Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от «__» _____ г. № _____

Об утверждении Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям законодательства Российской Федерации

в области персональных данных

В соответствии с пунктом 2 статьи 2 Федерального закона от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (Собрание законодательства Российской Федерации, 2008, № 52, ст. 6249; 2009, № 18, ст. 2140; № 29, ст. 3601; № 48, ст. 5711; № 52, ст. 6441; 2010, № 17, ст. 1988; № 18, ст. 2142; № 31, ст. 4160, 4193, 4196; № 32, ст. 4298; 2011, № 1, ст. 20; № 17, ст. 2310; № 23, ст. 3263; № 27, ст. 3880; № 30,
ст. 4590; № 48, ст. 6728) Правительство Российской Федерации п о с т а н о в л я е т :

Утвердить прилагаемое Положение о государственном контроле и надзоре за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

Председатель Правительства
Российской Федерации В. Путин

УТВЕРЖДЕН
постановлением Правительства
Российской Федерации
от «___»_____ № _____

Положение
о государственном контроле и надзоре
за соответствием обработки персональных данных
требованиям законодательства Российской Федерации
в области персональных данных

Настоящее Положение разработано на основании Федерального закона от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 20 августа 2009 г. № 689 «Об утверждении правил аккредитации граждан и организаций, привлекаемых органами государственного контроля (надзора) и органами муниципального контроля к проведению мероприятий по контролю» и устанавливает порядок осуществления государственного контроля и надзора за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

1. Государственный контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных на территории Российской Федерации и находящихся под юрисдикцией Российской Федерации территориях осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций непосредственно и через ее территориальные органы.

2. Государственный контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных включает в себя мониторинг

деятельности государственных органов, муниципальных органов, юридических лиц, индивидуальных предпринимателей и физических лиц, направленный на предупреждение, выявление и пресечение нарушений законодательства Российской Федерации в области персональных данных, а также контроль и надзор за соблюдением государственными органами, муниципальными органами, юридическими лицами, индивидуальными предпринимателями и физическими лицами обязательных требований, установленных федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации в области персональных данных, в том числе за выполнением организационных и технических мер по обеспечению безопасности персональных данных при обработке персональных данных в негосударственных информационных системах персональных данных (далее – обязательные требования в области персональных данных).

3. Государственный контроль и надзор за соблюдением обязательных требований в области персональных данных от имени Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций уполномочены осуществлять должностные лица - государственные инспекторы по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – должностные лица).

4. В целях осуществления государственного контроля и надзора за соблюдением обязательных требований в области персональных данных Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальные органы организуют и проводят плановые и внеплановые проверки.

5. Должностные лица Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций или ее территориальных органов при проведении проверки вправе:

5.1. запрашивать и получать на основании мотивированного письменного запроса от государственных органов, муниципальных органов, юридических лиц, индивидуальных предпринимателей и физических лиц информацию и документы, связанные с исполнением указанными органами и лицами обязательных требований в области персональных данных;

5.2. беспрепятственно по предъявлению служебного удостоверения и копии приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций или ее территориального органа о проведении проверки посещать и проводить обследования используемых государственными органами, муниципальными органами, юридическими лицами, индивидуальными предпринимателями и физическими лицами при осуществлении деятельности зданий, помещений, сооружений, негосударственных информационных систем персональных данных, технических средств,

оборудования, документов, а также проводить необходимые исследования, испытания, расследования, экспертизы и другие мероприятия по контролю;

5.3. выдавать обязательные для выполнения предписания об устранении выявленных нарушений в области персональных данных;

5.4. использовать технику и оборудование, принадлежащие Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций или ее территориальному органу;

5.5. получать доступ к государственным информационным системам персональных данных в режиме просмотра и выборки необходимой информации;

5.6. получать доступ и проверять выполнение организационных и технических мер по обеспечению безопасности персональных данных при обработке персональных данных в негосударственных информационных системах персональных данных;

5.7. составлять протоколы об административном правонарушении или направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении дел об административных правонарушениях;

5.8. направлять в органы прокуратуры, другие правоохранительные органы по подведомственности материалы для решения вопросов о возбуждении уголовных дел по признакам преступлений, связанных с нарушением обязательных требований в области персональных данных;

5.9. в рамках международного сотрудничества с уполномоченными органами по защите прав субъектов персональных данных иностранных государств оказывать правовую и организационную помощь по предотвращению, пресечению и прекращению незаконной деятельности в области персональных данных;

5.10. принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушениями обязательных требований в области персональных данных;

