УТВЕРЖДАЮ
Руководитель Федеральной
службы государственной статистики
_____А.Е. Суринов
«**09**» **сентября** **2013 г.**
от 09.09.2013 №7-У

ПРАВИЛА
ПО ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ,
ПОЛУЧЕННЫХ В ХОДЕ СТАТИСТИЧЕСКИХ НАБЛЮДЕНИЙ

1. Общие положения

1.1. Правила обработки персональных данных разработаны на основании требований:

Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон № 152-ФЗ);

Федерального закона от 29.11.2007 № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» (далее - Закон № 282-ФЗ);

Федерального закона от 02.07.2013 № 171-ФЗ «О внесении изменений в федеральный закон «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» и отдельные законодательные акты Российской Федерации» (далее - Закон № 171-ФЗ);

Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

Федерального закона от 25.01.2002 № 8-ФЗ «О Всероссийской переписи населения»;

постановления Правительства Российской Федерации от 02.06.2008 № 420 «О Федеральной службе государственной статистики»;

постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановления 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 соответствие с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила устанавливают единый порядок обработки персональных данных, полученных в ходе федеральных статистических наблюдений

территориальными органами Росстата и уполномоченными организациями, осуществляющими сбор и обработку персональных данных в целях формирования официальной статистической информации.

2. Обработка персональных данных

2.1 Основные понятия и определения

В настоящих Правилах используются следующие основные понятия:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

федеральное статистическое наблюдение - сбор первичных статистических данных и административных данных субъектами официального статистического учета;

первичные статистические данные - документированная информация по формам федерального статистического наблюдения, получаемая от респондентов, или информация, документируемая непосредственно в ходе федерального статистического наблюдения;

оператор - территориальные органы Росстата и уполномоченные организации, осуществляющие сбор и обработку персональных данных в целях формирования официальной статистической информации;

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых оператором с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники оператора;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

информационная система персональных данных - совокупность содержащихся в базах данных оператора персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

административные данные - используемая при формировании официальной статистической информации документированная информация, получаемая федеральными органами государственной власти, иными федеральными государственными органами, органами государственной власти субъектов Российской Федерации, иными государственными органами субъектов Российской Федерации, органами местного самоуправления, государственными организациями в связи с осуществлением ими разрешительных, регистрационных, контрольно-надзорных и других административных функций, а также иными организациями, на которые осуществление указанных функций возложено законодательством Российской Федерации.

2.2. Принципы обработки персональных данных

Принципами обработки персональных данных являются:

ограничение обработки персональных данных, полученных в ходе статистических наблюдений, достижением цели статистического наблюдения;

соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки;

недопущение обработки персональных данных, полученных в ходе статистических наблюдений, несовместимой с целями сбора персональных данных;

недопущение объединения баз данных, содержащих персональные данные, полученные в ходе статистических наблюдений, обработка которых осуществляется в целях, несовместимых между собой;

недопущение обработки персональных данных, избыточных по отношению к заявленным целям их обработки;

обеспечение проведения автоматизированной обработки персональных данных, только на аттестованных, в соответствии с требованиями безопасности информации, автоматизированных рабочих местах;

обеспечение точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;

обеспечение хранения персональных данных, полученных в ходе статистических наблюдений, с соблюдением условий, предотвращающих несанкционированный доступ.

2.3. Порядок обработки персональных данных

Территориальные органы Росстата и уполномоченные организации, осуществляющие сбор и обработку персональных данных в целях формирования официальной статистической информации, получают от респондентов сведения по формам федерального статистического наблюдения и обеспечивают их защиту в соответствии с законодательством Российской Федерации.

Обработка персональных данных должна осуществляться с соблюдением принципов, предусмотренных законодательством Российской Федерации, приведенных в п. 2.2 настоящих Правил,

Обработка персональных данных территориальными органами Росстата и уполномоченными организациями, осуществляющими сбор и обработку персональных данных в целях формирования официальной статистической информации, осуществляется при условии обязательного обезличивания персональных данных в соответствии с требованиями пункта 9 статьи 6 Закона № 152-ФЗ и требованиями пункта 4 статьи 9 Закона № 282-ФЗ (в редакции Закона № 171-ФЗ).

