

УТВЕРЖДЕНЫ
распоряжением
Уполномоченного по правам человека
в Новосибирской области
от 27.04.2015. № 23-р

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами государственного органа Новосибирской области Уполномоченный по правам человека в Новосибирской области и аппарат Уполномоченного по правам человека

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами государственного органа Новосибирской области Уполномоченный по правам человека в Новосибирской области и аппарат Уполномоченного по правам человека (далее – Правила) устанавливают порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном органе Новосибирской области Уполномоченный по правам человека в Новосибирской области и аппарат Уполномоченного по правам человека (далее – государственный орган).

2. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном органе осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон №152-ФЗ), постановлением Правительства Российской Федерации 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», настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом № 152-ФЗ.

4. Целью осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) является обеспечение защиты персональных данных от

несанкционированного доступа, неправомерного их использования или утраты, определение порядка и правил осуществления внутреннего контроля.

5. Внутренний контроль делится на текущий, плановый и внеплановый.

6. Текущий внутренний контроль осуществляется на постоянной основе ответственным за организацию обработки персональных данных в государственном органе (далее – ответственный за организацию обработки) в ходе мероприятий по обработке персональных данных.

Ответственный за организацию обработки имеет право:

- запрашивать у сотрудников государственного органа информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить Уполномоченному по правам человека в Новосибирской области предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить Уполномоченному по правам человека в Новосибирской области предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о персональных данных.

7. Плановый внутренний контроль осуществляется комиссией, образуемой распоряжением Уполномоченного по правам человека в Новосибирской области, в состав которой входят работники государственного органа, допущенные к обработке персональных данных.

Плановый внутренний контроль соответствия обработки персональных данных установленным требованиям в государственном органе проводится на основании утвержденного Уполномоченным по правам человека в Новосибирской области плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям, разрабатываемого председателем комиссии. Периодичность плановой проверки - не реже одного раза в год.

8. Внеплановый внутренний контроль может осуществляться на основании поступившего в государственный орган письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется председателем комиссии в течение 3 (трех) рабочих дней с момента поступления соответствующего заявления.

В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

9. При проведении внутреннего контроля ответственным за организацию обработки или комиссией должны быть полностью, объективно и всесторонне изучены:

- наличие, учет, порядок хранения и обезличивания персональных данных;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных;
- состояние учёта ПЭВМ и съемных носителей информации, содержащей персональные данные;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным;
- порядок проведения мероприятий и результаты по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- порядок проведения мероприятий по обеспечению целостности персональных данных.

10. В отношении персональных данных, ставших известными членам комиссии или ответственному за организацию обработки в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

11. Срок проведения плановой и внеплановой проверки не может составлять более 30 дней со дня принятия решения о её проведении.

12. Результаты внутреннего контроля оформляются в виде протокола проведения внутренней проверки (далее – протокол).

13. При выявлении в ходе внутреннего контроля нарушений ответственным за организацию обработки либо председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

14. Протоколы хранятся у ответственного за организацию обработки в течение текущего года. Уничтожение протоколов проводится ответственным за организацию обработки самостоятельно в январе года, следующего за проверочным годом.

15. О результатах внутреннего контроля и мерах, необходимых для устранения нарушений, Уполномоченному по правам человека в Новосибирской области докладывает ответственный за организацию обработки либо председатель комиссии.