ПРИКАЗ

МИНИСТРА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

№ 1500

«16» июня 2012 г. г. Москва

Об утверждении Положения об обработке персональных данных в центральном аппарате Министерства обороны Российской Федерации

1. Утвердить прилагаемое Положение об обработке персональных данных в центральном аппарате Министерства обороны Российской Федерации.

2. Возложить функцию по обеспечению безопасности персональных данных при их обработке в информационных системах Министерства обороны Российской Федерации на Восьмое управление Генерального штаба Вооруженных Сил Российской Федерации.

3. Руководителям центральных органов военного управления:

обеспечить доработку должностных регламентов (должностных обязанностей) лиц, уполномоченных на обработку персональных данных, в части закрепления ответственности, предусмотренной законодательством Российской Федерации за нарушение режима конфиденциальности, а также обеспечения безопасности обрабатываемых ими персональных данных;

определить места хранения персональных данных;

до 1 октября 2012 г. осуществить классификацию эксплуатируемых информационных систем персональных данных.

4. Контроль за выполнением настоящего приказа возложить на начальника Генерального штаба Вооруженных Сил Российской Федерации – первого заместителя Министра обороны Российской Федерации.

МИНИСТР ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

А.Сердюков

Верно:

ЗАМЕТИТЕЛЬ НАЧАЛЬНИКА УПРАВЛЕНИЯ ДЕЛАМИ
МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

“18” июня 2012 г.

С.Королев

Приложение
к приказу Министра обороны
Российской Федерации
от «16» июня 2012 г. № 1500

ПОЛОЖЕНИЕ
об обработке персональных данных в центральном аппарате Министерства обороны Российской Федерации

I. Общие положения

1. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» (Собрание законодательства Российской Федерации, 2004, № 31, ст. 3215; 2006, № 6, ст. 636; 2007, № 10, ст. 1151; № 16, ст. 1828; № 49, ст. 6070; 2008, № 13, ст. 1186; № 30 (ч. II), ст. 3616; № 52 (ч. I), ст. 6235; 2009, № 29, ст. 3597, 3624; № 48, ст. 5719; № 51, ст. 6150, 6159; 2010, № 5, ст. 459; № 7, ст. 704; № 49, ст. 6413; № 51 (ч. III), ст. 6810; 2011, № 1, ст. 31; № 27, ст. 3866; № 29, ст. 4295; № 48, ст. 6730; № 50, ст. 7337) (далее – Федеральный закон «О государственной гражданской службе Российской Федерации»), частью 2 статьи 4 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31 (ч. I), ст. 3451; 2009, № 48, ст. 5716; № 52 (ч. I), ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, 4196; № 49, ст. 6409; 2011, № 23, ст. 3263; № 31, ст. 4701) (далее – Федеральный закон «О персональных данных»), Указом Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» (Собрание законодательства Российской Федерации, 2005, № 23, ст. 2242; 2008, № 43, ст. 4921), постановлением 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» (Собрание

законодательства Российской Федерации, 2007, № 48 (ч. II), ст. 6001), постановлением Правительства Российской Федерации 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» (Собрание законодательства Российской Федерации, 2008, № 28, ст. 3384), постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (Собрание законодательства Российской Федерации, 2008, № 38, ст. 4320) и определяет правила и условия обработки персональных данных военнослужащих и федеральных государственных гражданских служащих Вооруженных Сил Российской Федерации, проходящих службу в центральном аппарате Министерства обороны Российской Федерации (далее – военнослужащие и гражданские служащие), и кандидатов на замещение вакантных должностей федеральной государственной гражданской службы Министерства обороны (далее – иные лица) в центральном аппарате Министерства обороны (далее – субъекты персональных данных).

2. Министерство обороны является оператором, самостоятельно или совместно с другими лицами организующим и (или) осуществляющим обработку персональных данных субъектов персональных данных (далее – персональные данные), а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

3. Обработка персональных данных в центральном аппарате Министерства обороны осуществляется в целях исполнения функций в области обороны, а также ведения кадровой работы (ведение и хранение личных дел, учетных карточек и трудовых книжек гражданских служащих, содействие в трудоустройстве, обучении и должностном росте, обеспечение личной безопасности военнослужащего (гражданского служащего) и членов его семьи,

учет результатов исполнения им должностных обязанностей, обеспечение сохранности имущества Министерства обороны, а также документов иных лиц.

II. Правила обработки персональных данных

4. Обработка персональных данных осуществляется с письменного согласия субъектов персональных данных, которое действует со дня их поступления на службу и на время ее прохождения, как с использованием средств автоматизации, так и без использования таких средств.

5. Представитель нанимателя в лице Министра обороны Российской Федерации (статс-секретаря – заместителя Министра обороны Российской Федерации), осуществляющего полномочия нанимателя от имени Российской Федерации, а также начальник Главного управления кадров Министерства обороны Российской Федерации обеспечивают защиту персональных данных, содержащихся в личных делах субъектов персональных данных, от неправомерного их использования или утраты.

6. Персональные данные и иные сведения, содержащиеся в личных делах субъектов персональных данных, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации), а в случаях, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации, – к сведениям, составляющим государственную тайну.

