Комментарий к Федеральному закону от 27.07.2006 N 152-ФЗ "О персональных данных"

Глава 1. Общие положения

Статья 1. Сфера действия настоящего Федерального закона

1. Статьей 1 комментируемого Закона определяется сфера действия Закона, а также уточняются отношения, на которые действие этого Закона не распространяется.

Персональные данные (ПД) могут обрабатывать федеральные органы государственной власти. Под федеральными органами власти следует понимать органы власти, осуществляющие властные полномочия на федеральном уровне. Напоминаем, что согласно ст. 10 Конституции РФ государственная власть в РФ осуществляется на основе разделения на законодательную, исполнительную и судебную. Статья 11 Конституции РФ гласит, что государственную власть в Российской Федерации осуществляют Президент РФ; Федеральное Собрание (Совет Федерации и Государственная Дума); Правительство РФ; суды РФ.

Правительство РФ в свою очередь состоит из членов Правительства РФ - Председателя Правительства РФ, заместителей Председателя Правительства РФ и федеральных министров.

Судебная власть в РФ представлена системой судов: Конституционный Суд РФ; Верховный Суд РФ; Высший Арбитражный Суд РФ; другие федеральные суды.

Следуем дальше. Действие комментируемого Закона распространяется также на органы государственной власти субъектов РФ, обрабатывающие ПД. На уровне субъектов РФ существуют органы исполнительной и законодательной власти субъектов РФ.

Субъектами, обрабатывающими ПД, также могут быть иные органы государственной власти, кроме тех, что перечислены выше. К ним, например, относятся Центральный банк РФ, Пенсионный фонд РФ, Федеральный фонд обязательного медицинского страхования, Фонд социального страхования РФ, Центральная избирательная комиссия РФ т.п.

Обработка ПД ведется и органами местного самоуправления.

Согласно ст. 34 Федерального закона от 06.10.2003 N 131-ФЗ "Об общих принципах организации местного самоуправления в Российской Федерации" структуру органов местного самоуправления составляют:

- представительный орган муниципального образования;
- глава муниципального образования;
- местная администрация (исполнительно-распорядительный орган муниципального образования);
- контрольный орган муниципального образования;
- иные органы и выборные должностные лица местного самоуправления, предусмотренные уставом муниципального образования и обладающие собственными полномочиями по решению вопросов местного значения.

Муниципальные органы, не входящие в систему органов местного самоуправления также обрабатывают ПД.

Если юридические лица обрабатывают ПД, на них также распространяется действие комментируемого Закона. Согласно ст. 48 Гражданского кодекса РФ (далее по тексту - ГК РФ) юридическим лицом признается организация, которая имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество и отвечает по своим обязательствам этим имуществом, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде. В РФ юридические лица могут быть коммерческими и некоммерческими (преследующими извлечение прибыли в качестве основной цели своей деятельности либо не имеющие извлечение прибыли в качестве такой цели и не распределяющие полученную прибыль между участниками). В качестве примера коммерческих организаций можно привести общества с ограниченной ответственностью, акционерные общества, производственные кооперативы и т.д. Самыми распространенными организационно-правовыми формами некоммерческих организаций являются некоммерческие партнерства, общественные организации, автономные некоммерческие организации и т.п.

Под физическими лицами, осуществляющими обработку ПД в рамках комментируемого Закона, понимаются граждане, осуществляющие предпринимательскую деятельность. Так, согласно ст. 23 ГК РФ гражданин вправе заниматься предпринимательской деятельностью без образования юридического лица с момента государственной регистрации в качестве индивидуального предпринимателя. К физическим лицам, осуществляющим обработку ПД, можно также отнести адвокатов, нотариусов, глав крестьянско-фермерских хозяйств.

Обращаем внимание, что согласно п. 1 комментируемой статьи обработка ПД может происходить как с использованием средств автоматизации так и без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации. Под средствам автоматизации понимаются технические средства, освобождающие человека частично или полностью от непосредственного участия в процессах получения, преобразования, передачи и использования информации. В качестве примера можно привести автоматизированные банковские системы, содержащие данные о сотрудниках банка, о клиентах, партнерах, биллинговые системы, содержащие данные о клиентах, осуществляющих оплату услуг, call-центры, содержащие данные о клиентах и сотрудниках в зависимости от предназначения call-центра, автоматизированные медицинские системы, содержащие данные о пациентах и т.п.

Автоматизированная обработка ПД включает в себя действия с автоматизированными файлами ПД. В случае с обработкой ПД понятие "автоматизированный файл ПД" обозначает любой комплекс данных о субъектах ПД, подвергающийся

автоматизированной обработке.

В ст. 2 Конвенции Совета Европы о защите личности в связи с автоматической обработкой персональных данных от 28.01.1981 г. "автоматизированная база данных" означает любой набор данных, к которым применяется автоматическая обработка. При этом "автоматическая обработка" включает следующие операции, если они полностью или частично осуществляются с применением автоматизированных средств:

- накопление данных;
- проведение логических или/и арифметических операций с такими данными;
- их изменение, стирание, восстановление или распространение.

Статья 5 Конвенции Совета Европы о защите личности в связи с автоматической обработкой персональных данных от 28.01.1981 г. гласит, что ПД, проходящие автоматизированную обработку, должны быть:

- получены и обработаны добросовестным и законным образом;
- накопленными для точно определенных и законных целей и не использоваться в противоречии с этими целями;
- адекватными, относящимися к делу и не избыточными применительно к целям, для которых они накапливаются;
- точными и в случае необходимости обновляться;
- сохранены в такой форме, которая позволяет идентифицировать субъектов данных, не дольше, чем этого требует цель, для которой эти данные накапливаются.

Статьей 6 вышеуказанной Конвенции устанавливается, что ПД о национальной принадлежности, политических взглядах либо религиозных или иных убеждениях, а равно ПД, касающиеся здоровья или сексуальной жизни, могут подвергаться автоматической обработке только в тех случаях, когда национальное право предусматривает надлежащие гарантии. Это же правило применяется к ПД, касающимся судимости. Кроме того Конвенция обязывает операторов ПД принимать надлежащие меры для охраны ПД, накопленных в автоматизированных базах данных, от случайного или несанкционированного разрушения или случайной утраты, а равно от несанкционированного доступа, изменения или распространения.

Идем дальше. Постановлением Правительства РФ от 15.09.2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" установлен порядок обработки ПД без использования средств автоматизации. Согласно упомянутому Постановлению обработкой ПД, содержащихся в информационной системе ПД либо извлеченных из такой системы, без использования средств автоматизации называется такая обработка, когда действия с ПД, такие как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов ПД, осуществляются при непосредственном участии человека. Важно помнить, что обработка ПД не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПД содержатся в информационной системе ПД либо были извлечены из нее.

Приведем пример. Так, если сотрудник организации занес данные о работниках в компьютер лишь с целью их распечатать, а затем удалил эти данные, такую обработку ПД можно считать неавтоматизированной. Однако если же оператор сохранил ПД в виде файла и хранит их на компьютере для дальнейшего использования, то, по мнению авторов, такую обработку ПД нужно рассматривать, в том числе, и как автоматизированную.

В том случае, если обработка ПД осуществляется без использования средств автоматизации, необходимо учитывать, что такая информация должна обособляться от иной информации. Такие ПД могут, например, фиксироваться на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

Так, согласно требованиям постановления Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" при фиксации ПД на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Поэтому для обработки различных категорий ПД для каждой категории ПД должен использоваться отдельный материальный носитель.

Часто в организациях используются типовые формы документов, характер информации в которых предполагает или допускает включение в них ПД. В этом случае типовая форма должна соответствовать некоторым требованиям. Так, сама типовая форма или связанные с ней документы (например, инструкции по ее заполнению, карточки, реестры и журналы) должны содержать:

- сведения о цели обработки ПД, осуществляемой без использования средств автоматизации;
- имя (наименование) и адрес оператора;
- фамилию, имя, отчество и адрес субъекта ПД;
- источник получения ПД;
- сроки обработки ПД;
- перечень действий с ПД, которые будут совершаться в процессе их обработки;
- общее описание используемых оператором способов обработки ПД.

Кроме того, типовая форма, которая предполагает включение в нее ПД, должна предусматривать поле, в котором субъект ПД может поставить отметку о своем согласии на обработку его данных, осуществляемую без использования средств автоматизации. Такое поле должно быть обязательно, если в соответствии с требованиями комментируемого Закона необходимо получения письменного согласия на обработку ПД от субъекта ПД.

Следует помнить, что типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПД, содержащихся в документе, имел возможность ознакомиться со своими ПД, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПД. А также типовая форма должна исключать объединение полей, предназначенных для

внесения ПД, цели обработки которых заведомо не совместимы.

Во многих организациях ведутся журналы (реестры, книги), необходимые для однократного пропуска субъекта ПД на территорию, на которой находится оператор, содержащие ПД. В подобных случаях оператором ПД должны выполняться определенные условия. Например, необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора. В акте будут содержаться следующие сведения:

- сведения о цели обработки ПД, осуществляемой без использования средств автоматизации;
- способы фиксации и состав информации, запрашиваемой у субъектов ПД;
- перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги);
- сроки обработки ПД;
- сведения о порядке пропуска субъекта ПД на территорию, на которой находится оператор, без подтверждения подлинности ПД, сообщенных субъектом ПД.

Копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается. Кроме того, ПД каждого субъекта ПД могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПД на территорию, на которой находится оператор.

Если требуется уточнить ПД, обработка которых осуществляется без использования средств автоматизации, то это должно быть произведено путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПД.

Постановлением Правительства РФ от 15.09.2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" устанавливаются и требования к обеспечению безопасности ПД при их обработке, осуществляемой без использования средств автоматизации. Обработка ПД должна осуществляться таким образом, чтобы в отношении каждой категории ПД можно было определить места хранения ПД (материальных носителей) и установить перечень лиц, осуществляющих обработку ПД либо имеющих к ним доступ. Необходимо обеспечивать раздельное хранение ПД (материальных носителей), обработка которых осуществляется в различных целях. Важно учитывать, что при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Пример.

Операторы, обрабатывающие ПД неавтоматизированным способом хранят каждую категорию полученных от граждан ПД в разных папках, ящиках, файлах и т.д. Приказом руководителя организации определяется перечень лиц, которые обрабатывают тот или иной информационный блок либо получают к нему доступ.

2. Пунктом 2 комментируемой статьи определяются случаи, на которые не распространяется действие Закона.

Обрабатывать ПД может физическое лицо, не являющееся индивидуальным предпринимателем. При этом ПД обрабатываются в личных целях при условии соблюдения прав субъектов ПД. Таким образом, гражданин имеет право для себя лично вести сбор и накопление ПД, например, на домашнем компьютере (сделать справочник с данными своих знакомых: адресами, фамилиями, датами рождения). Однако Закон требует, чтобы в таких случаях не нарушались права субъектов ПД. Т.е., справочник, приведенный в качестве примера, может использоваться гражданином только лично, передача его другим лицам не допустима.

Действие комментируемого Закона не распространяется на организацию хранение, комплектование, учет и использование содержащих ПД документов Архивного фонда РФ и других архивных документов в соответствии с Федеральным законом от 22.10.2004 N 125-ФЗ "Об архивном деле в Российской Федерации". Напоминаем, что Архивный фонд РФ содержит документы, относящиеся к федеральной, муниципальной и частной собственности, а также собственности субъектов РФ.

Например, к федеральной собственности, относятся такие документы как:

- документы, хранящиеся в федеральных государственных архивах, федеральных музеях и библиотеках, организациях Российской академии наук (за исключением архивных документов, переданных в эти архивы, музеи, библиотеки, организации Российской академии наук на основании договора хранения без передачи их в собственность),
- документы федеральных органов государственной власти, иных государственных органов РФ, в том числе органов прокуратуры РФ, Центральной избирательной комиссии РФ, Счетной палаты РФ, Центрального банка РФ (Банка России), Государственной корпорации по атомной энергии "Росатом";
- документы, бывших неприятельских государств, перемещенные в Союз ССР в результате Второй мировой войны и находящиеся на территории РФ, если иное не предусмотрено законодательством РФ о перемещенных культурных ценностях;
- другие документы, отнесенные к федеральной собственности федеральными законами.

Архивный фонд РФ составляют также следующие архивные документы субъектов РФ:

- документы, хранящиеся в государственных архивах субъекта РФ, музеях и библиотеках субъекта РФ (за исключением архивных документов, переданных в эти архивы, музеи и библиотеки на основании договора хранения без передачи их в собственность);
- документы, государственных органов и организаций субъекта РФ.

Кроме того, Архивный фонд РФ составляют документы, относящиеся к муниципальной собственности:

- документы органов местного самоуправления и муниципальных организаций;

- документы, хранящиеся в муниципальных архивах, музеях и библиотеках (за исключением архивных документов, переданных в эти архивы, музеи и библиотеки на основании договора хранения без передачи их в собственность).

Архивными документами, являющимися частной собственностью являются:

- документы организаций, действующих на территории РФ и не являющихся государственными или муниципальными, в том числе общественных объединений со дня их регистрации в соответствии с законодательством РФ об общественных объединениях и религиозных объединений после отделения церкви от государства;

- документы, созданные гражданами или законно приобретенные ими.

Почти все вышеперечисленные документы могут содержать ПД. Однако, как следует из содержания п. 2 комментируемой статьи обработка таких документов производится в соответствии с Федеральным законом от 22.10.2004 N 125-ФЗ "Об архивном деле в Российской Федерации". Так, в п. 3 ст. 25 указанного выше Закона указывается, что ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, устанавливается на срок 75 лет со дня создания указанных документов. С письменного разрешения гражданина, а после его смерти с письменного разрешения наследников данного гражданина ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, может быть отменено ранее чем через 75 лет со дня создания указанных документов.

Из сферы действия комментируемого Закона также исключается обработка сведений, подлежащих включению в единый государственный реестр индивидуальных предпринимателей (ЕГРИП). Но такое исключение допустимо лишь в том случае, если обработка осуществляется в связи с деятельностью физического лица в качестве индивидуального предпринимателя.

Согласно п. 2 ст. 5 Федерального закона от 08.08.2001 N 129-ФЗ "О государственной регистрации юридических лиц и индивидуальных предпринимателей" (далее по тексту - ФЗ "О государственной регистрации юридических лиц и индивидуальных предпринимателей" в ЕГРИП содержатся, в частности, следующие сведения об индивидуальном предпринимателе:

- фамилия, имя и (в случае, если имеется) отчество;

- пол;

- дата и место рождения;

- гражданство;

- место жительства в РФ;

- данные основного документа, удостоверяющего личность гражданина РФ на территории РФ;

- вид и данные документа, установленного федеральным законом или признаваемого в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина (в случае, если индивидуальный предприниматель является иностранным гражданином) и т.д.

В настоящее время порядок хранения таких ПД и порядок их передачи в архивы регулируется постановлением Правительства РФ от 16.10.2003 N 630 "О Едином государственном реестре индивидуальных предпринимателей, Правилах хранения в единых государственных реестрах юридических лиц и индивидуальных предпринимателей документов (сведений) и передачи их на постоянное хранение в государственные архивы, а также о внесении изменений и дополнений в постановления Правительства РФ от 19.06.2002 г. N 438 и 439".

Действие комментируемого Закона также не распространяется на обработку ПД, отнесенных к сведениям, составляющим государственную тайну. При этом порядок отнесения сведений к государственной тайне определен Законом РФ от 21.07.1993 N 5485-1 "О государственной тайне". Так, государственную тайну составляют защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. В соответствии со ст. 5 упомянутого выше Закона государственную тайну составляют следующие сведения и информация, которые могут содержать ПД:

- сведения в военной области (например, сведения о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил РФ, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов, о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке и т.п., см. п. 1 ст. 5 Закона РФ от 21.07.1993 N 5485-1 "О государственной тайне");

- сведения в области экономики, науки и техники (например, о содержании планов подготовки РФ и ее отдельных регионов к возможным военным действиям, о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства и т.п., см. п. 2 ст. 5 Закона РФ от 21.07.1993 N 5485-1 "О государственной тайне");

- сведения в области внешней политики и экономики (например, о внешнеполитической, внешнеэкономической деятельности РФ, преждевременное распространение которых может нанести ущерб безопасности государства, о финансовой

политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства, см. п. 3 ст. 5 Закона РФ от 21.07.1993 N 5485-1 "О государственной тайне");

- сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности (например, о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность, о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства, см. п. 4 ст. 5 Закона РФ от 21.07.1993 N 5485-1 "О государственной тайне").

Абзац 5 п. 2 комментируемой статьи был введен Федеральным законом от 28.06.2010 N 123-ФЗ "О внесении изменений в статью 1 Федерального закона "О персональных данных" и статью 15 Федерального закона "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" и вступил в силу 01.07.2010 года. Таким образом, в настоящее время действие комментируемого Закона также не распространяется на предоставление уполномоченными органами информации о деятельности судов в РФ. Порядок предоставления указанной информации регулируется Федеральным законом от 22.12.2008 N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации".

Под информацией о деятельности судов понимается информация, подготовленная в пределах своих полномочий судами, Судебным департаментом, органами Судебного департамента, органами судейского сообщества либо поступившая в суды, Судебный департамент, органы Судебного департамента, органы судейского сообщества и относящаяся к деятельности судов.

В соответствии со ст. 6 упомянутого Федерального закона доступ к информации о деятельности судов обеспечивается следующими способами:

- присутствием граждан (физических лиц), в том числе представителей организаций (юридических лиц), общественных объединений, органов государственной власти и органов местного самоуправления, в открытом судебном заседании;
- обнародованием (опубликованием) информации о деятельности судов в средствах массовой информации;
- размещением информации о деятельности судов в информационно-телекоммуникационной сети Интернет (далее - сеть Интернет);
- размещением информации о деятельности судов в занимаемых судами, Судебным департаментом, органами Судебного департамента, органами судейского сообщества помещениях;
- ознакомлением пользователей информацией с информацией о деятельности судов, находящейся в архивных фондах;
- предоставлением пользователям информацией по их запросу информации о деятельности судов.

Статья 2. Цель настоящего Федерального закона

Пунктом 2 комментируемой статьи определена основная цель Закона. Он призван обеспечить эффективную защиту прав и свобод человека и гражданина в соответствии с основными правами и свободами, провозглашенными Конституцией РФ.

Согласно ст. 17 Конституции РФ в России признаются и гарантируются права и свободы человека и гражданина согласно общепризнанным принципам и нормам международного права. Статьи 23-24 Конституции РФ устанавливают, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. При этом сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. На органы государственной власти и органы местного самоуправления, их должностные лица возлагается обязанность обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

В современном мире почти каждый желающий может найти в Интернете информацию о ПД граждан. При этом свои ПД граждане раскрывают зачастую сами, например, оформляя покупку товара с доставкой на дом, регистрируясь на веб-сайте. Но далеко не всегда лица, получающие такую информацию, добросовестно сохраняют ее.

Во всем мире ПД стремятся защищать на уровне государства, принимая законы, регулирующие порядок сбора, хранения и использования сведений о гражданах страны.

Обеспечивая защиту ПД, РФ укрепляет правовую защищенность и безопасность личности и создает благоприятную обстановку для всестороннего развития граждан и общества в целом. Кроме того, по мнению многих российский экспертов в области права, одной из целей принятия комментируемого Закона явилась необходимость устранения некоторых барьеров в торговле со странами Евросоюза, т.к. согласно Директиве Евросоюза ПД могут передаваться только в страны, обеспечивающие такой же уровень защиты, как и в Европе. Поэтому положения комментируемого Закона отчасти повторяют положения европейского законодательства в данной сфере.

Комментируемый Закон установил дополнительные гарантии защиты ПД в нашей стране, такие как:

- ограничение на передачу персональной информации третьим лицам без согласия человека;
- требование к информированию человека о целях и способах обработки информации о нем;
- необходимость получать согласие на сбор сведений о человеке у него самого;
- обеспечение безопасности и конфиденциальности персональных данных.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

1. В комментируемой статье законодатель формирует инструментарий, который затем используется в тексте Закона. Разъяснение основных понятий, используемых в Законе необходимо для более точного понимания положений этого нормативного акта.

Понятие "персональные данные" является основополагающим в Законе. Законодатель определяет ПД как любую информацию, которая:

- относится к определенному лицу;
- определяет это лицо.

Таким образом, например, только указанное в информационной базе место рождения не считается ПД, если эти сведения не будут связаны с конкретной фамилией человека. В то время как информация - Петров Иван Петрович, рожденный в селе Новолокти Тюменской области, - будет являться ПД конкретного гражданина.

Обращаем внимание, что Закон относит к ПД следующую информацию:

- фамилию, имя, отчество гражданина;
- год, месяц, дату и место рождения;
- адрес;
- семейное положение;
- социальное положение;
- имущественное положение;
- сведения об образовании;
- сведения о профессии;
- сведения о доходах;
- другие сведения, относящиеся к определенному или определяемому на основании такой информации физическому лицу.

Перечень информации, которую можно отнести к ПД, является открытым.

В соответствии с действующим законодательством состав и содержание ПД определяют операторы ПД в зависимости от целей их обработки. Как правило, операторы различных организаций, оказывающих услуги, просят предоставить им контактные данные клиента. Такие базы данных по контактам ведутся не только по постоянным клиентам, но и по информации, полученной в ходе рекламных кампаний. Все эти сведения являются ПД.

Понятие "персональные данные" ранее раскрывалось в Указе Президента РФ от 06.03.1997 N 188 "Об утверждении Перечня сведений конфиденциального характера". Так, к сведениям конфиденциального характера Указ относит сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

В ст. 85 Трудового кодекса РФ (далее по тексту - ТК РФ) также дается определение ПД работника. К ним относится информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Кроме комментируемого Закона порядок работы с ПД определяется и другими актами. Например, согласно приказу Судебного департамента при Верховном Суде РФ от 20.04.2007 N 52 "Об утверждении Инструкции о порядке защиты персональных данных, содержащихся в личных делах председателей, заместителей председателя и судей районных судов, а также гарнизонных военных судов" ПД, содержащиеся в личных делах председателей, заместителей председателя и судей районных судов, а также гарнизонных военных судов, относятся к сведениям конфиденциального характера, имеют ограниченный доступ и разглашению не подлежат, за исключением ПД, на которые в соответствии с федеральными законами не распространяются требования о соблюдении конфиденциальности. При этом личные дела председателей, заместителей председателя и судей районных судов, а также гарнизонных военных судов ведутся кадровыми службами управлений (отделов) Судебного департамента в субъектах РФ. Кадровые службы управлений (отделов) Судебного департамента в субъектах РФ обеспечивают защиту ПД, содержащихся в личных делах председателей, заместителей председателя, судей районных судов и гарнизонных военных судов от неправомерного их использования или утраты.

На охране ПД граждан стоят и суды. Например, в постановлении ФАС Московского округа от 29.04.2010 N КА-А40/4062-10 по делу N А40-159104/09-93-1333 указывается, что трудовой договор с руководителем, как документ, содержащий ПД, не может быть передан сторонним организациям и лицам для ознакомления без согласия на то субъекта ПД.

Следуем дальше. Как упоминалось выше, ПД - это определенная информация. Согласно ст. 2 Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (далее по тексту - ФЗ "Об информации, информационных технологиях и о защите информации"), информацией являются сведения (сообщения, данные) независимо от формы их представления. Информация может являться объектом публичных, гражданских и иных правовых отношений, а также свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения. Поэтому информация в зависимости от категории доступа к ней подразделяется на:

- общедоступную информацию;
- информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Таким образом, ПД граждан, кроме тех, которые относятся к общедоступным (ст. 8 Закона), являются информацией, доступ к которой ограничен комментируемым Законом.

Кроме того, вся информация согласно ФЗ "Об информации, информационных технологиях и о защите информации" в зависимости от порядка ее предоставления или распространения подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в РФ ограничивается или запрещается.

Существуют различные категории ПД, например:
- общедоступные ПД;
- специальные категории ПД;
- категории ПД, обрабатываемые в информационных системах персональных данных;
- биометрические ПД и т.д.;

2. Законодатель называет оператором ПД государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку ПД. Оператор также определяет цели и содержание обработки ПД. Таким образом, оператором ПД будет являться любая организация, осуществляющая пусть даже простую систематизацию или накопление ПД. Как правило, под это определение подходят почти все компании независимо от форм собственности, т.к. они как минимум осуществляют сбор, систематизацию, хранение и уточнение сведений о своих сотрудниках. Кроме этого большинство организаций по роду своей деятельности обрабатывают сведения о своих клиентах, партнерах, поставщиках.

Пример

Операторами ПД будут считаться:
- организации, которые нанимают работников по трудовым договорам, договорам гражданско-правового характера;
- страховые компании;
- операторы сотовой связи;
- учебные заведения;
- интернет-магазины;
- медицинские учреждения;
- государственные и муниципальные учреждения, ведомства и службы;
- перевозчики всех видов транспорта;
- банки и т.п.

Физические лица вынуждены представлять свои ПД подобным организациям, для заключения договоров, получения комплекса услуг. Но важно помнить, что оператору ПД не следует требовать от субъектов ПД сведений больше того, чем это нужно для какой-то конкретной цели. При этом храниться ПД могут не дольше, чем этого требуют цели, для которых они накапливались. По достижению такой цели или утраты необходимости в достижении цели ПД подлежат уничтожению. Кроме того операторы ПД обязаны гарантировать конфиденциальность информации и предоставить гражданину право самостоятельно решать какую информацию и в каком объеме он готов раскрывать.

Директору
ООО "Малахит"
г-ну Рыжикову Н.Г.
от Светловой Н.М.
проживающей по адресу:
г. Ульяновск, ул. Ленина, 8-90
10.10.2010 г.

Заявление

Я, Светлова Надежда Михайловна, 01.10.2010 г. предоставила свои персональные данные, а именно сведения об адресе, контактный телефон, ФИО, при получении дисконтной карты Вашего магазина.

Уведомляю Вас, что я возражаю против использования моих персональных данных для распространения любых рекламных сообщений и иных информационных материалов. В соответствии со ст. 14 ФЗ "О персональных данных" прошу прекратить использование всех моих персональных данных для этих целей, а также не передавать мои персональные данные третьим лицам.

Подпись _____

3. Обработка ПД включает следующие действия:
- сбор ПД;
- систематизацию ПД;
- накопление ПД;
- хранение ПД;
- уточнение (обновление, изменение) ПД;
- использование ПД;
- распространение (в том числе передачу) ПД;
- обезличивание ПД;

- блокирование ПД;
- уничтожение ПД;

Изучим понятие "обработка ПД" на примере обработки ПД работников организации. Обработкой ПД работников называется получение, хранение, комбинирование, передача или любое другое использование ПД работника.

Статьей 86 ТК РФ устанавливаются общие требования при обработке ПД работника и гарантии их защиты:

- обработка ПД работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- при определении объема и содержания обрабатываемых ПД работника работодатель должен руководствоваться Конституцией РФ, ТК РФ и иными федеральными законами, в т.ч. комментируемым Законом.
- все ПД работника работодатель должен получать у него самого. Если ПД работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения ПД, а также о характере подлежащих получению ПД и последствиях отказа работника дать письменное согласие на их получение;
- работодатель не имеет права получать и обрабатывать ПД работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;
- работодатель не имеет права получать и обрабатывать ПД работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением ряда случаев, предусмотренных ТК РФ или федеральными законами;
- при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на ПД работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;
- защита ПД работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном ТК РФ, и иными федеральными законами, в т.ч. комментируемым Законом;
- работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки ПД работников, а также об их правах и обязанностях в этой области;
- работники не должны отказываться от своих прав на сохранение и защиту тайны;
- работодатели, работники и их представители должны совместно вырабатывать меры защиты ПД работников.

Как упоминалось выше, все учебные заведения также осуществляют обработку ПД учащихся и студентов. Поэтому, следуя требованиям действующего законодательства, учебное учреждение должно получить согласие на обработку таких ПД. Если учащийся является несовершеннолетним, данное согласие должно быть получено от родителей ребенка.

Примерный образец согласия на обработку ПД учащегося (студента) от имени родителей ребенка

Согласие
на обработку персональных данных учащегося школы

Я, Соловьева Галина Сергеевна, паспорт 7899 122352 выдан 12.10.2009 г. ОВД Ленинского р-на г. Екатеринбурга, являясь матерью Соловьевой Ирины Николаевны, 10.09.1998 г. р., (далее - Обучающийся), в соответствии с федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" даю согласие на обработку персональных данных моего ребенка в средней школе N 5 г. Екатеринбурга (далее - Школа), с использованием средств автоматизации или без использования таких средств, включая хранение этих данных в архивах и размещение в информационно-телекоммуникационных сетях с целью предоставления доступа к ним на время учебы моего ребенка в Школе.

Перечень персональных данных, на обработку которых я даю согласие:

- ФИО ребенка;
- дата рождения ребенка;
- адрес;
- данные свидетельства о рождении;
- сведения о страховом медицинском полисе;
- сведения о заграничном паспорте;
- сведения о состоянии здоровья;
- сведения об успеваемости ребенка по учебным дисциплинам.

Доступ к персональным данным может предоставляться Обучающемуся, родителям (законным представителям) Обучающегося, а также административным и педагогическим работникам Школы.

Я даю разрешение на то, чтобы открыто публиковались фамилия, имя, отчество Обучающегося в связи с названиями и мероприятиями Школы и его структурных подразделений в рамках уставной деятельности.

Я предоставляю Школе право осуществлять следующие действия (операции) с ПД:

- сбор;

- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- использование;
- обезличивание;
- блокирование;
- уничтожение.

Я согласна, что Школа вправе включать обрабатываемые персональные данные Обучающегося в списки (реестры) и отчетные формы, предусмотренные нормативными документами федеральных и муниципальными органов управления образованием, регламентирующими предоставление отчетных данных.

Настоящее согласие дано мной 01.09.2010 г. и действует до 31.05.2011 г.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Школы по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Школы.

Подпись _____

Однако если договором между учащимся или его законным представителем, если учащийся является несовершеннолетним, за учащимся закреплена обязанность предоставления учебному учреждению определенных ПД, то получения согласия на обработку таких ПД не требуется в соответствии с абз. 2 п. 2 ст. 6 комментируемого Закона, за исключением случаев, когда учащимся предоставляются специальные категории ПД или биометрические ПД.

4. Из содержания п. 4 ст. 3 комментируемого Закона усматривается, что под распространением ПД понимается прежде всего передача ПД третьим лицам. При этом целями передачи ПД могут быть следующие:

- передача ПД определенному кругу лиц для определенных целей;
- ознакомление с ПД неограниченного круга лиц;
- обнародование ПД в средствах массовой информации;
- размещение ПД в информационно-телекоммуникационных сетях;
- предоставление доступа к ПД третьим лицам каким-либо иным способом.

Также, ст. 88 ТК РФ устанавливаются строгие требования к порядку передачи ПД работника:

- работодатель не имеет права сообщать ПД работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в некоторых других случаях, предусмотренных ТК РФ, комментируемым Законом или иными федеральными законами, о чем будет рассказано в последующих комментариях к статьям Закона;
- работодатель не имеет права сообщать ПД работника в коммерческих целях без его письменного согласия;
- работодатель обязан предупредить лиц, получающих ПД работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено (кроме случаев обмена ПД работников в порядке, установленном ТК РФ);
- работодатель обязан осуществлять передачу ПД работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;
- работодатель может разрешать доступ к ПД работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПД работника, которые необходимы для выполнения конкретных функций;
- работодатель не имеет права запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- работодатель должен передавать ПД работника представителям работников в порядке, установленном ТК РФ, комментируемым Законом и иными федеральными законами, и ограничивать эту информацию только теми ПД работника, которые необходимы для выполнения указанными представителями их функций.

Согласно ст. 2 ФЗ "Об информации, информационных технологиях и о защите информации" распространением информации называются действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц. Как указывалось выше, одним из видов распространения ПД является обнародование ПД в средствах массовой информации. Авторы напоминают, что в соответствии со ст. 2 Закона РФ от 27.12.1991 N 2124-1 "О средствах массовой информации" (далее по тексту - Закон "О средствах массовой информации" массовой информацией называется предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы. Под средством массовой информации понимается периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации.

Распространение ПД может происходить и в форме размещения ПД в информационно-телекоммуникационных сетях. Статья 2 ФЗ "Об информации, информационных технологиях и о защите информации" гласит, что информационно-телекоммуникационная сеть - это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Примером информационно-

телекоммуникационной сети является сеть Интернет.

Так, постановлением Правительства РФ от 18.05.2009 N 424 "Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям" устанавливается, что операторы федеральных государственных информационных систем, созданных или используемых в целях реализации полномочий федеральных органов исполнительной власти и содержащих сведения, указанные в перечне сведений о деятельности Правительства РФ и федеральных органов исполнительной власти, обязательных для размещения в информационно-телекоммуникационной сети Интернет, утвержденном постановлением Правительства РФ от 12.02.2003 г. N 98 "Об обеспечении доступа к информации о деятельности Правительства РФ и федеральных органов исполнительной власти"*(1), при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям, доступ к которым не ограничен определенным кругом лиц, обязаны обеспечить:

- защиту информации, содержащейся в информационных системах общего пользования, от уничтожения, изменения и блокирования доступа к ней;

- постоянный контроль возможности доступа неограниченного круга лиц к информационным системам общего пользования;

- восстановление информации, измененной или уничтоженной вследствие несанкционированного доступа к ней, в течение не более 8 часов;

- использование при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям средств защиты информации, прошедших оценку соответствия (в том числе в установленных случаях сертификацию), в порядке, установленном законодательством РФ;

Операторы информационных систем общего пользования и операторы связи обязаны обеспечивать информационную безопасность при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям.

5. Использование персональных данных. Согласно ст. 87 ТК РФ порядок хранения и использования ПД работников устанавливается работодателем с соблюдением требований ТК РФ, комментируемого Закона и иных федеральных законов. Таким образом, в организациях должно быть разработано и утверждено Положение о порядке хранения и использования ПД работников. Невыполнение этого требования законодательства влечет наложение административного штрафа на должностных лиц в соответствии с ст. 5.27 КоАП РФ в размере от одной тысячи до пяти тысяч рублей; на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, - от одной тысячи до пяти тысяч рублей или административное приостановление деятельности на срок до девяноста суток; на юридических лиц - от тридцати тысяч до пятидесяти тысяч рублей или административное приостановление деятельности на срок до девяноста суток.

В случае повторного нарушение этого требования законодательства должностным лицом, ранее подвергнутым административному наказанию за аналогичное административное правонарушение, - влечет дисквалификацию на срок от одного года до трех лет.

6. Блокирование ПД подразумевает временное прекращение сбора, систематизации, накопления, использования, распространения ПД, в том числе их передачи;

Следует отметить, что такой способ как блокирование ПД в отечественной практике введен впервые комментируемым Законом.

7. Уничтожение ПД. Существует ряд ситуаций, когда оператор обязан прекратить обработку ПД, блокировать или уничтожить их.

Оператор обязан это сделать по требованию субъекта ПД, если ПД являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели (см. ст. 14 комментируемого Закона).

Уничтожить ПД также нужно по достижении целей обработки или при утрате необходимости в их достижении (см. п. 2 ст. 5 комментируемого Закона).

Оператор обязан уничтожить ПД при невозможности устранить допущенные нарушения в отношении обработки ПД. В этом случае в соответствии со п. 3 ст. 21 комментируемого Закона оператор в срок, не превышающий трех рабочих дней с даты выявления нарушений в обработке ПД, должен устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПД, обязан уничтожить ПД. Об устранении допущенных нарушений или об уничтожении ПД оператор обязан уведомить субъекта ПД или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПД, - также указанный орган.

В случае отзыва субъектом ПД согласия на обработку ПД (п. 4 ст. 21 комментируемого Закона) оператор обязан прекратить обработку и уничтожить ПД в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом ПД. Об уничтожении ПД оператор обязан уведомить субъекта ПД.

Образец заявления об уничтожении персональных данных

Руководителю
Кадрового агентства "Престиж"
г-ну Феотистову Н.И.

Заявление об уничтожении персональных данных

1 июля года я обратился в Вашу организацию с целью получения помощи в поиске работы. При этом мной были предоставлены следующие персональные данные:

- ФИО;
- адрес;
- сведения об образовании;
- сведения о профессии;
- сведения о постановке на воинский учет;
- сведения о состоянии здоровья.

Кроме того при обращении в Вашу организацию производилась видео и фотосъемка.

Так как 20.07.2010 г. я был принят на постоянную работу и в услугах Вашей организации больше не нуждаюсь, прошу Вас в соответствии со ст. 21 ФЗ "О персональных данных" удалить всю информацию обо мне, включая материалы видео и фотосъемки и вернуть мне оригиналы предоставленных мною сведений.

Подпись _____

8. В результате обезличивания ПД становится невозможным определить принадлежность ПД конкретному субъекту ПД.

Рассмотрим некоторые случаи, когда целесообразно использовать этот способ обработки ПД.

В настоящее время в сети интернет существует множество веб-сайтов, требующих указать сведения о пользователе при регистрации. Согласно требованиям комментируемого Закона использование ПД пользователей таких ресурсов возможно только с письменного согласия того посетителя, которому эти данные соответствуют. Выходом в данной ситуации может быть обезличивание ПД. Таким образом, нужно сделать так, чтобы по этим ПД нельзя было идентифицировать пользователя.

9. Информационная система ПД. Приведем примеры информационных систем ПД:

- автоматизированные банковские системы, содержащие данные о сотрудниках банка, о клиентах, партнерах и т.п.;
- автоматизированные медицинские системы, содержащие данные о пациентах и т.п.;
- кадровые системы, содержащие данные о соискателях работы;
- бухгалтерские системы, содержащие данные о сотрудниках и клиентах организации;
- почтовые системы, содержащие данные о сотрудниках организации, клиентах, партнерах, заполненные карточки в адресных книгах почтовых систем и т.п.;
- системы документооборота, содержащие данные о сотрудниках организации, клиентах, партнерах;
- автоматизированные системы бюро пропусков, содержащие данные о посетителях.

Информационные системы по принадлежности можно классифицировать следующим образом:

- информационные системы государственных органов;
- информационные системы муниципальных органов;
- информационные системы юридических лиц;
- информационные системы физических лиц (за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд).

Приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13.02.2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" определяет следующие категории ПД, которые обрабатываются в информационных системах ПД:

- категория 1 - это ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 - это ПД, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 - это ПД, позволяющие идентифицировать субъекта персональных данных;
- категория 4 - это обезличенные и (или) общедоступные ПД.

Кроме того, информационные системы ПД подразделяются на типовые и специальные. Типовые информационные системы - это информационные системы, в которых требуется обеспечение только конфиденциальности ПД. Специальные информационные системы - это информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности ПД требуется обеспечить хотя бы одну из характеристик безопасности ПД, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

Следует учитывать, что к специальным информационным системам относят:

- информационные системы, в которых обрабатываются ПД, касающиеся состояния здоровья субъектов ПД;
- информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки ПД решений, порождающих юридические последствия в отношении субъекта ПД или иным образом затрагивающих его права и законные интересы.

По структуре информационные системы можно разделить:

- на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств,

предназначенные для обработки ПД (автоматизированные рабочие места);

- на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);

- на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на:

- информационные системы, имеющие подключения;
- информационные системы, не имеющие подключений.

По режиму обработки ПД в информационной системе информационные системы подразделяются на:

- однопользовательские информационные системы;
- многопользовательские информационные системы.

По разграничению прав доступа пользователей информационные системы подразделяются на:

- информационные системы без разграничения прав доступа;
- информационные системы с разграничением прав доступа.

В зависимости от местонахождения их технических средств информационные системы подразделяются на:

- информационные системы, все технические средства которых находятся в пределах РФ;
- информационные системы, технические средства которых частично или целиком находятся за пределами РФ.

По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:

- класс 1 (К1) - это информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов ПД;

- класс 2 (К2) - это информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к негативным последствиям для субъектов ПД;

- класс 3 (К3) - это информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПД;

- класс 4 (К4) - это информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПД.

Важно помнить, что результаты классификации информационных систем оформляются соответствующим актом оператора. При этом класс информационной системы может быть пересмотрен:

- по решению оператора на основе проведенных им анализа и оценки угроз безопасности ПД с учетом особенностей и (или) изменений конкретной информационной системы;

- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПД при их обработке в информационной системе.

10. Требования к сохранению конфиденциальности информации закреплены также Законом "О средствах массовой информации". Согласно ст. 41 упомянутого Закона редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне. Кроме того редакция обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом. Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, совершившего преступление либо подозреваемого в его совершении, а равно совершившего административное правонарушение или антиобщественное действие, без согласия самого несовершеннолетнего и его законного представителя.

Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" требует соблюдения конфиденциальности и при обработке ПД. В соответствии с указаниями этого документа любое лицо, действующее с санкции контролера (физического или юридического лица, официального органа, агентства или иного орган, который самостоятельно или совместно с другими определяет цели и средства обработки ПД) или обработчика (физического или юридического лица, официального органа, агентства или иного органа, который обрабатывает ПД по поручению контролера), включая самого обработчика имеющее доступ к ПД, не должно вести их обработку кроме как по указанию контролера, если это не требуется от него по закону.

11. Впервые вопрос о трансграничной передаче ПД возник, когда начался процесс объединения Европы. Ранее субъект ПД имел право отстоять свои интересы в собственной стране, но если нарушение его прав произошло за ее пределами, обеспечить полноценную защиту своих интересов он не мог.*(2)

12. Важно помнить, что сведения о субъекте ПД могут быть в любое время исключены из общедоступных баз ПД:

- по требованию субъекта ПД;
- по решению суда;
- по решению других уполномоченных государственных органов.

Статья 4. Законодательство Российской Федерации в области персональных данных

1. Комментируемая статья устанавливает перечень основных нормативно-правовых актов, которые формируют систему законодательства в области защиты ПД. Напоминаем, что нормативным правовым актом называется письменный официальный документ, принятый (изданный) в определенной форме правотворческим органом в пределах его компетенции и направленный на установление, изменение или отмену правовых норм. Нормативные правовые акты имеют общеобязательное государственное предписание постоянного или временного характера, рассчитанное на многократное применение.

Пунктом 1 комментируемой статьи устанавливается, что законодательство РФ в области ПД основывается прежде всего на:

- Конституции РФ;
- международных договорах РФ.

Конституция РФ - это основной закон РФ. Конституция РФ имеет высшую юридическую силу, прямое действие и применяется на всей территории РФ. Законы и иные правовые акты, принимаемые в РФ, не должны противоречить Конституции РФ. Таким образом, правовую основу системы защиты ПД составляют положения Конституции РФ.

Международный договор РФ - это международное соглашение, заключенное РФ с иностранным государством (или государствами), с международной организацией либо с иным образованием, обладающим правом заключать международные договоры, в письменной форме и регулируемое международным правом, независимо от того, содержится такое соглашение в одном документе или в нескольких связанных между собой документах, а также независимо от его конкретного наименования. Согласно положениям Федерального закона от 15.07.1995 N 101-ФЗ "О международных договорах Российской Федерации" международные договоры образуют правовую основу межгосударственных отношений, содействуют поддержанию всеобщего мира и безопасности, развитию международного сотрудничества в соответствии с целями и принципами Устава Организации Объединенных Наций. Международным договорам принадлежит важная роль в защите основных прав и свобод человека, в обеспечении законных интересов государств. Международные договоры РФ наряду с общепризнанными принципами и нормами международного права являются в соответствии с Конституцией РФ составной частью ее правовой системы.

Практика заключения международных договоров показывает стремление стран соблюдать международные стандарты защиты ПД.

Следуем далее. Законодательство РФ в области ПД состоит из комментируемого Закона; других определяющих случаи и особенности обработки ПД федеральных законов.

Например, требования по защите ПД закреплены в разных кодексах РФ. Кодекс - это систематизированный законодательный акт, в котором содержатся нормы какой-либо отрасли права. Расположение правовых норм в кодексе производится в порядке, отражающем систему данной отрасли права.

Кодексы РФ, в которых закреплены положения о ПД:

- КоАП РФ (ст. 13.11. "Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)", ст. 5.39 "Отказ в предоставлении информации", ст. 13.14 "Разглашение информации с ограниченным доступом");
- ТК РФ (гл. 14 "Защита персональных данных работника" (ст. 85-90));
- Уголовный кодекс РФ от 13.06.1996 г. N 63-ФЗ (ст. 137 "Нарушение неприкосновенности частной жизни", ст. 272 "Неправомерный доступ к компьютерной информации", ст. 138 "Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений", ст. 140 "Отказ в предоставлении гражданину информации");
- Воздушный кодекс РФ от 19.03.1997 г. N 60-ФЗ (ст. 85.1 "Персональные данные пассажиров воздушных судов").

В качестве примера федеральных законов, определяющих случаи и особенности обработки ПД можно привести следующие:

- Федеральный закон от 27.07.2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон от 15.11.1997 г. N 143-ФЗ "Об актах гражданского состояния";
- Федеральный закон от 22.10.2004 г. N 125-ФЗ "Об архивном деле в Российской Федерации";
- Федеральный закон от 12.08.1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности";
- Федеральный закон от 12.06.2002 г. N 67-ФЗ "Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации;
- Основы законодательства РФ об охране здоровья граждан от 22.07.1993 г. N 5487-I;
- Федеральный закон от 01.04.1996 г. N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования";
- Федеральный закон от 08.08.2001 г. N 129-ФЗ "О государственной регистрации юридических лиц и индивидуальных предпринимателей"
- Закон РФ от 21.07.1993 г. N 5485-I "О государственной тайне";
- Закон РФ от 28.03.1998 г. N 53-ФЗ "О воинской обязанности и военной службе".

2. Главным нормативным правовым актом, регулирующим особенности обработки ПД, является комментируемый Закон. Пунктом 2 комментируемой статьи законодатель установил, что государственные органы в пределах своих полномочий могут принимать нормативные правовые акты по отдельным вопросам, касающимся обработки ПД. Такие нормативные акты должны отвечать следующим требованиям:

- они не могут содержать положения, ограничивающие права субъектов ПД;
- они подлежат официальному опубликованию, за исключением нормативных правовых актов или отдельных положений

таких нормативных правовых актов, содержащих сведения, доступ к которым ограничен федеральными законами.

В качестве примера можно привести следующие нормативные правовые акты:

- постановление Правительства РФ от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных";

- постановление Правительства РФ от 06.07.2008 N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";

- постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

- приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных";

- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 16.07.2010 г. N 482 "Об утверждении образца формы уведомления об обработке персональных данных".

3. Пунктом 3 комментируемой статьи устанавливается, что особенности обработки ПД, осуществляемой без использования средств автоматизации, могут быть установлены иными федеральными законами и иными нормативными правовыми актами. При этом должны учитываться положения комментируемого Закона.

В настоящее время особенности обработки ПД, осуществляемой без использования средств автоматизации, регулируются прежде всего постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации". Федеральным органам исполнительной власти было дано указание в месячный срок привести свои акты по вопросам обработки ПД, осуществляемой без использования средств автоматизации, в соответствие с указанным Постановлением. Постановление было официально опубликовано в "Собрании законодательства РФ", 22.09.2008, N 38 и "Российской газете", N 200, 24.09.2008. Постановление вступило в силу 24.10.2008 года. См. также комментарий к п. 9 ст. 3 Закона.

4. Согласно п. 4 комментируемой статьи прежде всего в области обработки и защиты ПД применяются правила международного договора. Поэтому если международным договором РФ установлены иные правила, чем те, которые предусмотрены комментируемым законом, применяются правила международного договора.

"В 60-х и 70-х годах с приходом информационных технологий стал возрастать интерес к приватности. Возможность использования мощных компьютеров для слежки и контроля означала необходимость принятия особых правил, регулирующих сбор и обработку персональных данных. Во многих странах новые конституции отразили это право. Процесс обновления законодательства в данной области можно проследить со времени появления первого закона о защите данных, изданного в Германии в земле Гессен в 1970 г. После этого были приняты законы в Швеции (1973), Соединенных Штатах (1974), Германии (1977) и Франции (1978)"*(3).

Основными международными законодательные актами в области защиты ПД являются следующие:

- Директива Организации по экономическому сотрудничеству и развитию о защите неприкосновенности частной жизни и международных обменов персональными данными;

- Международная конвенция "Об охране личности в отношении автоматизированной обработки персональных данных" 1981 г.;

- Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных;

- Конвенция Совета Европы N 108 о защите личности в связи с автоматической обработкой персональных данных;

- Директива 97/66/ЕС от 15 декабря 1997 г. по обработке персональных данных и защите конфиденциальности в телекоммуникационном секторе.

"Мировой опыт позволяет назвать три главные причины для принятия специальных законов о защите приватности и персональных данных:

Приведение законодательства значительного числа стран к общемировым цивилизованным стандартам, отражающим высокий уровень защиты прав человека. Многие государства, особенно в Центральной и Восточной Европе (включая Россию), Южной Африке и Южной Америке, приняли соответствующие законы, чтобы исправить последствия нарушений прав человека при тоталитарных режимах прошлых лет.

Создание благоприятных условий для развития электронного бизнеса. Многие страны, особенно в Азии, уже приняли (или разрабатывают) законы, направленные на развитие электронной коммерции. Правительства понимают, что в современном мире, насыщенном высокотехнологичными коммуникациями, персональные данные потребителей находятся под угрозой - особенно когда они пересылаются по Интернету. Поэтому в законах об электронном бизнесе появляются гарантии приватности.

Приведение национального законодательства в соответствие с европейскими соглашениями. Большинство стран Центральной и Восточной Европы принимает законы, основываясь на Конвенции Совета Европы 1981 года и Директиве Европейского Союза о защите данных. Многие из этих стран в ближайшем будущем надеются стать членами ЕС. В других регионах мира государства приводят свои законы в соответствие требованиям ЕС просто потому, что иначе могут пострадать их торговые отношения с членами Евросоюза"*(4).

Статьи об обмене информацией включаются и в международные договоры о правовой помощи, об избежание двойного налогообложения, о сотрудничестве в определенной общественной, культурной сфере и т.п.

Так, например, в ст. 25 Договора между Российской Федерацией и Соединенными Штатами Америки об избежании двойного налогообложения и предотвращении уклонения от налогообложения в отношении налогов на доходы и капитал от 17

июня 1992 г. указывается, что любая полученная договаривающимся государством информация будет считаться конфиденциальной в той же степени, что и информация, полученная в соответствии с национальным законодательством этого государства, и будет раскрыта только лицам или органам (включая суды и административные органы), связанным с исчислением, взиманием, управлением, принудительным взысканием или исполнением решений или рассмотрением заявлений в отношении налогов, на которые распространяется договор. Такие лица или органы будут использовать информацию только для этих целей. Они могут раскрывать эту информацию в ходе открытого судебного заседания или при принятии юридических решений.

В ст. 15 Договора между РФ и Республикой Индией о взаимной правовой помощи по уголовным делам от 21 декабря 1998 г. прописывается, что запрашиваемая сторона может потребовать, чтобы предоставленная информация или доказательства либо источник такой информации или доказательств сохранялись конфиденциальными или были раскрыты или использованы только на определенных ею условиях. Если запрашивающая сторона принимает эту информацию или доказательства на таких условиях, она будет их соблюдать. Кроме того запрашиваемая сторона должна будет по запросу и в запрошенном объеме сохранять конфиденциальность запроса, его содержания, прилагаемых документов и любого действия, предпринимаемого в соответствии с запросом. Если запрос не может быть исполнен без нарушения конфиденциальности, запрашиваемая сторона должна уведомить об этом запрашивающую сторону, которая решает, должен ли запрос, несмотря на это, быть исполнен.

Глава 2. Принципы и условия обработки персональных данных

Статья 5. Принципы обработки персональных данных

1. В комментируемой статье определены принципы обработки ПД.

Необходимо отметить, что общие принципы обработки ПД были сформулированы в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" (см. ст. 6 упомянутого документа). А согласно ст. 7 Директивы 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" государства-участники обязаны обеспечить, чтобы личные данные обрабатывались только в случаях, если:

- субъект данных недвусмысленно дал свое согласие;
- или обработка необходима для исполнения контракта, в котором субъект данных является стороной или для принятия мер до заключения контракта по просьбе субъекта данных;
- или обработка необходима для выполнения юридического обязательства, субъектом которого является контролер (физическое или юридическое лицо, официальный орган, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных);
- или обработка необходима для защиты жизненных интересов субъекта данных;
- или обработка необходима в целях обеспечения законных интересов контролера или третьей стороны (сторон), которым раскрыты данные, кроме случаев, когда такие интересы перекрываются интересами фундаментальных прав и свобод субъекта данных, защита которых требуется согласно п. 1 ст. 1 упомянутого документа (государства-участники защищают фундаментальные права и свободы физических лиц, и, в частности, их право на неприкосновенность частной жизни применительно к обработке персональных данных).

Итак, ПД должны обрабатываться в первую очередь на основе принципа законности целей и способов обработки ПД и добросовестности. Анализ норм комментируемого Закона позволяет сформулировать некоторые основные практические советы, которыми должен руководствоваться оператор при обработке ПД для соблюдения требований действующего законодательства:

- должна быть обеспечена конфиденциальность ПД;
- ПД не должны передаваться третьим лицам без согласия субъекта данных;
- ПД должны быть защищены от несанкционированного доступа и распространения;
- ПД должны использоваться только для тех целей, для которых они были собраны и храниться не дольше, чем это требуется для достижения целей обработки;
- обработка ПД возможна только при условии согласия субъекта;
- оператор должен направить уведомление об обработке ПД в Уполномоченный орган (за исключением ряда случаев, о которых будет рассказано в комментарии к п. 2 ст. 22 Закона), а также иметь документ, в котором отражена политика обработки ПД;
- субъект ПД должен иметь возможность знакомиться с данными о себе;
- оператор должен информировать граждан о факте обработки ПД, предоставлять сведения о целях и способах обработки;
- граждане имеют право требовать уточнения информации, а также блокирования и уничтожения неточных ПД;
- обработка специальных категорий ПД, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни допускается только в исключительных случаях и при соблюдении определенных условий.

Законодатель требует, чтобы ПД обрабатывались также с соблюдением принципа соответствия целей обработки ПД целям, заранее определенным и заявленным при сборе ПД, а также полномочиям оператора. Поэтому в организациях,

обрабатывающих ПД, целесообразно иметь документ, который будет отражать политику организации в отношении обработки ПД. Это может быть Положение об обработке персональных данных. Такой документ может определять:

- цели и способы обработки ПД;
- категории, типы обрабатываемых ПД;
- категории субъектов, ПД которых обрабатываются;
- правовое основание обработки ПД;
- перечень действий с ПД;
- условия прекращения обработки ПД;
- порядок получения доступа к ПД;
- условия раскрытия и объем ПД, доступных партнерам и третьим лицам;
- перечень лиц, ответственных за рассмотрение жалоб и запросов.

Примерный образец приказа об утверждении Положения о защите персональных данных работников

ООО "ГЕРДА-М"

Приказ N 35

5 мая 2010 г. г. Волгоград

Об утверждении Положения
о защите персональных данных работников

В целях обеспечения защиты персональных данных работников организации, в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных" и иными федеральными законами

приказываю:

1) утвердить Положение о защите персональных данных работников ООО "ГЕРДА-М";

2) ознакомить под роспись всех работников предприятия с текстом данного документа.

Директор _____ Петров С.В.

Примерный образец Положения об обработке персональных данных студентов

Положение
об обработке персональных данных студентов Уральского технологического института

1. Основные понятия.

1.1. Настоящее Положение (далее - Положение) разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом "Об информации, информационных технологиях и о защите информации", Федеральным законом "О персональных данных", Федеральным законом "Об образовании", Федеральным законом "О высшем и послевузовском профессиональном образовании", международными обязательствами Российской Федерации в сфере соблюдения прав граждан, Уставом Уральского технологического института (далее - Института), Правилами внутреннего распорядка Института и определяет принципы и порядок работы с информацией, содержащей персональные данные, с использованием информационных систем персональных данных Института (далее - ИСПДн Института).

1.2. Понятия, используемые в Положении:

- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), являющемуся работником Организации, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
- распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том

числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- использование персональных данных - действия (операции) с персональными данными, совершаемые работодателем в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работника или других лиц, либо иным образом затрагивающих права и свободы работника или других лиц;

- блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

- уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

- обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

- информационная система персональных данных - система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

- конфиденциальность персональных данных - обязательное для соблюдения работодателем или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия работника или наличия иного законного основания;

- общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами Российской Федерации не распространяется требование соблюдения конфиденциальности.

- Работники Организации - лица, имеющие трудовые отношения с Организацией, либо кандидаты на вакантную должность, вступившие с Организацией в отношения по поводу приема на работу.

- оператор - лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

2. Общие положения.

2.1. В настоящем Положении под субъектами персональных данных, данные которых предполагается обрабатывать в ИСПДн Института, понимаются студенты Института (далее - субъекты персональных данных).

2.2. Порядок ввода в действие и изменения Положения:

2.2.1. Настоящее Положение вступает в силу с момента его утверждения ректором Института и действует бессрочно, до замены его новым Положением.

2.2.2. Все изменения в Положение вносятся приказом ректора.

2.2.3. Контроль соблюдения требований настоящего Положения и контроль организационных мероприятий осуществляет Первый проректор Института. Контроль технологических и технических мероприятий, связанных с исполнением норм Федерального закона "О персональных данных" и настоящего Положения, осуществляет руководитель управления информатизации Института.

2.2.4. Все субъекты персональных данных должны быть ознакомлены с настоящим Положением под роспись.

2.2.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания или по истечении сроков их обработки, или продлевается на основании заключения экспертной комиссии Института, если иное не определено законом.

3. Цели и задачи обработки персональных данных в Институте.

3.1. Институт, являясь оператором персональных данных, определяет цели и содержание обработки персональных данных.

3.2.Обработка персональных данных в Институте осуществляется с целью содействия субъектам персональных данных в осуществлении учебной, научной, трудовой деятельности, обеспечения личной безопасности, учета результатов исполнения договорных обязательств, а также наиболее полного исполнения Институтом обязательств и компетенций в соответствии с Федеральными законами "Об образовании" и "О высшем и послевузовском профессиональном образовании".

3.3. Обработка персональных данных студентов Института осуществляется для решения следующих задач:

- учета информации о студенческом составе вуза и о движении студентов, информации об обучении;

- формирования отчетов по Институту;

- назначения и начисление стипендий и иных выплат;

- обработки данных приемной кампании Института, учета личных данных абитуриентов и участников централизованного тестирования, обработка результатов вступительных испытаний;

- обработки личных дел и индивидуальных планов аспирантов, соискателей и докторантов, анализ деятельности по подготовке и аттестации научных и научно-педагогических кадров;

- комплексного мониторинга деятельности Института, мониторинга качества учебного процесса;

- бухгалтерского учета и контроля финансово-хозяйственной деятельности Института и исполнения финансовых обязательств по заключенным договорам;

- обработки электронных библиотечных карт и читательских билетов, обеспечение учета книговыдачи;

- предоставления субъекту сведений об его обучении в Институте в период обучения и после него;

- поддержания контактов с законными представителями субъекта персональных данных;

- иных задач, необходимых для повышения качества и эффективности деятельности Института.

4. Состав персональных данных субъектов персональных данных, обрабатываемых в Институте.

4.1. Состав персональных данных, обрабатываемых в Институте, определяется настоящим Положением, а также "Перечнем персональных данных" и соответствует целям и задачам сбора, обработки и использования персональных данных в соответствии с разделом 3 настоящего Положения.

4.2. Перечень персональных данных, обрабатываемых в Институте утверждается ректором Института.

При добавлении новых информационных полей, содержащих персональные данные, в базы данных ИСПДн Института проводится дополнительное анкетирование субъектов персональных данных. Если субъект ранее дал согласие на обработку своих персональных данных с использованием автоматизированной информационной системы, то, заполняя дополнительную анкету, он дает согласие на обработку дополнительной информации персонального характера, перечень которой указан в анкете. Форма дополнительной анкеты разрабатывается отдельно и утверждается ректором Института.

5. Права субъектов персональных данных.

5.1. Субъект персональных данных своей волей и в своем интересе принимает решение о предоставлении своих персональных данных и дает согласие на их обработку.

5.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных по письменному заявлению на имя ректора Института с указанием причин отзыва. При подаче заявления необходимо предъявить основной документ удостоверяющий личность. После отзыва согласия все персональные данные, содержащиеся в ИСПДн с использованием средств автоматизации в течение трех дней уничтожаются без возможности восстановления, о чем субъект персональных данных уведомляется в письменной форме. Данные находящиеся на бумажных носителях передаются в архив и хранятся в течение сроков, установленных законодательством.

5.3. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными.

5.4. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

5.5. Сведения о персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

5.6. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при получении письменного запроса субъекта персональных данных или его законного представителя. Письменный запрос должен быть адресован на имя ректора Института, содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. При подаче заявления субъект персональных данных должен предъявить основной документ удостоверяющий личность для проверки сведений указанных в заявлении.

5.7. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований ФЗ "О персональных данных" или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

5.8. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6. Порядок сбора, хранения и использования персональных данных.

6.1. Сбор персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, настоящим Положением и приказами Института.

6.2. Информация персонального характера может быть получена непосредственно от субъекта персональных данных и только с его письменного согласия.

6.3. При необходимости сбора персональных данных законных представителей абитуриентов, обучающихся, выпускников законные представители должны дать письменное согласие на обработку их персональных данных.

6.4. Оператор не вправе требовать от субъекта персональных данных предоставления информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и о его частной жизни без его письменного согласия.

6.5. Согласие субъекта персональных данных не требуется получать в следующих случаях:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи;

- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии.

6.6. Субъекты персональных данных при получении от них согласия на обработку персональных данных в ИСПДн Института должны быть ознакомлены с перечнем собираемых и используемых сведений, с целями и задачами сбора, хранения и использования персональных данных.

6.7. Анкеты, содержащие информацию персонального характера, а также согласие на обработку персональных данных с использованием ИСПДн Института должны храниться в личном деле.

6.8. Ввод персональных данных в автоматизированные ИСПДн Института осуществляется сотрудником в соответствии с его должностными обязанностями. На бумажном носителе информации, содержащей персональные данные (анкеты, личные листки и др.) работник, осуществляющий ввод данных, оставляет отметку с информацией о должности, фамилии, имени, отчестве лица, осуществившего ввод данных, а также дату ввода информации.

6.9. Сотрудники, осуществляющие ввод и обработку данных с использованием автоматизированных ИСПДн Института, несут ответственность за полноту введенной информации и не должны вносить изменения, противоречащие информации, полученной непосредственно от субъекта персональных данных.

6.10. Персональные данные могут храниться в бумажном и(или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных. Право на обработку персональных данных предоставляется работникам структурных подразделений и(или) должностным лицам, определенным настоящим Положением, а также "Перечнем сотрудников, допущенных к обработке персональных данных", распорядительными документами или письменными указаниями ректора.

6.11. Хранение и обработка персональных данных в автоматизированных ИСПДн Института осуществляется на серверах _____ с использованием специализированного программного обеспечения, отвечающего требованиям информационной безопасности.

6.12. В случае если для научных, прикладных исследований, для решения задач статистики необходимо сохранить персональные данные, которые больше не используются в тех целях, ради которых они были собраны, эти данные могут сохраняться преимущественно в обезличенной форме в виде анонимных сведений.

6.13. На сайте Института могут быть размещены общедоступные персональные данные, перечень которых определяется настоящим Положением и согласием субъекта персональных данных на момент передачи в открытые источники.

7. Предоставление доступа сотрудников к персональным данным и передача персональных данных третьим лицам.

7.1. Право доступа к персональным данным субъектов персональных данных имеют:

- ректор Института и лица его замещающие;

- сотрудники бухгалтерии;

- сотрудники деканатов;

- кураторы учебных групп (списки студентов, информация о контактных телефонах студентов, либо при отсутствии телефона - информация о фактическом месте проживания);

- руководители и сотрудники структурных подразделений в соответствии со своим направлением деятельности;

- иные сотрудники Института, которым в соответствии с их должностными обязанностями требуется доступ к персональным данным субъектов персональных данных Института в соответствии с "Перечнем сотрудников, допущенных к обработке персональных данных".

7.2. Доступ сотрудников к персональным данным осуществляется по спискам, которые готовятся руководителями структурных подразделений и утверждаются ректором Института. Руководители структурных подразделений несут ответственность за необоснованную выдачу допуска сотрудникам своих подразделений.

7.3. Ознакомление лиц с персональными данными субъектов персональных данных Института должно осуществляться только по необходимости и в тех объемах, которые необходимы для выполнения возложенных на них функций.

7.4. Списки кураторов учебных групп ежегодно в срок до "___" _____ г. готовятся лицом, ответственным за проведение кураторской работы, и утверждаются ректором Института.

7.5. Порядок передачи информации, содержащей персональные данные, обрабатываемые Институтом, внутри Института определяется должностными обязанностями сотрудников или приказами (распоряжениями) по Институту.

7.6. В соответствии с законодательством Российской Федерации персональные данные, обрабатываемые Институтом, могут быть переданы правоохранительным, судебным органам и другим учреждениям, которые имеют на это право на основании федерального законодательства, а также в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороноспособности страны и безопасности государства без получения

согласия субъекта персональных данных.

7.7. Решение о передаче информации, содержащей персональные данные, обрабатываемые Институтом, третьим лицам, принимается ректором Института на основании их письменного запроса, если иное не предусмотрено договором или федеральным законодательством.

7.8. Передача информации третьей стороне возможна только при письменном согласии субъектов персональных данных.

8. Ответственность за нарушение требований настоящего положения.

8.1. Оператор, а также должностные лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Примерный образец Расписки об ознакомлении с Положением о защите персональных данных

Расписка
об ознакомлении с Положением о защите персональных данных

Я, Сидоров Иван Сергеевич, ознакомлен с Положением о защите персональных данных _____.
(название организации)

Дата _____
Подпись _____

При сборе ПД организациям следует определить, какая информация действительно нужна, а какие данные могут быть обезличены или уничтожены без ущерба для деятельности организации. Необходимо избегать сбора и хранения избыточной информации без определенной цели, не нужно собирать и использовать ПД для целей, которые не относятся к сфере компетенции организации.

Как указывается в абз. 3 п. 1 комментируемой статьи при обработке ПД оператор должен также учитывать принцип соответствия объема и характера обрабатываемых ПД, способов обработки ПД целям обработки ПД и принцип достоверности ПД, их достаточности для целей обработки и недопустимости обработки ПД, избыточных по отношению к целям, заявленным при сборе ПД.

Выше указывалось, что основные цели обработки ПД должны быть зафиксированы оператором в Положении об обработке ПД. В дальнейшем оператор не может требовать с гражданина предоставления информации, большего объема, чем это требуют цели обработки ПД, заявленные в упомянутом локальном документе.

Например, работодатели часто собирают о будущем сотруднике всю информацию, объясняя это тем, что хотят иметь максимально полное представление о нем. При этом часто работодатель переходит тонкую грань, отделяющую ПД от сведений, составляющих тайну частной жизни, личную или семейную тайну гражданина. Среди документов и материалов, содержащих информацию, которую желают получать работодатели, принимая гражданина на работу, основное место занимают:

- документы, предъявляемые при заключении трудового договора (см. ст. 65 ТК РФ);
- документы о состоянии здоровья работника, если в соответствии с законодательством он должен пройти предварительный и периодические медицинские осмотры;
- документы о составе семьи работника, необходимые для предоставления ему гарантий, связанных с выполнением семейных обязанностей;
- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (об инвалидности, донорстве, нахождении в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и др.);
- документ о беременности работницы и возрасте детей для предоставления матери установленных законом условий труда, гарантий и компенсаций.

Авторы полагают, что среди ПД работника должны быть:

- трудовой договор;
- приказ (распоряжение) о приеме на работу;
- приказы (распоряжения) об изменении условий трудового договора, его прекращении;
- приказы (распоряжения) о поощрениях и дисциплинарных взысканиях, примененных к работнику;
- трудовая книжка.

К составу персональных данных работника можно отнести сведения, предусмотренные унифицированной формой учета кадров Т-2, утвержденной постановлением Госкомстата РФ от 05.01.2004 N 1 "Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты".

К таким сведениям относятся:

- фамилия, имя, отчество;

- дата рождения;
- гражданство;
- номер страхового свидетельства;
- ИНН;
- знание иностранных языков;
- данные об образовании (номер, серия дипломов, год окончания);
- данные о приобретенных специальностях
- семейное положение;
- данные о членах семьи (степень родства, ФИО, год рождения, паспортные данные, включая прописку и место рождения);
- фактическое место проживания;
- контактная информация;
- данные о военной обязанности;
- данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения, сведения о поощрениях, данные о повышении квалификации и т.п.).

Для того чтобы установить, в каком объеме работодатель вправе получать от работника ПД, необходимо обратить внимание на очень важное ограничение - это целевой характер использования персональных данных. Таким образом, обработка ПД может производиться исключительно в целях, указанных в п. 1 ст. 86 ТК РФ, а именно для обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Для осуществления разных целей обработки ПД следует использовать разные базы данных. В организациях, обрабатывающих ПД, целесообразно также установить правила целевого использования баз данных и своевременно вносить изменения в случае отзыва согласия на использование баз данных в оговоренных целях. Необходимо избегать объединения баз данных, созданных для несовместимых целей, в соответствии с принципом обработки ПД, указанном в абзаце 5 п. 1 комментируемой статьи.

2. В п. 2 комментируемой статьи определены общие правила хранения ПД:
- хранение ПД должно осуществляться в форме, позволяющей определить субъекта ПД;
- хранение ПД должно осуществляться не дольше, чем этого требуют цели их обработки;
- хранение ПД прекращается, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Примерный образец уведомления об уничтожении персональных данных

Уведомление
об уничтожении персональных данных

Г-ну Плотникову С.И.,
проживающему по адресу:
г. Тюмень, ул. Крылова,7-90

Сообщаем Вам, что в связи с достижением цели обработки обработка Ваших персональных данных, а именно _____ _____.
(перечислить персональные данные)
прекращена, и Ваши персональные данные будут уничтожены "___" _____ 20__ г.

Дата
Подпись должностного лица организации

Статья 6. Условия обработки персональных данных

1. Пункт 1 комментируемой статьи предоставляет оператору право обрабатывать ПД при условии получения согласия субъекта ПД на такую обработку. Субъект ПД должен принять решение о предоставлении своих ПД и дать согласие на их обработку своей волей и в своем интересе. При этом согласие на обработку ПД может быть отозвано субъектом ПД. Оператору ПД следует учитывать, что обязанность предоставить доказательство получения согласия гражданина на обработку его ПД, а в случае обработки общедоступных ПД обязанность доказывания того, что обрабатываемые ПД являются общедоступными,

возлагается на оператора. По мнению авторов, для обработки ПД достаточно устного согласия субъекта, за исключением случаев, когда необходимо получить письменное согласие субъекта ПД (п. 4 ст. 9 Закона).

Гражданам, перед тем как передать свои ПД банку, магазину, любой другой организации, оказывающей услуги, следует выяснить:

- для чего собирается эта информация и как она будет использована;
- как и где ПД будут храниться (в электронной базе данных, в Интернет, на бумажных носителях и т.п.);
- кто сможет получить доступ к ПД, кому они могут передаваться;
- как долго будут храниться ПД.

Если гражданином выяснено, что его ПД могут быть использованы не только для получения услуг, которые он желает, но и для иных целей, он вправе ограничить свое согласие на обработку данных только в четко определенных целях. Например, устраиваясь на работу и проходя собеседование, гражданин может возражать против проведения видеозаписи собеседования. При этом работодатель на этом основании не вправе отказать ему в приеме на работу.

С того момента, как любое лицо обратилось к гражданину с просьбой о предоставлении информации, и на протяжении всего периода, пока оно хранит сведения о гражданине, это лицо обязано соблюдать требования комментируемого Закона.

2. В некоторых случаях обработка ПД может происходить без предварительного согласия на то субъекта ПД. Рассмотрим эти случаи:

Во-первых, обработка ПД без согласия субъекта ПД может осуществляться на основании федерального закона, устанавливающего ее цель, условия получения ПД и круг субъектов, ПД которых подлежат обработке, а также определяющего полномочия оператора. Так, например, с 01.07.2009 г. общества с ограниченной ответственностью обязаны вести списки участников общества. Внесение сведений об участнике в такой список может, по мнению авторов, происходить без согласия субъекта ПД, т.к. обработка ПД в этом случае осуществляется на основании федерального закона.

Во-вторых, обработку ПД разрешается производить без согласия субъекта ПД, когда такая обработка необходима в связи с реализацией международных РФ о реадмиссии. Этот пункт статьи был введен Федеральным законом от 25.11.2009 N 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных" по вопросам реализации международных договоров Российской Федерации о реадмиссии". Реадмиссией называется согласие государства на прием обратно на свою территорию своих граждан (а также, в некоторых случаях, иностранцев, прежде находившихся или проживавших в этом государстве), которые подлежат депортации из другого государства.

В-третьих, обработка ПД будет происходить без согласия субъекта ПД, когда она осуществляется в целях исполнения договора, одной из сторон которого является субъект ПД. Так, например, в Постановлении Девятого арбитражного апелляционного суда (дело N 09АП-13027/2007-ГК) указывается, что по общему правилу (п. 1 ст. 6 Закона) обработка данных возможна только с согласия субъекта ПД, однако перечень исключений из этого правила содержится в п. 2 ст. 6 Закона, который допускает обработку ПД без согласия субъекта, если такая обработка проводится в целях исполнения договора, одной из сторон которого является субъект. Поэтому на обработку сведений об абоненте, использующихся для идентификации в целях исполнения договора возмездного оказания услуг связи, согласия субъекта не требуется.

Также по мнению Иванова Н.С., "заключая кредитный договор и предоставляя банку свои паспортные данные и иные сведения о себе, тем самым гражданин дает и свое письменное согласие на обработку банком своих персональных данных. При этом выполняются п. 1 ст. 9 Закона ("субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе") и частично п. 4 ст. 9 Закона ("в случаях, предусмотренных настоящим Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных")"*(5).

Трудовое законодательство, также обязывает поступающего на работу гражданина, предоставить работодателю следующие документы, содержащие ПД будущего работника (ст. 65 ТК РФ):

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки.

В-четвертых, если обработка ПД осуществляется для статистических или иных научных целей при условии обязательного обезличивания ПД, то согласия субъекта на такую обработку также не обязательно получать. Например, при составлении статотчетность о численности и фонде оплаты труда, бухгалтер не обязан получать на согласие на обработку таких ПД, т.к. по таким данным нельзя идентифицировать конкретного человека.

В-пятых, без согласия субъекта ПД осуществляется обработка ПД, необходимая для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПД. Однако отсутствие согласия на такую обработку будет правомерным только в том случае, если получение согласия субъекта ПД невозможно. Типичным примером может служить обработка ПД гражданина лечебным учреждением, куда гражданин доставлен в бессознательном состоянии.

В-шестых, обработка ПД без согласия производится:

- для доставки почтовых отправлений организациями почтовой связи;
- для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также

для рассмотрения претензий пользователей услугами связи.

Порядок доставки почтовых отправлений регулируется Федеральным законом от 17.07.1999 N 176-ФЗ "О почтовой связи". Почтовая связь - это вид связи, представляющий собой единый производственно-технологический комплекс технических и транспортных средств, обеспечивающий прием, обработку, перевозку, доставку (вручение) почтовых отправлений, а также осуществление почтовых переводов денежных средств. Услуги почтовой связи - это действия или деятельность по приему, обработке, перевозке, доставке (вручению) почтовых отправлений, а также по осуществлению почтовых переводов денежных средств. Организациями федеральной почтовой связи называются организации почтовой связи, являющиеся государственными унитарными предприятиями и государственными учреждениями, созданными на базе имущества, находящегося в федеральной собственности. В соответствии со ст. 15 упомянутого Закона тайна переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи, гарантируется государством. Осмотр и вскрытие почтовых отправлений, осмотр их вложений, а также иные ограничения тайны связи допускаются только на основании судебного решения. Все операторы почтовой связи обязаны обеспечивать соблюдение тайны связи. Информация об адресных данных пользователей услуг почтовой связи, о почтовых отправлениях, почтовых переводах денежных средств, телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые отправления, переводимые денежные средства, телеграфные и иные сообщения являются тайной связи и могут выдаваться только отправителям (адресатам) или их представителям.

Порядок предоставления услуг электросвязи регулируется Федеральным законом от 07.07.2003 N 126-ФЗ "О связи". Так, оператором связи является юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии. Средствами связи называются технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи. В соответствии с положениями ст. 63 ФЗ "О связи" на территории РФ гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами. Операторы связи обязаны обеспечить соблюдение тайны связи. Осмотр почтовых отправлений лицами, не являющимися уполномоченными работниками оператора связи, вскрытие почтовых отправлений, осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда, за исключением случаев, установленных федеральными законами. Сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только отправителям и получателям или их уполномоченным представителям, если иное не предусмотрено федеральными законами.

Однако операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, информацию о пользователях услугами связи и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами.

Авторы обращают внимание на то, что норма права, разрешающая без согласия клиента обрабатывать ПД в целях доставки почтовых отправлений организациями почтовой связи, осуществления операторами электросвязи расчетов за оказанные услуги связи, а также рассмотрения претензий абонентов внесена Постановлением Правительства РФ от 16.02.2008 N 93 "О внесении изменений в некоторые Постановления Правительства Российской Федерации по вопросам оказания услуг связи" во все правила оказания услуг связи и действует с марта 2008 г.

В-седьмых, без согласия субъекта может осуществляться обработка ПД в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности. Однако при этом, операторы ПД не должны нарушать права и свободы субъектов ПД.

В качестве примера можно привести Определение Верховного Суда РФ от 27.02.2008 N 3-Г08-3, в котором указывается, что аккредитация журналиста при органах, организациях и учреждениях непосредственно связана с его профессиональной деятельностью по поиску, получению и распространению информации и поэтому в соответствии с абзацем 6 п. 2 ст. 6 комментируемого Закона необходимый для реализации требований ст. 48 ФЗ "О средствах массовой информации" минимум ПД журналиста может передаваться в орган, осуществляющий его аккредитацию, и без согласия этого журналиста.

Наконец, в-восьмых, осуществляется без согласия субъектов ПД обработка ПД, подлежащих опубликованию в соответствии с федеральными законами, в том числе ПД, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Так, в избирательном процессе ПД кандидатов предоставляются прежде всего Центральной избирательной комиссии. Согласно ст. 38 Федерального закона от 18.05.2005 N 51-ФЗ "О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации" федеральный список кандидатов представляется уполномоченным представителем политической партии в Центральную избирательную комиссию РФ. При этом в федеральном списке кандидатов указываются, в частности, следующие ПД кандидатов:

- фамилия, имя и отчество;

- дата и место рождения;
- адрес места жительства;
- серия, номер и дата выдачи паспорта или документа, заменяющего паспорт гражданина, наименование или код органа, выдавшего паспорт или документ, заменяющий паспорт гражданина;
- образование и др.

Центральная избирательная комиссия РФ заверяет и регистрирует федеральные списки кандидатов, публикует зарегистрированные федеральные списки кандидатов, при этом не публикуются следующие сведения о каждом из кандидатов:
- адрес места жительства в части наименования улицы, номера дома и квартиры;
- серия, номер и дата выдачи паспорта или документа, заменяющего паспорт гражданина;
- наименование или код органа, выдавшего паспорт или документ, заменяющий паспорт гражданина.

3. Нужно обратить внимание на то, что порядок и условия обработки специальных категорий ПД, а также биометрических ПД устанавливаются соответственно ст. 10, 11 комментируемого Закона.

В специальную категорию ПД входят данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. К биометрическим ПД относятся сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность

4. Особые требования законодатель предъявляет к операторам, которые поручают обработку ПД другим лицам на основании договора. Существенным условием такого договора будет являться обязанность обеспечения указанным лицом конфиденциальности ПД и безопасности ПД при их обработке. При такой передаче ПД третьим лицам ответственность за ПД сохраняется и у оператора и у сторонней организации. Поэтому в договоре между этими сторонами должны быть указаны методы, способы защиты информации для каждой из сторон. В организации, которой по договору передаются для обработки ПД, необходимо разработать меры по обеспечению конфиденциальности ПД. Они могут включать в себя ограничение числа работников, имеющих доступ к ПД, охрану помещений и т.д.

Ю.А. Васильева указывает, что "если управляющая организация планирует воспользоваться услугами информационно-расчетного центра, ей следует получить согласие собственников помещений на передачу их персональных данных для целей расчета платы за жилое помещение коммунальные услуги. Согласие граждан на обработку их персональных данных расчетно-кассовым центром не требуется в случае, когда центр получает их непосредственно от граждан, а не от управляющей организации. Однако жилищное законодательство исключает такой вариант, поскольку у граждан нет никаких правоотношений с информационно-расчетными центрами. В договоре между управляющей организацией и расчетным центром должно быть обязательно указано условие об обеспечении конфиденциальности данных*(6)".

Статья 7. Конфиденциальность персональных данных

1. Пунктом 1 комментируемой статьи на операторов персональных данных и третьих лиц возлагается обязанность по обеспечению конфиденциальности персональных данных в процессе их обработки. Напоминаем, что под оператором персональных данных понимается государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

В общем смысле под конфиденциальностью информации следует понимать обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Согласно п. 10 ст. 3 комментируемого Закона конфиденциальностью персональных данных называется обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания. Таким образом требование о конфиденциальности персональных данных связано прежде всего с ограничением на распространение персональных данных без согласия субъекта персональных данных. Однако необходимо учитывать, что в ряде случаев согласия субъекта на обработку персональных данных все же не требуется (п. 2 ст. 6, п. 2 ст. 9 комментируемого Закона).

Важно знать, что Указом Президента РФ от 06.03.1997 N 188 "Об утверждении Перечня сведений конфиденциального характера" определен перечень сведений конфиденциального характера.

Так, согласно ст. 9 Федерального закона от 20.08.2004 N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" орган, осуществляющий меры безопасности (перечень органов указан в ст. 3 упомянутого Закона), может наложить запрет на выдачу сведений о защищаемом лице из государственных и иных информационно-справочных фондов, а также может своим решением изменить номера его телефонов и государственные регистрационные знаки, используемых им, или принадлежащих ему транспортных средств.

Статья 61 Основ законодательства РФ об охране здоровья граждан относит информацию о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, к врачебной тайне. При этом на врачей законом накладывается обязанность подтвердить гражданину гарантию конфиденциальности передаваемых им сведений. Как указывается в абз. 3 вышеупомянутого нормативно-правового акта передача сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в интересах обследования и лечения пациента, для проведения научных исследований, публикации в научной литературе, использования этих сведений в учебном процессе и в иных целях допускается, но лишь с согласия гражданина, чьи персональные данные планируется обрабатывать.

В ряд случаев в медицинских учреждениях сведения, составляющие врачебную тайну, могут быть переданы третьим лицам без согласия гражданина или его законного представителя. Например, это станет возможным в целях обследования и лечения гражданина, не способного из-за своего состояния выразить свою волю, или при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений, или по запросу органов дознания и следствия и суда в связи с проведением расследования или судебным разбирательством, или при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий и т.п.

Абзацем 2 ст. 16 Основ законодательства РФ о нотариате на нотариуса возлагается обязанность хранить в тайне сведения, которые стали ему известны в связи с осуществлением его профессиональной деятельности. Освободить нотариуса от этой обязанности может только суд и только в том случае, если против нотариуса возбуждено уголовное дело в связи с совершением нотариального действия.

Практикующие адвокаты также обязаны хранить сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. Статья 8 Федерального закона от 31.05.2002 N 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" называет такие сведения адвокатской тайной. Так, адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием. Кроме того проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается только на основании судебного решения. Следует также учитывать, что право адвоката собирать сведения, необходимые для оказания юридической помощи, и обязанность соответствующего органа предоставить такую информацию не распространяются на конфиденциальные сведения.

Так, например, определением Верховного Суда РФ от 12.05.2010 N 49-В10-5 отказано в удовлетворении заявления о признании неправомерными действий миграционного органа по отказу в предоставлении по запросу адвоката адресной справки на гражданина, т.к. у адвоката отсутствуют законные основания для получения такой конфиденциальной информации.

Федеральным законом от 07.07.2003 N 126-ФЗ "О связи" в РФ обеспечивается тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Согласно п. 3 ст. 63 упомянутого выше закона осмотр почтовых отправлений лицами, не являющимися уполномоченными работниками оператора связи, вскрытие почтовых отправлений, осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда, за исключением ряда особых случаев. Важно учитывать, что сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только отправителям и получателям или их уполномоченным представителям.

По мнению авторов, для эффективного обеспечения конфиденциальности персональных данных операторами и третьими лицами, получающими доступ к персональным данным, в организациях необходимо разрабатывать качественную и действенную систему мер по предотвращению утечки охраняемой информации.

2. Законодатель делает исключение из условия о конфиденциальности персональных данных для общедоступных и обезличенных персональных данных.

Авторы напоминают, что персональные данные могут называться обезличенными тогда, когда невозможно определить принадлежность персональных данных конкретному субъекту персональных данных. Например, статистическая отчетность о численности и фонде оплаты труда, передаваемая бухгалтером в органы статистики содержит обезличенные персональные данные, т.к. эти сведения нельзя соотнести ни с одним конкретным работником.

Под общедоступными понимаются такие персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности. Простым примером общедоступных персональных данных являются сведения, размещенные в различных справочниках, адресных книгах.

Статья 8. Общедоступные источники персональных данных

1.Анализ п. 1 комментируемой статьи позволяет прийти к выводу, что общедоступные источники персональных данных должны обладать следующими признаками:

- доступ к общедоступным источникам персональных данных должен быть неограничен;
- они могут быть использованы любыми людьми по их усмотрению.

В настоящее время к таким общедоступным источникам персональных данных можно отнести следующие:

- различные справочники, издаваемые в печатном или электронном виде, либо размещаемые в сети Интернет;
- адресные книги;
- энциклопедии;
- различные базы данных, накапливаемые в библиотеках, архивах, органах государственной власти и местного самоуправления и т.п.

Следует знать, что согласно ст. 7 Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Важным

моментом является указание в законе на то, что обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Закон позволяет включать в общедоступные источники персональных данных следующие сведения о гражданах:

- фамилия, имя, отчество гражданина;
- год и место рождения гражданина;
- адрес гражданина;
- абонентский номер;
- иные сведения о гражданине.

Однако все вышеуказанные сведения могут включаться в общедоступные источники персональных данных только с согласия субъекта персональных данных. При этом обязанность доказывания того, что такое согласие получено, возложена на оператора персональных данных. Таким образом, оператору необходимо позаботиться о получении от субъекта персональных данных письменного согласия на использования сведений о нем в общедоступном источнике информации.

Примерный образец согласия работника на включение сведений о нем в общедоступный источник персональных данных.

Согласия на включение персональных данных в корпоративный справочник

Я, Лаврентьев Иван Александрович, менеджер ООО "Сигма", согласен на включение моих персональных данных, а именно:

1) фамилии, имени, отчества;
2) должности;
3) года и места рождения;
4) сведений об образовании и профессии;
5) сведений о месте жительства

в корпоративный справочник ООО "Сигма".

Дата
Подпись

Похожая норма права закреплена также в п. 2 ст. 53 Федерального закона от 07.07.2003 N 126-ФЗ "О связи". Так, операторам связи разрешено использовать созданные ими базы данных об абонентах для осуществления информационно-справочного обслуживания, в том числе для подготовки и распространения информации различными способами, в частности на магнитных носителях и с использованием средств телекоммуникаций. При этом при подготовке данных для информационно-справочного обслуживания могут быть использованы фамилия, имя, отчество абонента-гражданина и его абонентский номер, наименование (фирменное наименование) абонента, являющегося юридическим лицом, указанные им абонентские номера и адреса установки оконечного оборудования. Однако вышеупомянутый закон запрещает включать в данные для информационно-справочного обслуживания сведения об абонентах-гражданах без их письменного на то согласия.

2. Так как включение в общедоступные источники информации сведений о гражданине возможно только с его согласия, то субъект персональных данных имеет право в любое время потребовать исключения своих персональных данных из таких общедоступных источников, особенно, если они туда попали без согласия этого гражданина. Кроме того удаление сведений о субъекте персональных данных может произойти по решению суда или уполномоченного на то государственного органа.

Примерный образец требования об исключении персональных данных из адресного справочника

Г-ну Федорову М.Н.,
владельцу веб сайта www._____.ru

Требование
об исключении персональных данных из адресного справочника

5 мая 2010 г. я обнаружил свои персональные данные, а именно фамилию, имя, отчество, год рождения и адрес моего проживания в адресном справочнике г. Магнитогорска, расположенном в Интернете на Вашем сайте www._____ru.

Уведомляю Вас, что своего согласия на включение моих персональных данных в указанный выше адресный справочник я никогда не давал.

Таким образом, в соответствии со ст. ФЗ "О персональных данных" прошу Вас в срок до 20 мая 2010 г. исключить мои

персональные данные из адресного справочника. В случае невыполнения моих требований я буду вынужден обратиться за защитой моих прав в суд.

Дата
Подпись

Примерный образец искового заявления об исключении персональных данных из адресного справочника

В Правобережный районный суд г. Магнитогорска
Истец: Петров В.Г.
Адрес: г. Магнитогорск, пр. К. Маркса, 145-90
Ответчик: Федоров М.Н.
Адрес: г. Магнитогорск, пр. К. Маркса, 30-5

Исковое заявление
об исключении персональных данных из адресного справочника

5 мая 2010 г. я обнаружил свои персональные данные, а именно фамилию, имя, отчество, год рождения и адрес моего проживания в адресном справочнике г. Магнитогорска, расположенном в Интернете на сайте www._____ru. При этом своего согласия на включение моих персональных данных в адресный справочник я никогда не давал.

10 мая 2010 г. я обратился к владельцу вышеуказанного веб-сайта, г-ну Федорову М.Н., с просьбой исключить мои персональные данные из справочника, но он ответил мне отказом.

На основании вышеизложенного и руководствуясь ст. 6, 8 ФЗ "О персональных данных", ст. 151 ГК РФ, ст. 3 ГПК РФ

прошу:

Обязать ответчика исключить мои персональные данные из адресного справочника, находящегося в Интернете на сайте www._____ru.

