|  |  |
| --- | --- |
|  | Приложение 3  к приказу руководителя *Организации*  от № |

Правила обработки персональных данных в *Организации*

Раздел I

Общие положения

1. Настоящие Правила обработки персональных данных (далее — Правила) в *Организации* разработаны в соответствии с законодательством Российской Федерации и законодательством Тверской области и устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

Раздел II

Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

1. Источником информации о нарушениях законодательства Российской Федерации в сфере персональных данных являются:
2. сообщения сотрудников или пользователей информационных систем персональных данных *Организации* (далее - ИСПДн);
3. сообщения субъектов персональных данных;
4. уведомления (сообщения) органов, осуществляющих контроль или надзор за деятельностью *Организации*;
5. При получении сообщения о нарушениях законодательства Российской Федерации в сфере персональных данных по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например, путем совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных указанных в подписи сообщения или названных при звонке).
6. Сотрудник, получивший информацию о нарушениях законодательства Российской Федерации в сфере персональных данных, сообщает об этом ответственному за организацию обработки персональных данных в *Организации*.
7. Должностное лицо, ответственное за организацию обработки персональных данных, в письменной форме сообщает о факте нарушения *руководителю Организации*.
8. Приказом *руководителя Организации* для разбора факта нарушения законодательства Российской Федерации в сфере персональных данных создается комиссия, в состав которой могут входить:
9. ответственный за организацию обработки персональных данных;
10. руководитель структурного подразделения *Организации*, в котором зафиксирован факт нарушения законодательства Российской Федерации в сфере персональных данных;
11. руководитель *Организации*;
12. заместитель руководителя *Организации*;
13. субъект персональных данных, права которого в сфере персональных данных нарушены.
14. Комиссия собирает и анализирует все данные об обстоятельствах нарушения законодательства Российской Федерации в сфере персональных данных (электронные письма, файлы протоколов ИСПДн, объяснения сотрудников и др.), устанавливает, имела ли место утечка сведений и обстоятельства ей сопутствующие, определяет перечень лиц, виновных в нарушении предписанных федеральным законодательством и законодательством Тверской области мероприятий по защите персональных данных, устанавливает причины и условия, способствовавшие нарушению.
15. По итогам работы комиссии руководителю *Организации* предоставляется отчет, в котором указываются причина нарушения законодательства Российской Федерации в сфере персональных данных, последствия данного факта, лица, виновные в возникновении нарушения законодательства Российской Федерации в сфере персональных данных, предложения об организации наказания виновных лиц и мерах по недопущению подобных инцидентов в будущем.

Раздел III

Процедуры, определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения

1. Процедуры, определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения сводятся в соответствующую таблицу.

Раздел IV

Порядок учета, хранения и передачи машинных

носителей персональных данных

1. Учет всех видов машинных носителей и накопителей, содержащих персональные данные и используемых в электронно-вычислительной технике (в т.ч дисков, съемных носителей), осуществляется в журнале учета машинных носителей, содержащих персональные данные.
2. Порядок учета машинных носителей определяется в Инструкции об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные ИСПДн.

Раздел V

Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

1. По окончании указанных в разделе 3 сроков хранения персональных данных, они физически уничтожаются с целью невозможности восстановления и дальнейшего использования.
2. Уничтожение персональных данных на программно-технических средствах ИСПДн производится специальными программными средствами, осуществляющими удаление информации без возможности ее восстановления.
3. Уничтожение персональных данных, расположенных на оптических дисках осуществляется путем физического уничтожения носителя.
4. Для уничтожения персональных данных приказом руководителя *Организации* создается комиссия, в состав которой могут входить:
5. ответственный за организацию обработки персональных данных в *Организации*;
6. руководитель *Организации*;
7. заместитель руководителя *Организации*;
8. руководитель структурного подразделения *Организации*, в котором проводится обработка персональных данных;
9. сотрудник *Организации*, имеющий право обработки персональных данных.

Уничтожение персональных данных производится в присутствии всех членов комиссии, которые несут персональную ответственность за правильность и полноту уничтожения персональных данных.

1. По результатам работы комиссии составляется в трех экземплярах Акт уничтожения персональных данных на программно-технических средствах ИСПДн (Приложение к Правилам).

|  |  |
| --- | --- |
|  | Приложение  к правилам обработки персональных данных в *Организации* |

АКТ

уничтожения персональных данных

на программно-технических средствах ИСПДн

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

(Должность, Ф.И.О)

Члены комиссии:

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

(Должность, Ф.И.О)

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

(Должность, Ф.И.О)

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

(Должность, Ф.И.О)

составили настоящий акт в том, что «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. произведено уничтожение персональных данных, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

(наименование персональных данных)

находящихся на \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование ИСПДн и носителя информации)

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

Персональные данные были уничтожены путем \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(способ уничтожения информации)

Председатель комиссии:

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

(Ф.И.О.) (подпись)

Члены комиссии:

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

(Ф.И.О.) (подпись)

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

(Ф.И.О.) (подпись)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.