Приложение 2

к приказу комитета

от 25.08.2021 №134

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в комитете по финансам, налоговой и кредитной политике города Барнаула

1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в комитете по финансам, налоговой и кредитной политике города Барнаула (далее – Правила) разработаны в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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», 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в комитете по финансам, налоговой и кредитной политике города Барнаула (далее – комитет).

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в комитете организовывается проведение внутренних плановых и внеплановых проверок условий обработки персональных данных на предмет соответствия Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам в сфере персональных данных (далее – проверки).

3. Проверки проводятся в комитете не реже одного раза в год на основании ежегодного плана внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных в комитете (далее – ежегодный план проверок), составляемого по форме согласно приложению 1 к Правилам, или на основании поступившего в комитет письменного обращения (заявления) о нарушениях правил обработки персональных данных (внеплановые проверки).

Ежегодный план проверок разрабатывается лицом, ответственным за организацию обработки персональных данных в комитете, и утверждается председателем комитета.

4. Проверки проводятся лицом, ответственным за организацию обработки персональных данных в комитете, непосредственно на месте обработки персональных данных путем опроса либо путем осмотра рабочих мест муниципальных служащих и лиц, не являющихся муниципальными служащими, комитета, осуществляющими обработку персональных данных (далее – операторы).

5. Основанием для проведения внеплановой проверки является поступившее в комитет письменное обращение (заявление) субъекта персональных данных или его представителя о нарушении правил обработки персональных данных.

6. Обращения (заявления), не позволяющие установить лицо, обратившееся в комитет, а также обращения (заявления), не содержащие сведений о фактах нарушения законодательства Российской Федерации в области персональных данных, не могут служить основанием для проведения внеплановой проверки.

7. Проведение внеплановой проверки организуется не позднее трех рабочих дней с даты поступления в комитет письменного обращения (заявления), указанного в пункте 5 Правил.

8. Срок проведения проверки не может превышать один месяц со дня принятия решения о ее проведении.

9. При проведении проверки лицо, ответственное за организацию обработки персональных данных в комитете, в пределах своей компетенции вправе:

запрашивать и получать от структурных подразделений комитета необходимые документы (сведения) для достижения целей проведения внутреннего контроля;

получать доступ к информационным системам персональных данных;

принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушениями требований законодательства Российской Федерации в области персональных данных;

требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

выдавать обязательные для исполнения оператором предписания об устранении выявленных нарушений в области персональных данных;

вносить на рассмотрение председателю комитета предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в области персональных данных, о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

осуществлять иные права, предусмотренные законодательством Российской Федерации и нормативными правовыми актами в сфере персональных данных.

10. При проведении проверки лицо, ответственное за организацию обработки персональных данных в комитете, не вправе:

требовать предоставления документов и информации, которые не относятся к предмету проверки;

нарушать режим конфиденциальности персональных данных субъектов персональных данных, раскрывать третьим лицам и распространять персональные данные без согласия субъекта персональных данных;

распространять информацию, полученную в результате проведения проверки и составляющую государственную, служебную, иную охраняемую законом тайну, за исключением случаев, предусмотренных законодательством Российской Федерации.

11. Оператор должен обеспечить необходимые условия для проведения проверки и обязан организовать доступ лицу, ответственному за организацию обработки персональных данных в комитете, к оборудованию, в помещения, где осуществляется обработка персональных данных, предоставить необходимую информацию и документацию для достижения целей проверки.

12. Оператор при проведении проверки имеет право непосредственно присутствовать при проведении проверки, давать объяснения по вопросам, относящимся к предмету проверки, знакомиться с результатами проверки.

13. По результатам проверки лицом, ответственным за организацию обработки персональных данных в комитете, в срок не позднее пяти рабочих дней с даты окончания проверки составляется [протокол](file:///C%3A%5CUsers%5Claw-oss%5CAppData%5CLocal%5CTemp%5Cprilozhenie-3-k-prikazu-_81.doc#Par283) проведения внутренней проверки соответствия обработки персональных данных требованиям к защите персональных данных в комитете (далее – протокол) по форме согласно приложению 2 к Правилам.

14. При выявлении по результатам проверки нарушений лицом, ответственным за организацию обработки персональных данных в комитете, в протоколе делается запись о необходимости проведения мероприятий по их устранению и сроках их устранения.

15. О результатах проверки и мерах, необходимых для устранения нарушений, лицо, ответственное за организацию обработки персональных данных в комитете, докладывает председателю комитета.

16. По существу вопросов, поставленных в обращении (заявлении), указанном в пункте 5 Правил, заявителю в срок не позднее 30 календарных дней со дня регистрации письменного обращения (заявления) направляется письменный ответ, который подлежит согласованию с председателем комитета и подписывается лицом, ответственным за организацию обработки персональных данных в комитете.

17. Информация о результатах проверок фиксируется лицом, ответственным за организацию обработки персональных данных в комитете, в Журнале учета внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных в комитете по форме согласно приложению 3 к Правилам.