Приложение № 3

к Распоряжению Мэра ЗАТО Северск

 от 01.08.2018\_\_№ \_145 рм\_

**ПРАВИЛА**

**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных**

1. ОБЩИЕ ПОЛОЖЕНИЯ
2. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Думе ЗАТО Северск (далее – Правила) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», 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 или муниципальными органами».
3. Настоящие Правила определяют порядок и методику осуществления внутреннего контроля соответствия обработки персональных данных в Думе ЗАТО Северск (далее-Дума) требованиям к защите персональных данных, установленных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов.
4. Контроль за соблюдением настоящих Правил возлагается на ответственного за организацию обработки персональных данных.
5. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК
6. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, в Думе организуется проведение периодических проверок условий обработки персональных данных в соответствии с планом внутренних проверок условий обработки персональных данных, а также внеплановых проверок условий обработки персональных данных.
7. Проведение внутренних проверок в Думе организует и осуществляет ответственный за организацию обработки персональных данных.
8. Проверки проводятся постоянной комиссией в области обработки персональных данных в Думе, созданной распоряжением Мэра ЗАТО Северск.
9. Внеплановые проверки проводятся в случае поступления в Думу сведений об имеющихся нарушениях при осуществлении обработки персональных данных в соответствии с распоряжением Мэра ЗАТО Северск*.*
10. По результатам проверки ответственным лицом за организацию обработки персональных данных производится запись в журнале учета внутренних проверок и оформляется соответствующий протокол проведения внутренней проверки.
11. В протоколе проведения внутренней проверки производится отметка о соответствии/несоответствии проверяемых критериев, заданных методикой, предусмотренной разделом III настоящих Правил, а также запись о мероприятиях по устранению выявленных нарушений, сроках их устранения и ответственных за устранение выявленных нарушений лицах.
12. Протоколы хранятся у ответственного лица за организацию обработки персональных данных в течение текущего года. Уничтожение протоколов обеспечивается ответственным лицом (комиссией) самостоятельно в январе года, следующего за проверочным.
13. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, ответственный за организацию обработки персональных данных докладывает Мэру ЗАТО Северск.
14. МЕТОДИКА ПРОВЕДЕНИЯ ПРОВЕРКИ
15. Проверки осуществляются комиссией непосредственно на месте обработки персональных данных путем опроса сотрудников Думы, осмотра рабочих мест сотрудников Думы, участвующих в процессе обработки персональных данных, а также в иных формах в соответствии с действующим законодательством.
16. Проверка организационной части включает в себя:

|  |  |
| --- | --- |
| 31 | Наличие действующего распоряжения о назначении постоянной комиссии по персональным данным в Думе |
| 2 | Наличие действующего распоряжения о назначении ответственного лица за организацию обработки персональных данных |
| 43 | Наличие актуальных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных |
| 74 | Наличие актуального перечня сотрудников, допущенных к обработке персональных данных |
| 85 | Наличие актуального перечня информационных систем персональных данных |
| 96 | Наличие актуального перечня персональных данных |
| 17 | Проверка наличия и актуальности внутренних организационно-распорядительных документов (Правила, положения, инструкции, регламенты, план мероприятий). |
| 18 | Проверка наличия актуальных документов, определяющих политику обработки персональных данных в общедоступных источниках |
| 99 | Проверка наличия документов, подтверждающих факт ознакомления допущенных к обработке сотрудников с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, с документами, определяющими политику Думы в отношении обработки персональных данных, с локальными актами по вопросам обработки персональных данных и (или) обучения указанных сотрудников |
| 110 | Наличие актуального (полного и достоверного) отправленного в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) уведомления об обработке персональных данных (письма о внесении изменений в уведомление) |
| 111 | Наличие согласий работников на обработку их персональных данных |
| 112 | Наличие письменных обязательств сотрудников, допущенных к обработке персональных данных, о неразглашении персональных данных |
| 113 | Наличие соглашений (существенных условий договоров) с контрагентами о соблюдении конфиденциальности передаваемых персональных данных (в случае такой передачи по договору) |
| 114 | Наличие согласий субъектов на опубликование их персональных данных в общедоступных источниках |
| 115 | Наличие и ведение журнала запросов субъектов персональных данных по вопросам обработки персональных данных и наличие правил обработки таких запросов |
| 216 | Проверка соблюдения оператором правил работы (хранения и уничтожения) с носителями персональных данных |
| 217 | Наличие актуального плана мероприятий по обеспечению безопасности персональных данных и ведение журнала внутренних проверок в области обработки персональных данных |
| 218 | Проверка соблюдения сотрудниками правил доступа в помещения, в которых происходит обработка и хранение бумажных носителей персональных данных, а также в которых расположены компоненты информационной системы персональных данных |
| 219 | Своевременность проведения мероприятий по уничтожению персональных данных |

Приложение № 1

к Правилам осуществления внутренних

проверок в области обработки

персональных данных в

Думе ЗАТО Северск

**Форма журнала учета внутренних проверок**

**в области обработки персональных данных**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Дата начала и окончания проверки**  | **Исполнитель/ Проверяющий** | **Результат проверки** | **Подпись ответственного за организацию обработки персональных данных** | **Примечание** |
| **1** | **2** | **3** | **4** | **5** | **6** |
|  |  |  |  |  |  |

Примечание.

Заполнение полей журнала:

1-порядковый номер проверки в данном журнале.

2-даты начала и окончания проверки в соответствии с распоряжением о проведении проверки.

3-заносятся ФИО исполнителя (исполнителей), назначенных распоряжением руководителя аппарата Думы.

4-указывается дата составленного Протокола по результатам проведения проверки.

5-подпись и расшифровка подписи (Ф.И.О.) ответственного лица за организацию обработки персональных данных.

6-заносится номер и дата распоряжения о проведении проверки, вид проверки (плановая/внеплановая (в связи с чем)) и другая полезная по мнению ответственного за организацию обработки персональных данных информация.

Приложение № 2

к Правилам осуществления внутренних

проверок в области обработки персональных

данных в Думе ЗАТО Северск

**Форма Протокола о проведении внутренней проверки**

**в области обработки персональных данных**

ПРОТОКОЛ

проведения внутренней проверки в области обработки персональных данных

Настоящий Протокол составлен в том, что в срок с «\_\_\_»\_\_\_\_\_\_\_\_\_ 20\_\_ г. по «\_\_\_»\_\_\_\_\_\_\_\_\_ 20\_\_ г. комиссией в составе:

Председатель комиссии:

- \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

Члены комиссии:

- \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

- \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

утвержденной распоряжением от \_\_\_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_, проведена внутренняя проверка в области обработки персональных данных на соответствие условий обработки ПДн требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов.

Проверка является плановой (внеплановой, в связи с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) и осуществлялась на основании Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (утв. распоряжением Мэра ЗАТО Северск от \_\_\_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_) и Плана мероприятий по обеспечению безопасности персональных данных (утв. распоряжением от \_\_\_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_).

В ходе проверки было выявлено:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№****п/п** | **Критерий** | **Соответствие/ Несоответствие (+/ -)** | **Выявленное нарушение** | **Меры по устранению нарушений** | **Сроки устранения нарушений** | **Ответственный** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Председатель комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

Члены комиссии:

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.