На титульном листе бланков форм федерального статистического наблюдения, содержащих персональные данные, расположена линия отрыва, обеспечивающая обезличивание персональных данных при их обработке в соответствии с требованиями Формуляра-образца формы федерального статистического наблюдения, утвержденного приказом Росстата от 16.04.2008 № 85 (признан не нуждающимся в государственной регистрации (письмо Минюста России от 07.05.2008 № 01/4541-АБ).

Также на титульном листе бланков форм федерального статистического наблюдения, содержащих персональные данные, содержится гриф об обязательном обезличивании персональных данных при их статистической обработке.

Персональные данные, полученные после выполнения процедуры их обезличивания, должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия. На упаковках указывается оператор, ответственный за организацию обработки персональных данных. Упаковки опечатываются таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок.

На упаковке необходимо указать: количество листов, индекс формы, периодичность, срок хранения.

Оператор обязан обеспечить:

предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права на доступ к персональным данным;

своевременное обнаружение фактов несанкционированного доступа к персональным данным;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к персональным данным;

недопущение воздействия на технические средства обработки персональных данных, в результате которого нарушается их функционирование;

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

постоянный контроль за обеспечением уровня защищенности персональных данных.

2.4. Обеспечение безопасности персональных данных

В соответствии со статьей 7 Закона № 152-ФЗ оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные, полученные в ходе статистических наблюдений.

Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты поступивших от респондентов 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.

Для предотвращения несанкционированного доступа к персональным данным применяются следующие организационно-технические меры:

назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;

ограничение состава лиц, имеющих доступ к персональным данным;

организация учета, хранения и обращения носителей информации;

определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;

разработка на основе модели угроз системы защиты персональных данных;

применение защищенных каналов связи при передаче персональных данных в электронном виде;

аттестация по соответствию требованиям безопасности информации программно-аппаратных средств обработки персональных данных;

разграничение доступа пользователей к информационным ресурсам и программно-аппаратным средствам обработки информации;

регистрация и учет действий пользователей информационных систем персональных данных;

использование антивирусных средств и средств восстановления системы защиты персональных данных;

применение средств межсетевого экранирования, обнаружения вторжений, анализа защищенности персональных данных, полученных в ходе статистических наблюдений;

применение процедуры обезличивания персональных данных, полученных в ходе статистических наблюдений, перед размещением в открытом доступе на сайте Росстата;

организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

немедленное уведомление о фактах утраты ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

2.5. Хранение персональных данных

Хранение персональных данных осуществляется структурными подразделениями Оператора.

Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях.

Во избежание несанкционированного доступа к персональным данным следует оборудовать отдельное помещение, либо помещение, где хранятся такие данные, в сейфах, металлических шкафах или специальных помещениях, позволяющих обеспечить их сохранность под ответственностью лиц.

Подразделения Оператора, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденному постановлением Правительства Российской Федерации от 15.09.2008 №687.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители территориальных органов Росстата и уполномоченных на обработку статистических данных организаций.

2.6. Уничтожение персональных данных

Персональные данные субъектов подлежат уничтожению в порядке и случаях, предусмотренных законодательством Российской Федерации.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации в сфере обработки персональных данных.

Упаковки, предназначенные для уничтожения, вскрывает только оператор, ответственный за организацию обработки персональных данных. Если содержимое упаковки не соответствует указанному в письме или сама упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то составляется акт.

Уничтожение документов, содержащих персональные данные, осуществляется в порядке, предусмотренном архивным законодательством Российской Федерации.

Бумажные носители персональных данных уничтожаются путем сожжения или измельчения.

Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путём механического нарушения целостности

носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

Уничтожение производится по акту комиссией в составе не менее двух человек. В акте указывается, что уничтожается и в каком количестве. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении.

2.7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Ответственный за организацию обработки персональных данных в территориальном органе назначается руководителем территориального органа из числа государственных служащих, относящихся к высшей и (или) главной группе должностей категории "руководители" в соответствии с распределением обязанностей.

Ответственный за обработку персональных данных в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящими Правилами.

Ответственный за обработку персональных данных обязан:

организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в территориальных органах 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;

осуществлять внутренний контроль за соблюдением государственными служащими требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

доводить до сведения государственных служащих положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

Ответственный за обработку персональных данных несёт ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных в территориальном органе в соответствии с положениями законодательства Российской Федерации в области персональных данных.