**[Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) "О персональных данных"](http://www.consultant.ru/document/cons_doc_LAW_61801/)**

**Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом**

(введена Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_117437/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100156) от 25.07.2011 N 261-ФЗ)

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, [документов](http://www.consultant.ru/document/cons_doc_LAW_155347/), определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со [статьей 19](http://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/#dst100368) настоящего Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Правительство Российской Федерации устанавливает [перечень](http://www.consultant.ru/document/cons_doc_LAW_127610/6c269d7e8fda206ad95dc5a6ea1655abfd4ad4e0/#dst100008) мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

4. Оператор обязан представить документы и локальные акты, указанные в [части 1](http://www.consultant.ru/document/cons_doc_LAW_61801/eeeebe22bf738fd65bb66b95cc278911ae2525ee/#dst100358) настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в [части 1](http://www.consultant.ru/document/cons_doc_LAW_61801/eeeebe22bf738fd65bb66b95cc278911ae2525ee/#dst100358) настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.

**Статья 19. Меры по обеспечению безопасности персональных данных при их обработке**

(в ред. Федерального [закона](http://www.consultant.ru/document/cons_doc_LAW_117437/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100168) от 25.07.2011 N 261-ФЗ)

(см. текст в предыдущей редакции)

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) [уровни защищенности](http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100025) персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) [требования](http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100009) к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) [требования](http://www.consultant.ru/document/cons_doc_LAW_78154/784a455903b8b06cb18b66f1aafa873f6ceaa55f/#dst100009) к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с [частью 3](http://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/#dst100380) настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным [органом](http://www.consultant.ru/document/cons_doc_LAW_43763/95a81cd3278196d426c4241b8dd29a0497706514/#dst100213) исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным [органом](http://www.consultant.ru/document/cons_doc_LAW_14031/9b13a25cec35f1d26a1331611204f68c696b5c53/#dst100045) исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

КонсультантПлюс: примечание.

По вопросу разработки нормативных правовых актов, определяющих угрозы безопасности персональных данных, см. [Методические рекомендации](http://www.consultant.ru/document/cons_doc_LAW_185051/), утв. ФСБ России 31.03.2015 N 149/7/2/6-432.

5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с [частью 5](http://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/#dst100385) настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

7. Проекты нормативных правовых актов, указанных в [части 5](http://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/#dst100385) настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в [части 6](http://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/#dst100386) настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в [порядке](http://www.consultant.ru/document/cons_doc_LAW_135466/29f5bea427f84942a85c11f9d485673b895b99fc/#dst100009), установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в [части 6](http://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/#dst100386) настоящей статьи, должно быть мотивированным.

8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным [органом](http://www.consultant.ru/document/cons_doc_LAW_43763/95a81cd3278196d426c4241b8dd29a0497706514/#dst100213) исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным [органом](http://www.consultant.ru/document/cons_doc_LAW_14031/9b13a25cec35f1d26a1331611204f68c696b5c53/#dst100045) исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9. Федеральный [орган](http://www.consultant.ru/document/cons_doc_LAW_43763/95a81cd3278196d426c4241b8dd29a0497706514/#dst100213) исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный [орган](http://www.consultant.ru/document/cons_doc_LAW_14031/9b13a25cec35f1d26a1331611204f68c696b5c53/#dst100047) исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

#  ПЕРЕЧЕНЬ

**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**

1. Операторы, являющиеся государственными или муниципальными органами, принимают следующие меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_61801/) "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами:

а) назначают ответственного за организацию обработки персональных данных в государственном или муниципальном органе из числа государственных или муниципальных служащих (далее - служащие) данного органа;

(в ред. [Постановления](http://www.consultant.ru/document/cons_doc_LAW_149732/#dst100006) Правительства РФ от 20.07.2013 N 607)

(см. текст в предыдущей редакции)

б) утверждают актом руководителя государственного или муниципального органа следующие документы:

- правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;

- правила рассмотрения запросов субъектов персональных данных или их представителей;

- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/#dst100368) "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;

- [правила](http://www.consultant.ru/document/cons_doc_LAW_187282/1ed9baa4f06ed93a831b4094cd9408e5e22b60bc/#dst100010) работы с обезличенными данными в случае обезличивания персональных данных;

(в ред. [Постановления](http://www.consultant.ru/document/cons_doc_LAW_168403/#dst100007) Правительства РФ от 06.09.2014 N 911)

(см. текст в предыдущей редакции)

- перечень информационных систем персональных данных;

- перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

(в ред. [Постановления](http://www.consultant.ru/document/cons_doc_LAW_149732/#dst100008) Правительства РФ от 20.07.2013 N 607)

(см. текст в предыдущей редакции)

- перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных;

(в ред. [Постановления](http://www.consultant.ru/document/cons_doc_LAW_168403/#dst100008) Правительства РФ от 06.09.2014 N 911)

(см. текст в предыдущей редакции)

- перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

- должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных в государственном или муниципальном органе;

(в ред. [Постановления](http://www.consultant.ru/document/cons_doc_LAW_149732/#dst100009) Правительства РФ от 20.07.2013 N 607)

(см. текст в предыдущей редакции)

- типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

(в ред. [Постановления](http://www.consultant.ru/document/cons_doc_LAW_149732/#dst100010) Правительства РФ от 20.07.2013 N 607)

(см. текст в предыдущей редакции)

- типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

-

порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных;

в) при эксплуатации информационных систем персональных данных в случае, если государственный или муниципальный орган является оператором таких информационных систем, принимают правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные соответствующими нормативными правовыми актами, для выполнения установленных Правительством Российской Федерации [требований](http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100009) к защите персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

г) при обработке персональных данных, осуществляемой без использования средств автоматизации, выполняют требования, установленные [постановлением](http://www.consultant.ru/document/cons_doc_LAW_80028/) Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

д) в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуют проведение периодических проверок условий обработки персональных данных в государственном или муниципальном органе. Проверки осуществляются ответственным за организацию обработки персональных данных в государственном или муниципальном органе либо комиссией, образуемой руководителем государственного или муниципального органа. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю государственного или муниципального органа докладывает ответственный за организацию обработки персональных данных в государственном или муниципальном органе либо председатель комиссии;

е) осуществляют ознакомление служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных служащих;

ж) уведомляют уполномоченный орган по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных, за исключением случаев, установленных Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_61801/d996966e22e1320c9de1ab82d9f6be12c3d9d765/#dst100163) "О персональных данных";

з) в случаях, установленных нормативными правовыми актами Российской Федерации, в соответствии с [требованиями и методами](http://www.consultant.ru/document/cons_doc_LAW_151882/4152ee35eceba228c154ad318d27a70941c2371e/#dst100011), установленными уполномоченным органом по защите прав субъектов персональных данных, осуществляют обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

(пп. "з" в ред. [Постановления](http://www.consultant.ru/document/cons_doc_LAW_168403/#dst100009) Правительства РФ от 06.09.2014 N 911)

(см. текст в предыдущей редакции)

2. Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.