5.11. требовать от государственных органов, муниципальных органов, юридических лиц, индивидуальных предпринимателей и физических лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

6. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальные органы при осуществлении мероприятий по контролю в части выполнения юридическими лицами, индивидуальными предпринимателями и физическими лицами организационных и технических мер по обеспечению безопасности персональных данных при обработке персональных данных в негосударственных информационных системах персональных данных привлекают экспертов, экспертные организации,

аккредитованных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций в порядке, определенном постановлением Правительства Российской Федерации от 20 августа 2009 г. № 689 «Об утверждении правил аккредитации граждан и организаций, привлекаемых органами государственного контроля (надзора) и органами муниципального контроля к проведению мероприятий по контролю».

7. Плановые и внеплановые проверки проводятся должностными лицами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами в форме документарной или выездной проверки.

8. Запросы в адрес государственных органов, муниципальных органов, юридических лиц, индивидуальных предпринимателей и физических лиц о получении информации по существу вопросов, указанных в обращении, поступившем в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальный орган, направленные в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» не являются документарной проверкой.

9. Плановые проверки проводятся на основании ежегодного плана проведения плановых проверок, утверждаемого руководителем Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций на текущий календарный год.

Порядок подготовки ежегодного плана проведения плановых проверок, его представления в органы прокуратуры и согласования, а также типовая форма ежегодного плана проведения плановых проверок установлены постановлением Правительства Российской Федерации от 30 июня 2010 г. № 489 «Об утверждении Правил подготовки органами государственного контроля (надзора) и органами муниципального контроля ежегодных планов проведения плановых проверок юридических лиц и индивидуальных предпринимателей».

10. Плановые проверки проводятся в отношении государственных органов, муниципальных органов, юридических лиц, индивидуальных предпринимателей и физических лиц, организующих и (или) осуществляющих обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

11. Основанием для включения плановой проверки в План является:

11.1. начало осуществления государственным органом, муниципальным органом и физическим лицом деятельности по обработке персональных данных;

11.2. истечение трех лет со дня:

11.2.1. государственной регистрации юридического лица, индивидуального предпринимателя в качестве таковых;

11.2.2. окончания проведения последней плановой проверки юридического лица, индивидуального предпринимателя.

12. Внеплановые проверки проводятся по следующим основаниям:

12.1. истечение срока исполнения государственным органом, муниципальным органом, юридическим лицом, индивидуальным предпринимателем и физическим лицом выданного Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций предписания об устранении выявленного нарушения обязательных требований в области персональных данных;

12.2. поступление в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций или ее территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления и средств массовой информации о фактах:

12.2.1. возникновения угрозы причинения вреда жизни, здоровью граждан;

12.2.2. причинения вреда жизни, здоровью граждан;

12.3. приказ руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций или ее территориального органа, изданный в соответствии с поручениями Президента Российской Федерации, Правительства Российской Федерации;

12.4. нарушение прав и законных интересов граждан действиями (бездействием) государственных органов, муниципальных органов, юридических лиц, индивидуальных предпринимателей и физических лиц при обработке их персональных данных;

12.5. нарушение государственным органом, муниципальным органом, юридическим лицом, индивидуальным предпринимателем и физическим лицом обязательных требований в области персональных данных, а также несоответствие сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности.

13. Проведение внеплановых проверок по основаниям, предусмотренным подпунктом 12.2. пункта 12 настоящего Положения, требует согласования с органами прокуратуры.

14. Срок проведения как плановой, так и внеплановой проверки не может превышать двадцать рабочих дней.

В исключительных случаях, связанных с необходимостью проведения сложных и (или) длительных исследований, испытаний, специальных экспертиз и расследований на основании мотивированных предложений должностных лиц Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций

или ее территориальных органов, проводящих проверку, срок проведения каждой из проверок может быть продлен руководителем Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций или руководителем ее территориального органа, но не более чем на двадцать рабочих дней.

15. При проведении проверок в отношении государственных органов, муниципальных органов, юридических лиц, которые осуществляют свою деятельность на территориях нескольких субъектов Российской Федерации, срок проведения каждой из проверок устанавливается отдельно по каждому филиалу, представительству, обособленному структурному подразделению, при этом общий срок проведения проверки не может превышать шестьдесят рабочих дней.

16. Порядок проведения и оформление результатов проводимых проверок осуществляется в соответствии с положениями Федерального закона от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

17. В приказе о проведении проверки и акте проверки в обязательном порядке подлежат указанию фамилия, имя, отчество эксперта и (или) наименование экспертной организации, привлекаемые Федеральной службой по надзору в сфере связи, информационным технологиям и массовым коммуникациям или ее территориальными органами к проведению мероприятий по контролю при осуществлении проверки.

