



**АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
КОРЕНОВСКИЙ РАЙОН**

РАСПОРЯЖЕНИЕ

от 11.02.2020

№ 67-р

г. Кореновск

**Об утверждении правил
осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных в
администрации муниципального образования Кореновский район**

В целях исполнения требований Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

1. Утвердить правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования Кореновский район согласно приложению к настоящему распоряжению.

2. Заместителю главы муниципального образования Кореновский район Н.Г. Лысенко ознакомить сотрудников администрации муниципального образования Кореновский район, участвующих в обработке персональных данных субъектов администрации муниципального образования Кореновский район с настоящим распоряжением.

3. Признать утратившим силу распоряжение администрации муниципального образования Кореновский район от 07.05.2015 № 159-р «Об утверждении правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования Кореновский район».

4. Отделу по делам СМИ и информационному сопровождению администрации муниципального образования Кореновский район обеспечить размещение настоящего распоряжения на официальном сайте администрации муниципального образования Кореновский район в информационно-телекоммуникационной сети «Интернет».

5. Контроль за выполнением настоящего распоряжения возложить на заместителя главы муниципального образования Кореновский район Н.Г.Лысенко.

6. Распоряжение вступает в силу со дня его подписания.

Глава
муниципального образования
Кореновский район

С.А. Голобородько

ПРИЛОЖЕНИЕ

УТВЕРЖДЕНЫ

распоряжением администрации
муниципального образования

Кореновский район
от 11.02.2020 г. № 67-р

ПРАВИЛА

**осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных в
администрации муниципального образования Кореновский район**

1. Общие положения

Настоящие правила разработаны в соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и требованиями по соблюдению 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, утверждённых постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, и определяют порядок организации и осуществления контроля выполнения соответствия обработки персональных данных требованиям к защите персональных данных в отраслевых (функциональных) органах администрации муниципального образования Кореновский район (далее – Администрация).

Правила обязательны для исполнения всеми должностными лицами Администрации, осуществляющими контроль состояния защиты персональных данных.

Контроль выполнения соответствия обработки персональных данных требованиям к защите персональных данных в отраслевых (функциональных) органах Администрации осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, правильности обработки персональных данных ответственными лицами в этих органах, а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных Администрации. Для участия в проведении контроля решением ответственного за организацию обработки персональных данных могут также привлекаться другие специалисты отраслевых (функциональных) органов Администрации (по согласованию с их руководителями). В таких случаях контроль носит комплексный характер.

Контроль проводится в форме плановых и внеплановых проверок.

Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

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 или нарушения требований по обработке и защите персональных данных.

Сроки проведения контрольных проверок доводятся руководителям проверяемых отраслевых (функциональных) органов Администрации не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых отраслевых (функциональных) органов Администрации.

Периодичность и сроки проведения плановых проверок отраслевых (функциональных) органов Администрации устанавливаются планом, утверждаемым главой муниципального образования Кореновский район. Сроки проведения плановых проверок доводятся руководителям проверяемых отраслевых (функциональных) органов Администрации не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании приказа главы муниципального образования Кореновский район. Ответственный за организацию обработки персональных данных Администрации подготавливает предложения по составу комиссии или группы проверяющих лиц. Проект приказа о проверке подготавливает ответственный за организацию обработки персональных данных Администрации.

Проверяющие лица обязаны получить у руководителей проверяемых отраслевых (функциональных) органов Администрации информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного отраслевого (функционального) органа.

3. Порядок проведения проверки

По прибытию в отраслевой (функциональный) орган Администрации для проведения проверки председатель комиссии (старший по проверке) прибывает к руководителю проверяемого отраслевого (функционального) органа Администрации, представляется ему и представляет других прибывших на проверку лиц.

Руководитель проверяемого отраслевого (функционального) органа Администрации обязан оказывать содействие комиссии по проверке или группе проверяющих лиц и в случае необходимости определяет должностное лицо,

ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите персональных данных, выявление ответственных за обработку и защиту персональных данных и установление факта ознакомления сотрудников проверяемого отраслевого (функционального) органа Администрации со своей ответственностью;

2) получение при содействии сотрудников проверяемого отраслевого (функционального) органа Администрации документов, касающихся обработки и защиты персональных данных в данном органе;

3) анализ полученной документации;

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

При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проведения проверки, а также каких должностных лиц отраслевого (функционального) органа Администрации необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по обработке и защите персональных данных в проверяемом отраслевом (функциональном) органе Администрации рассматриваются в частности следующие показатели:

1) в части общей организации работ по обработке персональных данных:

а) соответствие информации, указанной в уведомлении об обработке персональных данных и в положении о порядке обработки персональных данных Администрации, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (персональных данных), их полнота, в соответствии с нормативными правовыми актами и локальными актами, принятыми в Администрации;

в) наличие нормативных документов по защите персональных данных;

г) знание нормативных документов сотрудниками (служащими), имеющими доступ к персональным данным;

д) полнота и правильность выполнения требований нормативных документов Администрации сотрудниками (служащими), имеющими доступ к персональным данным;

е) наличие документов, определяющих состав сотрудников, ответственных за организацию защиты персональных данных в отраслевом (функциональном) органе Администрации, соответствие этих документов реальному штатному составу отраслевого (функционального) органа Администрации, а также подтверждение факта ознакомления ответственных сотрудников с данными документами;

ж) уровень подготовки сотрудников, ответственных за организацию защиты персональных данных в подразделении;

з) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных.

2) в части защиты персональных данных в информационных системах персональных данных (далее - ИСПДн):

а) соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

б) структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных;

в) соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

г) наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах вычислительной техники;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль журналов учёта носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);

з) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к персональным данным;

б) правильность установления уровня защищенности персональных данных в информационной системе;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о отраслевых (функциональных) органах Администрации, должностных инструкциях сотрудников ;

г) порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих персональные данные;

ж) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

з) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

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.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

1) актом - при проведении проверки комиссией;

2) служебной запиской - при проведении проверки назначенными специалистами.

Акт и/или служебная записка составляется в двух экземплярах и подписывается членами комиссии или группой проверяющих лиц.

Один экземпляр хранится у ответственного за организацию обработки персональных данных Администрации. Второй экземпляр хранится в Администрации в установленном порядке. Копия акта о проверке остается в проверяемом отраслевом (функциональном) органе Администрации.

Результаты проверок отраслевых (функциональных) органов Администрации периодически обобщаются ответственным за организацию обработки персональных данных Администрации и доводятся до руководителей отраслевых (функциональных) органов Администрации. При необходимости принятия решений по результатам проверок отраслевых (функциональных) органов Администрации на имя главы муниципального образования Кореновский район готовятся соответствующие служебные записки.

Заместитель главы
муниципального образования
Кореновский район

Н.Г. Лысенко