УТВЕРЖДЕНО

Приказом Директора ООО «Астомстрой»

№\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_

ПОЛОЖЕНИЕ

о порядке осуществления внутреннего контроля за обработкой персональных данных

1. Настоящее Положение:
   1. разработано в соответствии с локальными правовыми актами ООО «Астомстрой» (далее – Организация), в том числе:

* политикой обработки персональных данных, утвержденной приказом Директора ООО «Астомстрой» …………
* политикой обработки персональных данных в процессе трудовой деятельности, утвержденной приказом Директора ООО «Астомстрой» …………
* политикой обработки файлов cookie, утвержденной приказом Директора ООО «Астомстрой» …………;
* политикой информационной безопасности, утвержденной приказом Директора ООО «Астомстрой» от 16.06.2023 г. № 239/1;
* положением о порядке доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе), утвержденным приказом Директора ООО «Астомстрой» от 04.08.2025 г. № 222;
* перечнем информационных ресурсов (систем), содержащих персональные данные, и категориями персональных данных, подлежащих включению в них, утвержденным приказом Директора ООО «Астомстрой» от 05.06.2025 г. №159.
  1. определяет порядок проведения внутреннего контроля за обработкой персональных данных (далее - контроль), направленного на выявление и предотвращение нарушений:
* требований законодательства о персональных данных в Организации;
* локальных правовых актов, принятых в целях обеспечения защиты персональных данных (далее - локальные правовые акты), в том числе:
* документов, определяющих политику Организации в отношении обработки персональных данных;
* порядка доступа в Организации к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе).

1. Целями осуществления контроля в Организации являются:

* проверка выполнения работниками требований законодательства о персональных данных и локальных правовых актов;
* оценка уровня осведомленности и знаний работников в области обработки и защиты персональных данных;
* оценка необходимости и достаточности применяемых мер по обеспечению защиты персональных данных;
* выявление и упреждение нарушений законодательства о персональных данных;
* оказание методической помощи работникам по вопросам обработки персональных данных.

1. Контроль осуществляется специалистом по внутреннему контролю за обработкой персональных данных (далее - специалист) путем проведения мониторинга и внеплановых проверок (далее, если не определено иное, - проверка).
2. Мониторинг каждого структурного подразделения Организации проводится не реже одного раза в год в соответствии с планом проведения мониторинга на соответствующий год по форме согласно приложению 1.

План проведения мониторинга на предстоящий год готовится Специалистом и представляется на утверждение Директору Организации (лицу, исполняющему его обязанности) не позднее 20 декабря на последующие годы. В плане проведения мониторинга определяются структурные подразделения Организации и сроки проведения мониторинга.

1. Внеплановые проверки проводятся по устному поручению Директора Организации (лица, исполняющего его обязанности) в течение пяти рабочих дней с даты поступления соответствующего поручения.
2. В ходе подготовки к проведению проверки Специалист определяет:

структурное подразделение (работника), деятельность которого подлежит проверке;

объекты контроля (процессы обработки персональных данных; информационные ресурсы и системы, содержащие персональные данные);

проверяемый период.

1. Проверка включает проведение мероприятий по:

* анализу полноты выполнения работниками требований законодательства о персональных данных и локальных правовых актов;
* анализу ведения работниками Организации реестра обработки персональных данных (далее - реестр), его своевременной актуализации;
* проверке соответствия сроков хранения персональных данных срокам, указанным в реестре согласно требованиям законодательства;
* анализу реализации порядка доступа в Организации к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе);
* проверке соблюдения сроков обучения работников Организации по вопросам защиты персональных данных;
* контролю знаний работников Организации законодательства о персональных данных и локальных правовых актов;
* иным вопросам, касающимся обработки персональных данных в Организации.

1. 8. Срок проверки не должен превышать пяти рабочих дней.

При необходимости и по устному распоряжению Директора Организации (лица, исполняющего его обязанности) срок проведения проверки может быть продлен.

1. Специалист не позднее чем за пять рабочих дней до начала проведения мониторинга уведомляет руководителя проверяемого структурного подразделения и представляет ему для ознакомления план проведения мониторинга.

При проведении внеплановой проверки уведомление руководителя проверяемого структурного подразделения об этом не производится и план проведения проверки не составляется.

10. Проверки проводятся Специалистом непосредственно на рабочем месте соответствующих работников, осуществляющих обработку персональных данных, в их присутствии.

