проводятся в соответствии с ежегодным планом проведения проверок, утвержденным  распоряжением Администрации.

3.5.  План проведения проверок разрабатывается лицом, ответственным за организацию обработки персональных данных в Администрации.

3.6. Внеплановые проверки проводятся на основании поступившего в Администрацию на имя главы Администрации письменного заявления физического лица (субъекта персональных данных) о нарушениях правил обработки персональных данных.

3.7. В течение трех рабочих дней с момента поступления в Администрацию заявления о нарушениях правил обработки персональных данных принимается решение о проведении внеплановой проверки, которое оформляется распоряжением Администрации.

3.8. Проведение внеплановой проверки организуется в течение трех рабочих дней с момента оформления Распоряжения Администрации о проведении внеплановой проверки.

3.9. При проведении проверок условий обработки персональных данных 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.

3.10.    В случае выявления фактов:

несоблюдения установленного порядка обработки персональных данных;

несоблюдения условий хранения носителей персональных данных;

использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;

нарушения заданного уровня безопасности персональных данных (конфиденциальность/ целостность/доступность);

в обязательном порядке устанавливаются причины нарушения обработки персональных данных и наличие (отсутствие) вины.

3.11.    Комиссия по персональным данным имеет право:

запрашивать у сотрудников 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.

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

3.13. В случаях выявления нарушенийобработки персональных данных, требующих немедленного устранения, принимаются меры оперативного реагирования.

3.14.  Плановая  проверка должна быть завершена не позднее чем через месяц со дня её назначения.  Заключение о результатах проведенной проверки и принятых по устранению выявленных нарушений мерах, а также мерах, необходимых для устранения нарушений, направляется главе администрации за подписью председателя Комиссии по персональным данным.  

3.15. Устранение выявленных нарушений проводится не позднее 30 дней с момента  завершения  проверки.

3.16. В отношении персональных данных, ставших известными Комиссии по персональным данным в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

 3.17. По результатам проверки составляется протокол проведения внутренней проверки. Форма протокола приведена в Приложении к настоящим Правилам. При проверке назначенным сотрудником может составляться акт по произвольной форме.

3.18. При выявлении в ходе проверки нарушений, в протоколе или акте делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.19. Протоколы и акты хранятся у ответственного за организацию обработки персональных данных. Уничтожение протоколов и актов проводится ответственным самостоятельно в январе года, следующего за проверочным годом. При необходимости протоколы и акты могут храниться до полного устранения нарушений.

3.20. О результатах проверки и мерах, необходимых для устранения нарушений, главе Администрации докладывает ответственный за организацию обработки персональных данных в Администрации.

|  |  |
| --- | --- |
|  | Приложение  к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных  в администрации Жирятинского района |

|  |  |
| --- | --- |
|  | **УТВЕРЖДАЮ**  **Глава администрации**  **Жирятинского района**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **«\_\_\_» \_\_\_\_\_\_\_\_ 20\_\_ г.** |

Протокол

проведения внутренней проверки условий обработки персональных данных администрации Жирятинского района

Настоящий Протокол составлен в том, что \_\_.\_\_.20\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (комиссией)

(должность, Ф.И.О. сотрудника)

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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Председатель комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия

Члены комиссии:

Должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия

Должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия

Должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия

Должность руководителя проверяемого

подразделения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия