ПРИЛОЖЕНИЕ № 3

УТВЕРЖДЕНЫ

распоряжением администрации Новоминского сельского поселения Каневского района

от 01.12.2020 № 67-р

Правила

осуществления внутреннего контроля соответствия

обработки персональных данных требованиям к защите персональных данных в администрации Новоминского сельского поселения Каневского района

# Общие положения

* 1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Новоминского сельского поселения Каневского района (далее – Администрация) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным законодательством Российской Федерации и принятыми в соответствии с ним нормативными правовыми актами.
  2. Настоящие Правила разработаны в соответствии с:

Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке информационных системах персональных данных».

* 1. Настоящими Правилами в своей работе должны руководствоваться сотрудники Администрации, осуществляющие внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных.

# Структура процессов по внутреннему контролю

* 1. Контроль выполнения требований по защите персональных данных в структурных подразделениях Администрации осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработки мер по их устранению и недопущению в дальнейшем.
  2. Контроль выполнения требований по защите персональных данных в структурных подразделениях Администрации осуществляет ответственный за организацию обработки персональных данных в Администрации.
  3. Общий контроль выполнения требований по обеспечению безопасности персональных данных осуществляет ответственный за выполнение мероприятий по контролю исполнения в структурных подразделениях Администрации требований документов по обеспечению безопасности персональных данных.
  4. Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.
  5. Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.
  6. Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов персональных данных или нарушения требований по защите персональных данных.
  7. Сроки проведения контрольных проверок доводятся главой Администрации не позднее, чем за 24 часа до начала проверки.
  8. Проверки по частным вопросам могут проводиться без уведомления.
  9. Периодичность и сроки проведения плановых проверок устанавливаются планом проверок на календарный год. Сроки проведения плановых проверок доводятся главой Администрации, не менее чем за 10 суток до начала проверки.

# Порядок подготовки к проверке

* 1. Общий контроль выполнения требований по обеспечению безопасности персональных данных в Администрации осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных Администрации (форма представлена в приложении № 1), утвержденным главой Администрации.
  2. Ответственный за выполнение мероприятий по контролю исполнения требований документов по обеспечению безопасности персональных данных подготавливает предложения по составу комиссии или группы проверяющих лиц.
  3. Контроль в Администрации, осуществляемый ответственными за обеспечение контроля процессов обеспечения безопасности персональных данных, осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных (форма представлена в приложении № 2). Данные Планы утверждаются главой Администрации и согласовываются с ответственным за выполнение мероприятий по контролю исполнения требований документов по обеспечению безопасности персональных данных.
  4. Проверяющие лица обязаны получить у проверяемых структурных подразделений Администрации информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения Администрации.

# Порядок проведения проверки

* 1. Проверяемое подразделения Администрации обязано оказывать содействие комиссии по проверке или группе проверяющих лиц и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.
  2. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям должен исключать ознакомление проверяющих лиц с конкретными персональными данными.
  3. Должны быть согласованы конкретные вопросы по объему, содержанию, срокам проведения проверки, а также каких сотрудников подразделений необходимо привлечь к проверке и какие помещения следует посетить.
  4. Общий порядок проведения проверки включает:

выявление сотрудников, задействованных в обработке персональных данных;

проверка факта ознакомления сотрудников проверяемого подразделения Администрации с нормативными документами, регламентирующими вопросы обработки и защиты персональных данных;

получение при содействии сотрудников проверяемого подразделения документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;

анализ полученной документации;

непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

* 1. В ходе осуществления контроля выполнения требований по защите персональных данных в подразделении рассматриваются следующие показатели работ по защите персональных данных:

наличие согласий на обработку персональных данных субъектов персональных данных, в случаях, предусмотренных законодательствам Российской Федерации;

соответствие состава и сроков обработки целям обработки ПДн;

соответствие Перечня лиц, имеющих доступ в помещения, в которых ведется обработка персональных данных реальному составу сотрудников;

наличие нормативных документов по защите персональных данных;

знание нормативных документов и уровень подготовки сотрудников, имеющих доступ к персональным данным;

полнота и правильность выполнения требований нормативных документов сотрудниками, имеющими доступ к персональным данным;

наличие документов, подтверждающих учет и сохранность материальных носителей персональных данных;

* 1. В ходе осуществления контроля выполнения требований по защите персональных данных в подразделении Администрации дополнительно рассматриваются следующие показатели работ по защите персональных данных:

соответствие информации, указанной в уведомлении об обработке персональных данных, реальному положению дел;

наличие и корректность перечня информационных систем;

наличие документа, подтверждающего:

правильность определения уровня защищенности персональных данных, обрабатываемых в информационных системах, а также классов защищенности информационных систем;

наличие документа, подтверждающего факт определения угроз безопасности персональных данных, а также его актуальность (срок актуальности документа не может превышать 3 года);

соответствие требованиям по организации разграничения доступа пользователей к информационным ресурсам (в том числе сетевым);

порядок защиты персональных данных при передаче по сети;

оценка эффективности принимаемых мер по обеспечению безопасности персональных данных.

* 1. Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.
  2. Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

# Оформление результатов проверки

* 1. Результаты проверки оформляются актом.
  2. Акт составляется в одном экземпляре и подписывается членами комиссии. Оригинал документа с результатами проверки хранится (передается) у ответственного за выполнение мероприятий по контролю исполнения подразделениями Администрации требований документов по обеспечению безопасности персональных данных.
  3. Результаты проверок подразделений периодически обобщаются ответственным за выполнение мероприятий по контролю исполнения подразделениями Администрации и доводятся до сведения ответственного за организацию обработки и обеспечение безопасности персональных данных Администрации.
  4. При необходимости принятия решений по результатам проверки структурного подразделения Администрации – ответственному за организацию обработки и обеспечение безопасности персональных данных Администрации готовится соответствующая служебная записка.

# Корректирующие мероприятия и контроль за их исполнением

* 1. Структурное подразделение Администрации анализирует акт о результатах внутренней проверки и в пятидневный срок определяет перечень мероприятий, необходимых для устранения нарушений и их причин.
  2. Перечень мероприятий согласуется с ответственным за организацию обработки и обеспечение безопасности персональных данных Администрации.
  3. Если корректирующие мероприятия касаются других структурных подразделений Администрации, то к анализу привлекаются специалисты соответствующих структурных подразделений.
  4. Выполнение корректирующих мероприятий и их достаточность определяется ответственным за организацию обработки и обеспечение безопасности персональных данных Администрации.
  5. Внутренняя проверка считается оконченной после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

Начальник общего отдела

администрации Новоминского сельского

поселения Каневского района Л.Е.Власенко

ПРИЛОЖЕНИЕ № 1

к Правилам

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

в администрации Новоминского сельского поселения Каневского района

**ПЛАН**

**проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных администрации Новоминского сельского поселения Каневского района**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование структурного подразделения | Наименование мероприятия | Период проведения проверки | Отметка о выполнении (№ акта проверки) | Отметка о выполнении корректирующих мероприятий | Примечание |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Глава администрации Новоминского сельского поселения Каневского района | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) | А.В. Плахутин |

ПРИЛОЖЕНИЕ № 2

к Правилам

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

в администрации Новоминского сельского поселения Каневского района

**ПЛАН**

**проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных структурных подразделений администрации Новоминского сельского поселения Каневского района**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование мероприятия | Период проведения проверки | Отметка о выполнении (№ акта проверки) | Отметка о выполнении корректирующих мероприятий | Примечание |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Глава администрации Новоминского сельского поселения Каневского района | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) | А.В. Плахутин |