7. При обработке персональных данных в целях реализации возложенных на Министерство обороны полномочий лица, уполномоченные на обработку персональных данных (далее – уполномоченные должностные лица), обязаны соблюдать следующие требования:

а) объем и характер обрабатываемых персональных данных, способы обработки персональных данных должны соответствовать целям обработки персональных данных;

б) защита персональных данных от неправомерного их использования или уничтожения обеспечивается в порядке, установленном нормативными правовыми актами Российской Федерации;

в) передача персональных данных не допускается без письменного согласия субъекта персональных данных, за

исключением случаев, установленных федеральными законами. В случае если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение персональных данных либо отсутствует письменное согласие субъекта персональных данных на передачу его персональных данных, Министерство обороны вправе отказать в предоставлении персональных данных. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации;

г) обеспечение конфиденциальности персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

д) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Указанные сведения подлежат уничтожению по достижении цели обработки или в случае утраты необходимости в их достижении, если иное не установлено законодательством Российской Федерации. Факт уничтожения персональных данных оформляется актом;

е) опубликование и распространение персональных данных допускается в случаях, установленных законодательством Российской Федерации.

8. Обработка биометрических и специальных категорий персональных данных осуществляется с письменного согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации в области персональных данных. Использование и хранение биометрических и специальных категорий персональных данных вне информационных систем персональных данных может 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, уничтожения, изменения, блокирования, копирования, распространения.

9. В целях обеспечения защиты персональных данных субъекты персональных данных вправе:

а) получать полную информацию о своих персональных данных и способе обработки этих данных (в том числе автоматизированной);

б) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, за исключением случаев, предусмотренных Федеральным законом «О персональных данных»;

в) требовать внесения необходимых изменений, уничтожения или блокирования персональных данных, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

г) обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействие) уполномоченных должностных лиц.

10. Министерство обороны в соответствии с Федеральным законом «О государственной гражданской службе Российской Федерации» вправе осуществлять обработку (в том числе автоматизированную) персональных данных гражданских служащих при формировании кадрового резерва.

11. Трансграничная передача персональных данных на территории иностранных государств осуществляется в соответствии со статьей 12 Федерального закона «О персональных данных» и Указом Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (Собрание законодательства Российской Федерации, 2008, № 12, ст. 1110; № 43, ст. 4919; 2011, № 4, ст. 572).

12. Министерство обороны в соответствии с Федеральным законом «О государственной гражданской службе Российской Федерации» и Положением о конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации, утвержденным Указом Президента Российской Федерации от 1 февраля 2005 г. № 112 (Собрание законодательства Российской Федерации, 2005, № 6, ст. 439; 2011, № 4, ст. 578) вправе осуществлять обработку (в том числе автоматизированную) персональных данных иных лиц.

13. При переводе или назначении гражданского служащего на должность федеральной государственной гражданской службы в другом государственном (муниципальном) органе его личное дело передается в государственный (муниципальный) орган по новому

месту замещения должности гражданской службы по письменному запросу соответствующего органа.

III. Правила обработки персональных данных, осуществляемой без использования средств автоматизации

14. Обработка персональных данных без использования средств автоматизации осуществляется как на бумажных носителях, так и в электронном виде на материальных носителях информации.

15. Неавтоматизированная обработка персональных данных в электронном виде должна осуществляться на съемных материальных носителях информации.

16. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на съемных материальных носителях информации необходимо принимать организационные (охрана помещений) и технические (установка сертифицированных средств защиты информации) меры, исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

17. Учет материальных носителей информации, содержащих персональные данные, осуществляется служебным делопроизводством. Допускается ведение журналов учета в электронном виде.

18. При обработке персональных данных без использования средств автоматизации уполномоченными должностными лицами не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

19. Обработка персональных данных на бумажных носителях осуществляется в соответствии с правовыми актами Министерства обороны по делопроизводству.

20. При разработке и использовании типовых форм документов, необходимых для реализации возложенных на Министерство обороны полномочий, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, адрес Министерства

обороны, фамилию, имя, отчество и адрес субъекта персональных данных, чьи персональные данные вносятся в указанную типовую форму, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи персональные данные содержатся в типовой форме, при ознакомлении со своими персональными данными не имел возможности доступа к персональным данным других лиц, содержащихся в указанной типовой форме;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

21. Уничтожение или обезличивание персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

22. Уточнение персональных данных при их обработке без использования средств автоматизации производится путем изготовления нового материального носителя с уточненными персональными данными.

IV. Правила обработки персональных данных в информационных системах персональных данных

23. Обработка персональных данных в информационных системах персональных данных осуществляется после завершения работ по созданию системы защиты персональных данных в информационной системе, проверки ее комиссией, назначаемой приказом органа военного управления, и оценки соответствия информационной системы персональных данных требованиям безопасности информации.

24. Безопасность персональных данных при их обработке в информационных системах Министерства обороны обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

25. Выбор методов и способов защиты информации в информационных системах персональных данных осуществляется в соответствии с Положением о методах и способах защиты информации в информационных системах персональных данных, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. № 58* на основе угроз безопасности персональных данных (модели угроз) в зависимости от класса информационной системы персональных данных.

Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781.

26. Класс информационной системы персональных данных определяется в соответствии с приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»**.

27. Классификация (пересмотр класса) информационной системы персональных данных проводится комиссией органа (органов) военного управления, в интересах которого создается (эксплуатируется) информационная система, с привлечением органа

---

*Зарегистрирован в Министерстве юстиции Российской Федерации 19 февраля 2010 г., регистрационный № 16456.

**Зарегистрирован в Министерстве юстиции Российской Федерации 3 апреля 2008 г., регистрационный № 11462.

военного управления, осуществляющего по доверенности функции государственного заказчика вооружения, военной, специальной техники и военно-технического имущества в рамках государственного оборонного заказа, и специалистов по обеспечению безопасности информации на этапе создания или в ходе эксплуатации информационной системы.

28. Разрешением на обработку персональных данных на объекте информационной системы персональных данных является приказ руководителя органа военного управления о вводе указанного объекта в эксплуатацию, который издается на основании положительных выводов комиссии и результатов оценки соответствия требованиям безопасности информации.

29. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

30. Персональные данные могут быть предоставлены для ознакомления:

а) сотрудникам, допущенным к обработке персональных данных с использованием средств автоматизации, в части, касающейся их должностных обязанностей;

б) уполномоченным работникам федеральных органов исполнительной власти в порядке, установленном законодательством Российской Федерации.

31. Уполномоченными должностными лицами при обработке персональных данных в информационных системах персональных данных должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

32. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации организационных мер и путем применения программных и технических средств.

33. Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к

информационно-телекоммуникационной сети Интернет, не допускается.

34. Доступ пользователей к персональным данным в информационных системах персональных данных Министерства обороны разрешается после обязательного прохождения процедуры идентификации и аутентификации.

35. Структурными подразделениями (должностными лицами) Министерства обороны, ответственными за обеспечение безопасности персональных данных при их обработке в информационных системах, должно быть обеспечено:

а) своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководящих должностных лиц Министерства обороны;

б) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) постоянный контроль за обеспечением уровня защищенности персональных данных;

д) знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;

з) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по

предотвращению возможных опасных последствий подобных нарушений.

36. В случае выявления нарушений порядка обработки персональных данных в информационных системах Министерства обороны уполномоченными должностными лицами принимаются меры по установлению причин нарушений и их устранению.

V. Правила допуска и доступа к персональным данным

37. Уполномоченные должностные лица допускаются к информации, содержащей персональные данные, в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими служебных обязанностей.

38. Допуск к персональным данным разрешается руководителем органа военного управления с соблюдением требований настоящего Положения.

39. Фактом ознакомления с разрешением на допуск является подпись уполномоченного должностного лица об ознакомлении со списком должностных лиц, доступ которых к персональным данным необходим для выполнения служебных обязанностей.

40. Доступ уполномоченных должностных лиц к персональным данным в информационных системах осуществляется после прохождения процедуры, установленной в пункте 34 настоящего Положения.

41. В соответствии с частью 3 статьи 6 Федерального закона «О персональных данных» Министерство обороны вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного контракта, либо на основании правового акта Министерства обороны. Лицо, осуществляющее обработку персональных данных по поручению Министерства обороны, обязано соблюдать принципы и правила обработки персональных данных.

42. В поручении Министерства обороны (правовом акте, контракте, договоре, соглашении) должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность

такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

43. Допуск к персональным данным, в том числе содержащимся в информационных системах персональных данных сторонних организаций, деятельность которых не связана с исполнением функций Министерства обороны, регламентируется законодательством Российской Федерации, контрактами (договорами, соглашениями) и другими нормативными правовыми актами Российской Федерации.

44. Доступ к техническим (программно-техническим) средствам информационных систем персональных данных Министерства обороны предоставляется сторонним организациям, выполняющим работы на договорной основе.

Порядок допуска указанных организаций определяется в договоре на выполнение работ (оказание услуг). Решением о допуске является подписанный в установленном порядке договор на выполнение работ (оказание услуг).

45. Доступ к персональным данным сторонних организаций осуществляется на основании письменных запросов или письменных соглашений (договоров) сторон об обмене информацией.

В письменном запросе (соглашении, договоре) должны быть указаны следующие сведения:

цель получения информации;

конкретное наименование информации (состав персональных данных);

способ доступа (предоставления), а также сведения о регистрации в уполномоченных органах по защите прав субъектов персональных данных, осуществляющих функции по контролю и надзору в сфере информационных технологий и связи.

При наличии соглашения со сторонней организацией о допуске к персональным данным (предоставлении информации) доступ к персональным данным осуществляется в порядке, указанном в подписанном соглашении (договоре).

46. Доступ к персональным данным, в том числе содержащимся в информационных системах персональных данных

сторонних организаций, выполняющих работы на договорной основе, осуществляется на основании подписанного договора на оказание услуг, а также настоящего Положения.

47. Запрещается передача электронных копий баз (банков) данных, содержащих персональные данные, любым сторонним организациям, за исключением случаев, предусмотренных законодательством Российской Федерации.