При проведении проверки работник обязан предоставить Специалисту доступ к своей документации, рабочему месту, а также к служебному компьютеру и служебному смартфону.

В случае отсутствия работника в период проведения проверки (болезнь, отпуск, командировка и т.п.) решение о переносе срока проведения проверки или проведении проверки в отсутствие такого работника принимается на основании устного поручения Директора Организации (лица, исполняющего его обязанности).

В случае проведения проверки в отсутствие работника, осмотр его документации, рабочего места, служебного компьютера и служебного смартфона осуществляется в присутствии его непосредственного руководителя (лица, исполняющего его обязанности).

1. Проверка может проводиться в удалённом формате с использованием доступа к корпоративным информационным системам, рабочему компьютеру сотрудника и необходимым документам, при условии идентификации проверяемого лица и соблюдения конфиденциальности.
2. Специалист при осуществлении проверки имеет право:
   1. рекомендовать руководителю структурного подразделения (работнику), деятельность которого проверяется:

принять меры по устранению выявленных недостатков обработки персональных данных исходя из требований законодательства о персональных данных и локальных правовых актов;

актуализировать реестр, в том числе привести его записи в соответствие фактически складывающимся действиям по обработке персональных данных.

* 1. вносить Директору Организации (лицу, исполняющему его обязанности) предложения, направленные на предупреждение нарушения законодательства о персональных данных и локальных правовых актов, в том числе:
* о совершенствовании правового, организационного и технического обеспечения защиты персональных данных при их обработке Организации;
* поручении руководителям соответствующих структурных подразделений (работникам) актуализировать реестр;
* привлечении к дисциплинарной ответственности работников, нарушивших законодательство о персональных данных или локальные правовые акты.

**Не допускается вмешательство в деятельность Специалиста при осуществлении контроля**.

1. По итогам проведения проверки Специалистом в течение пять рабочих дней после ее завершения готовится отчет по форме согласно приложению 2, в котором указываются:

* сроки проведения проверки, форма проведения проверки (мониторинг, внеплановая проверка), наименование структурного подразделения (работника), деятельность которого проверена;
* проведенные мероприятия;
* выявленные недостатки (при их наличии);
* предложения по совершенствованию обработки персональных данных и сроки устранения выявленных недостатков (при их наличии).

По истечении сроков устранения выявленных недостатков Специалист проводит повторную проверку (при необходимости).

Отчет представляется Директору Организации (лицу, исполняющему его обязанности).

Отчеты хранятся у Специалиста до полного устранения недостатков, но не более трех лет.

1. Специалист ежегодно не позднее 31 января представляет Директору Организации сводный отчет о проведении проверок за предыдущий год.

 

|  |  |
| --- | --- |
|  | Приложение 1  к Положению о порядке  осуществления внутреннего  контроля за обработкой  персональных данных |

Форма

|  |  |  |
| --- | --- | --- |
|  | УТВЕРЖДАЮ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
|  | (наименование должности) | |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | (подпись) | (И.О.Фамилия) |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  | (дата) |  |

ПЛАН

проведения мониторинга

обработки персональных данных

на \_\_\_\_\_\_ год

|  |  |  |
| --- | --- | --- |
| Структурное подразделение (лицо) | Объект контроля | Проверяемый период |
|  |  |  |

|  |  |
| --- | --- |
|  | Приложение 2  к Положению о порядке  осуществления внутреннего  контроля за обработкой  персональных данных |

ОТЧЕТ N \_\_\_\_

о проведении проверки

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Настоящий отчет составлен о том, что в период с \_\_\_\_\_\_\_\_ по \_\_\_\_\_\_\_ | | | | |
|  | | | (дата) | (дата) |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | |
| (должность, Ф.И.О. работника, проводившего проверку) | | | | |
| проведена проверка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. | | | | |
|  | (форма проверки) | (наименование структурного подразделения) | | |

В ходе проверки осуществлены следующие мероприятия:

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

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

Выявленные недостатки и срок их устранения (при наличии):

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

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

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

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

Предложения по совершенствованию обработки персональных данных:

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

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

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

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

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

|  |  |  |
| --- | --- | --- |
| Специалист по внутреннему контрою за обработкой персональных данных | \_\_\_\_\_\_\_\_\_\_  (подпись) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (И.О.Фамилия) |

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

(дата)