Приложение:

1) квитанция об оплате государственной пошлины;
2) копия обращение на имя директора Федорова М.Н. от 10.05.2010 г.

Дата Подпись

В случае удовлетворения требований истца, ему будет выдано решение суда об исключении персональных данных заявителя из указанного им общедоступного источника информации. Напоминаем, что под решением суда следует понимать постановление суда первой инстанции, которым дело разрешается по существу, и принимаемым именем РФ. Решения суда вступают в законную силу по истечении срока на апелляционное или кассационное обжалование, если они не были обжалованы. Авторы напоминают, что в случае подачи апелляционной жалобы решение мирового судьи вступает в законную силу после рассмотрения районным судом этой жалобы, если обжалуемое решение суда не отменено. Если решением районного суда отменено или изменено решение мирового судьи и принято новое решение, оно вступает в законную силу немедленно. В случае подачи кассационной жалобы решение суда, если оно не отменено, вступает в законную силу после рассмотрения дела судом кассационной инстанции.

Статья 9. Согласие субъекта персональных данных на обработку своих персональных данных

1. Как упоминалось ранее, обработка ПД возможна только при условии согласия субъекта ПД, за исключением ряда случаев, перечисленных в п. 2 ст. 6 комментируемого Закона. Из содержания статьи следует, что согласие может быть дано как в устной так и в письменной форме. При этом субъекту ПД предоставляется право в любое время отозвать свое согласие на обработку ПД. По мнению авторов, из смысла анализируемого пункта статьи 9 Закона усматривается, что субъект ПД не обладает правом требовать прекращения обработки своих ПД в тех случаях, когда его согласия на обработку ПД в соответствии с Законом не требуется. В комментируемом Законе не указывается, в какой форме субъекту ПД следует предоставлять отзыв согласия на обработку ПД. Вероятней всего он должен быть в той же форме, в какой было подано заявление о согласии на обработку ПД.

Примерная форма отзыва согласия на обработку ПД

_____

Наименование (Ф.И.О.) оператора

_____

Адрес оператора

_____

Ф.И.О. субъекта персональных данных

_____

Адрес, субъекта персональных данных

_____

Номер основного документа, удостоверяющего его личность

_____

Дата выдачи указанного документа

_____

Наименование органа, выдавшего документ

Отзыв согласия на обработку персональных данных

Прошу Вас прекратить обработку моих персональных данных в связи с:

_____

(указать причину, например, "в связи неправомерным их использованием".)

"__" _____ 20__ г. _____ _____

Дата
Подпись

2. В пункте 2 комментируемой статье определяется перечень случаев, когда предоставления субъектом ПД своих данных уполномоченному органу, лицу или организации является обязательным. Это может потребоваться:

- в целях защиты основ конституционного строя;
- в целях защиты нравственности, здоровья, прав и законных интересов других лиц;
- в целях обеспечения обороны страны и безопасности государства.

Конституционный строй - это определенная форма, определенный способ организации государства, закрепленный в его конституции. Конституционный строй характеризуется основными принципами, лежащими в основе взаимоотношений человека, общества и государства.

Под основами конституционного строя следует понимать находящуюся под защитой государства систему принципов, определяющих и регламентирующих общественные отношения, являющиеся объектом конституционно-правового регулирования. Основы конституционного строя РФ закреплены в гл. 1 Конституции РФ.

В соответствии со ст. 2 Конституции РФ человек, его права и свободы признаются высшей ценностью. При этом признание, соблюдение и защита прав и свобод человека и гражданина является обязанностью государства. Однако согласно ст. 55 Конституции РФ права и свободы человека и гражданина все-таки могут быть ограничены федеральным законом, но только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Так, например, ст. 13 УПК РФ установлено, что ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения. Наложение ареста на почтовые и телеграфные отправления и их выемка в учреждениях связи, контроль и запись телефонных и иных переговоров, получение информации о соединениях между абонентами и (или) абонентскими устройствами могут производиться также только на основании судебного решения.

Кроме того, ст. 6 федерального закона от 12.08.1995 N 144-ФЗ "Об оперативно-розыскной деятельности" предусмотрено, что при осуществлении оперативно-розыскной деятельности возможно проведение таких оперативно-розыскных мероприятий, связанных с получением ПД, как:

- опрос;
- наведение справок;
- исследование предметов и документов;
- наблюдение;
- отождествление личности;
- контроль почтовых отправлений, телеграфных и иных сообщений;
- прослушивание телефонных переговоров;
- снятие информации с технических каналов связи;
- оперативное внедрение;
- оперативный эксперимент и т.п.

Но важно помнить, что проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения и при наличии следующей информации:

- о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно;
- о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно;
- о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации.

Прослушивание телефонных и иных переговоров допускается только в отношении лиц, подозреваемых или обвиняемых в совершении преступлений средней тяжести, тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях. Фонограммы, полученные в результате прослушивания телефонных и иных переговоров, хранятся в опечатанном виде в условиях, исключающих возможность их прослушивания и тиражирования посторонними лицами. В случае возбуждения уголовного дела в отношении лица, телефонные и иные переговоры которого прослушиваются, фонограмма и бумажный носитель записи переговоров передаются следователю для приобщения к уголовному делу в качестве вещественных доказательств. Дальнейший порядок их использования определяется уголовно-процессуальным законодательством РФ.

Кроме того, в случае возникновения угрозы жизни, здоровью, собственности отдельных лиц по их заявлению или с их согласия в письменной форме разрешается прослушивание переговоров, ведущихся с их телефонов, на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность, с обязательным уведомлением соответствующего суда (судьи) в течение 48 часов.

Следуем далее. В ст. 1 Закона РФ от 05.03.1992 N 2446-I "О безопасности" дается определение понятию "безопасности". Под безопасностью понимается состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. К основным объектам безопасности относятся:

- личность, ее права и свободы;
- общество - его материальные и духовные ценности;
- государство - его конституционный строй, суверенитет и территориальная целостность.

При обеспечении безопасности не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных законами. Должностные лица, превысившие свои полномочия в процессе деятельности по обеспечению безопасности, несут ответственность в соответствии с законодательством.

Федеральный закон от 03.04.1995 N 40-ФЗ "О Федеральной службе безопасности" также устанавливает, что проведение контрразведывательных мероприятий, ограничивающих права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, допускается только на основании постановления судьи. А проведение мероприятий по борьбе с терроризмом, ограничивающих права граждан на неприкосновенность жилища, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений граждан, допускается только на основании постановления судьи, получаемого в порядке, предусмотренном для получения судебного решения о допустимости проведения контрразведывательных мероприятий, ограничивающих конституционные права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, на неприкосновенность жилища, и на основании мотивированного ходатайства руководителя органа по борьбе с терроризмом или его заместителя.

Также Закон РФ от 18.04.1991 N 1026-I "О милиции" позволяет этому органу для выполнения возложенных на нее обязанностей осуществлять, в частности, такие действия, как:

- проверять документы, удостоверяющие личность, у граждан, если имеются достаточные основания подозревать их в совершении преступления или полагать, что они находятся в розыске, либо имеется повод к возбуждению в отношении их дела об административном правонарушении;
- осуществлять в порядке, установленном в соответствии с законодательством об административных правонарушениях, личный досмотр граждан, досмотр находящихся при них вещей при наличии достаточных данных полагать, что граждане имеют при себе оружие, боеприпасы, взрывчатые вещества, взрывные устройства, наркотические средства или психотропные вещества;
- получать от граждан и должностных лиц необходимые объяснения, сведения, справки, документы и копии с них и т.д.

Но необходимо учитывать, что милиция не имеет права собирать, хранить, использовать и распространять информацию о частной жизни лица без его согласия, за исключением случаев, предусмотренных федеральными законами. Кроме того сотрудники милиции обязаны обеспечить лицу возможность ознакомления с документами и материалами, в которых непосредственно затрагиваются его права и свободы, если иное не предусмотрено федеральными законами.

3. Законодатель возлагает на оператора ПД обязанность доказывания того, что субъект ПД дал свое согласие на обработку его данных. Если оператор обрабатывал без согласия субъекта ПД его данные, находящиеся в общедоступном источнике информации, оператор будет обязан доказать, что такие ПД действительно являлись общедоступными. Предоставление упомянутых выше доказательств может потребоваться, например, в случае судебного разбирательства

Поэтому, авторы считают очень важным включать соответствующую информацию о целях и способах обработки ПД в

текст анкеты, бланка, запроса, договора. Если организация собирает данные для передачи третьим лицам - необходимо получить специальное согласие на это у субъекта ПД до того, как ПД будут переданы. Обращаем внимание на то, что если организация получила ПД субъекта не от него самого или возникла необходимость использовать данные субъекта для целей, которые не были согласованы заранее, необходимо направить субъекту данных уведомление об обработке ПД, которое будет включать следующую информацию:

- наименование и адрес оператора ПД;
- цель обработки ПД;
- предполагаемые пользователи ПД;
- права субъекта ПД.

Очень важно учитывать то, что если организация планирует использовать ПД сразу для нескольких целей, то в этом случае следует запрашивать согласие субъекта ПД на каждый случай отдельно. В любом случае согласие на обработку ПД не должно быть вынужденным. Субъект ПД всегда должен иметь возможность отказаться от использования его данных во вторичных целях, не отказываясь при этом от получения услуг. Целесообразно включать в анкету или уведомление о порядке обработки и использования ПД пунктов, в соответствии с которыми у гражданина берется согласие на использование данных во вторичных целях, например: "я хочу получать рекламную информацию", "не возражаю, против получения новых предложений об участии в опросах компании" и т.п.

Как упоминалось ранее, согласно абз. 2 п. 2 ст. 6 комментируемого Закона, согласие субъекта ПД на обработку ПД не требуется, если обработка ПД осуществляется в целях исполнения договора, одной из сторон которого является субъект ПД. Таким образом, оператору ПД следует составлять договор с субъектом ПД (например, об оказании услуг) таким образом, чтобы из него явно усматривалось, что предоставление и обработка определенных ПД необходима в связи с исполнением такого договора. В качестве альтернативного варианта, по мнению авторов, оператор может получить письменное согласие от субъекта ПД на обработку данных для того, чтобы имелись соответствующие доказательства на случай спорных ситуаций, даже если письменная форма такого согласия является необязательной в соответствие с комментируемым Законом.

Примерный образец согласия пациента на обработку ПД медицинским учреждением

Согласие на обработку персональных данных медицинским учреждением

Я, Крылов Владимир Сергеевич, проживающий по адресу г. Волгоград, ул. Зеленая, 8, в соответствии с требованиями статьи 9 Федерального закона от 27.07.06 г. "О персональных данных" N 152-ФЗ, подтверждаю свое согласие на обработку Медицинским центром "Здоровье-плюс" (далее - Оператор) моих персональных данных, включающих:

- фамилию, имя, отчество;
- пол;
- дату рождения;
- адрес проживания;
- контактный телефон;
- реквизиты полиса ОМС (ДМС);
- страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС);
- данные о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью.
- в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

В процессе оказания Оператором мне медицинской помощи я предоставляю право медицинским работникам, передавать мои персональные данные, содержащие сведения, составляющие врачебную тайну, другим должностным лицам Оператора, в интересах моего обследования и лечения.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов) по ОМС (договором ДМС).

Оператор имеет право во исполнение своих обязательств по работе в системе ОМС (по договору ДМС) на обмен (прием и передачу) моими персональными данными со страховой медицинской организацией ООО "Астра-металл" с использованием машинных носителей или по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их прием и обработка будут осуществляется лицом, обязанным сохранять профессиональную тайну.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов и составляет двадцать пять лет.

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной 3 июня 2010 года и действует бессрочно.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа,

который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчетов по оплате оказанной мне до этого медицинской помощи.

Дата
Подпись

Примерный образец об использовании персональных данных кадровым агентством

Соглашение об использовании персональных данных кадровым агентством

10 сентября 2010 г. г. Магнитогорск

Кадровое агентство "Премиум", именуемое в дальнейшем "Агентство", с одной стороны, и Соискатель Щедров Вячеслав Григорьевич, совместно именуемые "Стороны", заключили настоящий соглашение о нижеследующем:

1. Настоящее соглашение определяет порядок использования Агентством персональных данных Соискателя при предоставлении услуг по трудоустройству.

2. Соискатель разрешает Агентству передавать свои персональные данные в форме Резюме любым третьим лицам, а также осуществлять их обработку любым другим способом в соответствии с действующим законодательством в целях, определенных пунктом 1 настоящего Соглашения.

3. Срок использования Агентством персональных данных не должен превышать 3-х месяцев с момента заключения настоящего Соглашения.

4. Все споры и разногласия между Сторонами по соглашению, в связи с соглашением и/или его исполнением Стороны будут стремиться урегулировать путем переговоров. Если в результате переговоров Стороны не достигли взаимоприемлемого решения, спор подлежит разрешению в суде (указать наименование региона).

5. В случае невыполнения условий настоящего Соглашения Стороны несут ответственность на условиях и в порядке, установленных действующим законодательством.

6. Изменение условий соглашения. Настоящее соглашение может быть изменено только с согласия обеих Сторон.

Подписи и реквизиты сторон

4. В ряде случаев для обработки ПД требуется обязательное получение оператором ПД письменного согласия на то от субъекта данных.

Так, получить согласие субъекта ПД в письменной форме придется оператору при обработке специальных категорий ПД, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Обрабатывать такие ПД без письменного согласия субъекта ПД категорически запрещено (за исключением случаев, когда они являются общедоступными). Обращаем внимание, что письменное согласие на подобные действия необходимо, даже если субъекта ПД и оператора связывают договорные отношения. В общественных объединениях или религиозных организациях обработка специальных категорий ПД членов (участников) осуществляется при условии, что ПД не будут распространяться без согласия субъектов, данного в письменной форме.

При обработке биометрических ПД, т.е. сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (сведения об особенностях строения папиллярных узоров пальцев рук человека, сетчатки глаз, о коде ДНК и т. д.), также необходимо получить письменное согласие субъекта ПД. Это требование также должно соблюдаться независимо от наличия договорных отношений между субъектом ПД и оператором, кроме отношений, связанных с прохождением государственной гражданской службы.

При передаче ПД субъекта оператором через Государственную границу РФ органу власти иностранного государства, физическому или юридическому лицу иностранного государства, не обеспечивающему адекватную защиту прав субъекта ПД, требуется также получение на то письменного согласия субъекта ПД.

В соответствие со ст. 8 комментируемого Закона согласие субъекта ПД нужно получить, если оператор планирует включить такие ПД в общедоступных источник данных. Согласно п. 2 ст. 16 комментируемого Закона решение, порождающее юридические последствия в отношении субъекта ПД или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПД только при наличии согласия в письменной форме субъекта ПД или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Письменное согласие субъекта ПД на обработку его данных должно включать в себя следующее:

- фамилию, имя, отчество субъекта ПД;

- адрес субъекта ПД;

- номер основного документа, удостоверяющего личность субъекта ПД, сведения о дате выдачи указанного документа и выдавшем его органе. К данному виду документов в соответствии с Указом Президента РФ от 13 марта 1997 г. N 232 "Об основном документе, удостоверяющем личность гражданина Российской Федерации на территории Российской Федерации" относится прежде всего паспорт гражданина РФ. Кроме того, в ст. 10 Федерального закона от 25 июля 2002 г. N 115-ФЗ "О правовом положении иностранных граждан в Российской Федерации" определены иные документы, удостоверяющие личность граждан. Так, для иностранного гражданина в РФ такими документами являются паспорт иностранного гражданина либо иной документ, установленный федеральным законом или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина. Для лица без гражданства в РФ документами, удостоверяющими личность, выступают документ, выданный иностранным государством и признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность лица без гражданства, разрешение на временное проживание, вид на жительство, иные документы, предусмотренные федеральным законом или признаваемые в соответствии с международным договором РФ в качестве документов, удостоверяющих личность лица без гражданства.