18. Форма проведения проверки определяется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций или ее территориальным органом самостоятельно, с учетом оснований, предусмотренных пунктами 11 и 12 Положения.

19. В ходе проведения проверки Федеральная служба по надзору в сфере связи, информационным технологиям и массовым коммуникациям или ее территориальные органы осуществляют следующие мероприятия по контролю:

19.1. рассмотрение документов государственных органов, муниципальных органов, юридических лиц, индивидуальных предпринимателей и физических лиц, в том числе:

19.1.1. уведомлений об обработке персональных данных;

19.1.2. документов, необходимых для проверки фактов, содержащих признаки нарушения законодательства Российской Федерации в области персональных данных, изложенных в обращениях граждан и информации, поступившей в Федеральную службу по надзору в сфере связи,

информационным технологиям и массовым коммуникациям или ее территориальный орган;

19.1.3. документов, подтверждающих выполнение государственным органом, муниципальным органом, юридическим лицом, индивидуальным предпринимателем и физическим лицом предписания об устранении ранее выявленных нарушений законодательства Российской Федерации в области персональных данных;

19.1.4. документов, подтверждающих наличие в установленных законодательством Российской Федерации в области персональных данных случаях согласия субъекта персональных данных на обработку его персональных данных в письменной или иной форме;

19.1.5. документов, подтверждающих соблюдение обязательных требований в области персональных данных при обработке специальных категорий и биометрических персональных данных;

19.1.6. документов, подтверждающих уничтожение государственным органом, муниципальным органом, юридическим лицом, индивидуальным предпринимателем и физическим лицом персональных данных субъектов персональных данных по достижении цели обработки;

19.1.7. локальных актов, определяющих политику государственных органов, муниципальных органов, юридических лиц, индивидуальных предпринимателей и физических лиц в отношении обработки персональных данных, по вопросам обработки персональных данных, а также устанавливающих процедуры, направленные на предотвращение и выявление нарушений обязательных требований в области персональных данных, устранение последствий таких нарушений;

19.2. исследование (обследование) государственной и негосударственной информационной системы персональных данных, в части касающейся проверки соблюдения установленного порядка и условий обработки персональных данных;

19.3. исследование (обследование) негосударственной информационной системы персональных данных, в том числе по вопросам применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в указанных информационных системах персональных данных, необходимых для выполнения обязательных требований к защите персональных данных;

19.4. оценка соответствия действий государственных органов, муниципальных органов, юридических лиц, индивидуальных предпринимателей и физических лиц по обезличиваю и деобезличиванию персональных данных требованиям и методам, установленным Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций;

19.5. оценка достаточности принимаемых государственным органом, муниципальным органом мер, направленных на обеспечение выполнение обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

20. При осуществлении мероприятий по контролю в рамках проведения проверки с привлечением экспертов и (или) экспертных организаций должностными лицами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами также осуществляется:

20.1. обследование и определение уровня защищенности информационных систем персональных данных, используемых юридическими лицами, индивидуальными предпринимателями и физическими лицами при осуществлении своей непосредственной деятельности;

20.2. оценка соответствия применяемых юридическими лицами, индивидуальными предпринимателями и физическими лицами технических средств защиты информации;

20.3. оценка достаточности и эффективности принимаемых юридическими лицами, индивидуальными предпринимателями и физическими лицами технических мер по обеспечению безопасности персональных данных при их обработке в негосударственных информационных системах персональных данных;

20.4. проведение исследований, а также проведение экспертиз, направленных на установление причинно-следственной связи выявленного нарушения обязательных требований в области персональных данных.

21. В случае выявления в ходе или по результатам проверки административного правонарушения, предусмотренного Кодексом Российской Федерации об административных правонарушениях, в том числе невыполнения в установленный срок ранее выданного предписания об устранении выявленного нарушения обязательных требований в области персональных данных, должностные лица Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций или ее территориального органа составляют протокол об административном правонарушении в порядке, установленном законодательством Российской Федерации или направляют материалы в органы прокуратуры, другие правоохранительные органы для разрешения вопроса о возбуждении дела об административном правонарушении, а также о возбуждении уголовного дела, при наличии оснований для возбуждения уголовных дел по признакам преступлений, выявленных в ходе проверки и связанных с нарушением обязательных требований в области персональных данных, в соответствии с подведомственностью.