- наименование (или фамилию, имя, отчество) оператора, получающего согласие субъекта ПД;

- адрес оператора, получающего согласие субъекта ПД. Согласно п. 2 ст. 54 ГК РФ место нахождения юридического лица определяется местом его государственной регистрации. Государственная регистрация юридического лица осуществляется по месту нахождения его постоянно действующего исполнительного органа, в случае отсутствия постоянно действующего исполнительного органа - по месту нахождения иного органа или лица, имеющих право действовать от имени юридического лица без доверенности.

- цель обработки ПД;

- перечень ПД, на обработку которых дается согласие субъекта ПД. Перечень может включать в себя разнообразные данные. Например, возраст, пол, уровень заработной платы, семейное положение, образование и т. д.

- перечень действий с ПД, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПД;

- срок, в течение которого действует согласие, а также порядок его отзыва. В соглашении заключаемым оператором и субъектом ПД следует указать срок, в течение которого оператор имеет право обрабатывать ПД субъекта. Конкретный срок работы с ПД законодательством не предусмотрен, поэтому он устанавливается оператором исходя из потребности.

Общий образец согласия субъекта ПД на обработку ПД

_____

Наименование (Ф.И.О.) оператора

_____

Адрес оператора

_____

Ф.И.О. субъекта персональных данных

_____

Адрес, где зарегистрирован субъект персональных данных

_____

Номер основного документа, удостоверяющего его личность

_____

Дата выдачи указанного документа

_____

Наименование органа, выдавшего документ

Согласие на обработку персональных данных

Я, _____ (Ф.И.О.) даю свое согласие на обработку следующих моих персональных данных: _____

_____

(перечень персональных данных, для которых требуется получение

_____

письменного согласия)

для _____.

(указать цель обработки персональных данных)

Я предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

В случае неправомерного использования предоставленных данных настоящее согласие может быть в любое время отозвано мной.

Данное соглашение действует с "__" _____ 20__ г. по
"__"__ 20__ г.

Дата _____
Подпись

Авторы обращают внимание, что Федеральным законом от 27.07.2010 N 227-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "Об организации предоставления государственных и муниципальных услуг" внесены изменения в комментируемую статью. Изменения вступили в силу 1 января 2011 г. Рассмотрим их.

Так, п. 4 комментируемой статьи допускает, что равнозначным содержащему собственноручную подпись письменному согласию субъекта ПД на бумажном носителе признается согласие в форме электронного документа, подписанного электронной цифровой подписью или в случаях, предусмотренных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами, иным аналогом собственноручной подписи. Напоминаем, что электронный документ согласно ст. 3 Федерального закона от 10.01.2002 N 1-ФЗ "Об электронной цифровой подписи" - это документ, в котором информация представлена в электронно-цифровой форме. Электронная цифровая подпись - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Также в п. 4 добавляется абзац 7, в соответствии с которым законодатель уточняет, что письменное согласие субъекта ПД должно также содержать собственноручную подпись субъекта ПД.

В комментируемую статью добавляется п. 4.1., в котором указывается, что порядок получения согласия субъекта ПД в форме электронного документа на обработку его ПД в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, определяется Правительством РФ.

5. Из п. 5 комментируемой статьи следует, что для обработки ПД, которые содержатся в согласии, данном субъектом в письменной форме, дополнительного согласия не требуется. Так, например, если работодателем получено письменное согласие от работника на обработку его ПД, то получать дополнительное согласие, например, на передачу сведений в службу охраны организации для оформления пропуска, не потребуется. Также не требуется дополнительного разрешения и для указания данных сотрудника в доверенностях, приказах, расчетно-платежных ведомостях и в других рабочих документах.

6. В том случае, если гражданин, у которого планируется получить ПД для дальнейшей обработки, является недееспособным, то согласие в письменной форме об обработке ПД такого гражданина следует получать у законного представителя субъекта ПД. Авторы напоминают, что под дееспособностью понимается способность гражданина своими действиями приобретать и осуществлять гражданские права, создавать для себя гражданские обязанности и исполнять их (гражданская дееспособность). Дееспособность возникает в полном объеме с наступлением совершеннолетия, то есть по достижении восемнадцатилетнего возраста. В случае, когда законом допускается вступление в брак до достижения восемнадцати лет, гражданин, не достигший восемнадцатилетнего возраста, приобретает дееспособность в полном объеме со времени вступления в брак. Приобретенная в результате заключения брака дееспособность сохраняется в полном объеме и в случае расторжения брака до достижения восемнадцати лет. При признании брака недействительным суд может принять решение об утрате несовершеннолетним супругом полной дееспособности с момента, определяемого судом.

Можно выделить несколько групп недееспособных граждан.

Во-первых, это несовершеннолетние граждане в возрасте до 18 лет.

Во-вторых, это ограниченно дееспособные лица, признанные таковыми по решению суда, вступившему в законную силу. Гражданское право выделяет также ограниченно дееспособных лиц, чьи имущественные права и интересы в судах представляют их попечители. В силу ст. 30 ГК РФ суд может ограничить гражданина в дееспособности, если он вследствие злоупотребления спиртными напитками или наркотическими средствами ставит свою семью в тяжелое материальное положение. Лица, ограниченные в дееспособности, самостоятельно несут имущественную ответственность по совершенным сделкам и за причиненный вред. Они вправе совершать мелкие бытовые сделки, однако совершать иные сделки, получать заработок, пенсию, другие доходы и распоряжаться ими могут только с согласия попечителя.

В-третьих, это недееспособные граждане, признанные судом таковыми по вступившему в законную силу решению. К ним, например, относятся граждане, которые вследствие психического расстройства не могут понимать значения своих действий или руководить ими. Над ними устанавливается опека, их интересы представляет опекун.

Законными представителями недееспособных граждан могут быть родители, усыновители, опекуны, попечители, иные лица на основании предоставленного им федеральным законом права.

7. Пунктом 7 комментируемой статьи устанавливается, что в случае смерти субъекта ПД согласие на обработку его ПД в письменной форме могут дать наследники субъекта ПД, если такое согласие не было дано субъектом данных при его жизни.

В общепринятом смысле слова наследником является лицо, вступающее в имущественные или другие права после смерти другого лица.

Согласно ст. 1111 ГК РФ наследование осуществляется по завещанию и по закону. Однако не наследуют ни по закону, ни по завещанию граждане, которые своими умышленными противоправными действиями, направленными против наследодателя, кого-либо из его наследников или против осуществления последней воли наследодателя, выраженной в завещании, способствовали либо пытались способствовать призванию их самих или других лиц к наследованию либо способствовали или пытались способствовать увеличению причитающейся им или другим лицам доли наследства, если эти обстоятельства подтверждены в судебном порядке. Но граждане, которым наследодатель после утраты ими права наследования завещал имущество, вправе наследовать это имущество. Также не наследуют по закону родители после детей, в отношении которых родители были в судебном порядке лишены родительских прав и не восстановлены в этих правах ко дню открытия наследства. Кроме того по требованию заинтересованного лица суд отстраняет от наследования по закону граждан, злостно уклонявшихся от выполнения лежавших на них в силу закона обязанностей по содержанию наследодателя.

Наследники по закону призываются к наследованию в порядке очередности. Например, наследниками первой очереди по закону являются дети, супруг и родители наследодателя. Если нет наследников первой очереди, наследниками второй очереди по закону являются полнородные и неполнородные братья и сестры наследодателя, его дедушка и бабушка как со стороны отца, так и со стороны матери. Если нет наследников первой и второй очереди, наследниками третьей очереди по закону являются полнородные и неполнородные братья и сестры родителей наследодателя (дяди и тети наследодателя) и т.п.

Статья 10. Специальные категории персональных данных

1. Статьей 10 комментируемого Закона определяется порядок обработки специальной категории ПД. Как отмечалось ранее, к специальной категории ПД относятся данные, касающиеся:

- расовой, национальной принадлежности гражданина;
- политических взглядов гражданина;
- религиозных или философских убеждений гражданина;
- состояния здоровья гражданина;
- сведений об интимной жизни гражданина.

Положение о запрете обработки специальной категории ПД содержится в ст. 8 Директивы 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных", в соответствие с которой государства-участники взяли на себя обязательство запретить обработку ПД, раскрывающих расовое или этническое происхождение, политические взгляды, вероисповедание или философское воззрение, членство в профессиональном союзе, а также обработку данных, касающихся здоровья или интимной жизни.

Комментируемый Закон также запрещает обработку специальной категории ПД кроме ряда случаев, которые будут рассмотрены ниже.

2. Пунктом 2 комментируемой статьи определяются некоторые случаи, когда возможна обработка специальной категории ПД.

Такая обработка возможна, если субъект ПД дал согласие в письменной форме на обработку своих ПД.

Примерный образец согласия на обработку специальной категории персональных данных

Согласие на обработку специальной категории персональных данных

Я, Иванова Светлана Петровна, даю свое добровольное согласие ООО "Кадры" на включение в анкету данных о моем состоянии здоровья для оказания мне содействия в поиске подходящей работы.

Предоставляю ООО "Кадры" право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

В случае неправомерного использования предоставленных мною данных, я имею право в любое время отозвать настоящее согласие.

Данное согласие действует до 1 сентября 2010 года.

Дата
Подпись

Обработка специальной категории ПД возможна, и если они являются общедоступными, т.е. размещены в легальном общедоступном источнике данных.

8 декабря 2009 г. вступили в силу изменения в п. 2 комментируемой статьи, в соответствии с которыми обработка специальной категории ПД стала также возможна, если такая обработка необходима в связи с реализацией международных

договоров РФ о реадмиссии. Напоминаем, что реадмиссия - это согласие государства на прием обратно на свою территорию своих граждан (а также, в некоторых случаях, иностранцев, прежде находившихся или проживавших в этом государстве), которые подлежат депортации из другого государства.

Кроме того, изменения в данный пункт были внесены и Федеральным законом от 27.07.2010 N 204-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации". Данные изменения вступили с силу 30.07.2010 г. Такие изменения стали необходимы в связи с проведением Всероссийской переписи населения. Порядок проведения Всероссийской переписи населения регулируется Федеральным законом от 25.01.2002 N 8-ФЗ "О Всероссийской переписи населения". Согласно п. 1 ст. 6 упомянутого Закона, при проведении переписи у граждан могут быть получены следующие данные, включающие и специальную категорию ПД:

- пол;
- возраст (дата рождения);
- гражданство (состояние в гражданстве, наличие двойного гражданства, наименование государства или государств, гражданином которых является опрашиваемое лицо);
- национальная принадлежность;
- владение языками (родной язык, русский язык, другой язык или другие языки);
- образование (дошкольное, начальное общее, основное общее, среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное, послевузовское профессиональное);
- состояние в браке;
- количество детей;
- отношения с членами домохозяйства;
- место рождения;
- место жительства и (или) место пребывания;
- жилищные условия;
- источники средств к существованию;
- занятость либо безработица;
- миграция.

Могут обрабатываться данные, относящиеся к состоянию здоровья субъекта ПД, если их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта ПД невозможно. Как упоминалось ранее, согласно ст. 61 Основ законодательства РФ об охране здоровья граждан информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Поэтому передача таких сведений другим гражданам, в том числе должностным лицам возможна только с согласия субъекта ПД или его законного представителя и в интересах обследования и лечения пациента, для проведения научных исследований, публикации в научной литературе, использования этих сведений в учебном процессе и в иных целях. А предоставление указанных сведений без согласия гражданина или его законного представителя допускается только:

- в целях обследования и лечения гражданина, не способного из-за своего состояния выразить свою волю;
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу органов дознания и следствия и суда в связи с проведением расследования или судебным разбирательством;
- в случае оказания помощи несовершеннолетнему гражданину;
- при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий;
- в целях проведения военно-врачебной экспертизы в порядке, установленном положением о военно-врачебной экспертизе, утверждаемым уполномоченным федеральным органом исполнительной власти.

Идем дальше. Обработка специальной категории ПД возможна, если такие действия осуществляется:

- в медико-профилактических целях;
- в целях установления медицинского диагноза;
- в целях оказания медицинских и медико-социальных услуг.

Важным условием при этом является то, что такая обработка ПД может осуществляться только лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну. Напоминаем, что медицинская деятельность подлежит лицензированию в соответствии с Постановлением Правительства РФ от 22.01.2007 N 30 "Об утверждении Положения о лицензировании медицинской деятельности".

Особое право на обработку специальной категории ПД законодатель предоставляет общественным объединениям или религиозной организациям. Им разрешается обрабатывать ПД своих членов (участников), относящиеся к специальной категории ПД, если это необходимо для достижения законных целей организаций, предусмотренных их учредительными документами. Однако указанные организации обязаны не допускать распространения таких ПД без согласия в письменной форме субъектов ПД. В качестве примера можно привести общественные организации инвалидов. При вступлении в такие общественные объединения, инвалиды предоставляют в организацию сведения о своем состоянии здоровья, подтверждающие их инвалидность. Это необходимо, т.к. общественными организациями инвалидов признаются организации, созданные инвалидами и лицами, представляющими их интересы, в целях защиты прав и законных интересов инвалидов, обеспечения им равных с другими гражданами возможностей, решения задач общественной интеграции инвалидов, среди членов которых

инвалиды и их законные представители (один из родителей, усыновителей, опекун или попечитель) составляют не менее 80 процентов, а также союзы (ассоциации) указанных организаций.

Обработка специальной категории ПД возможна также, если это необходимо в связи с осуществлением правосудия или в соответствии с законодательством РФ о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством РФ. Речь идет прежде всего об обработки ПД, относящихся к специальной категории ПД, в соответствии с правилами, установленными ФЗ "О безопасности", ФЗ "Об оперативно-розыскной деятельности" и УПК РФ. О некоторых случаях обработки ПД для указанных выше целей говорилось в комментарии к предыдущей статье Закона. Стоит лишь добавить, что согласно ст. 8 ФЗ "Об оперативно-розыскной деятельности" гражданство, национальность, пол, место жительства, имущественное, должностное и социальное положение, принадлежность к общественным объединениям, отношение к религии и политические убеждения отдельных лиц не являются препятствием для проведения в отношении их оперативно-розыскных мероприятий на территории РФ, если иное не предусмотрено федеральными законами.

Авторы обращают внимание, что Федеральный закон от 29 ноября 2010 г. N 313-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "Об обязательном медицинском страховании в Российской Федерации" внес изменения в п. 2 комментируемой статьи.

Так, с 1 января 2011 обработка специальной категории ПД возможна также в целях обязательного социального страхования в соответствии с федеральными законами о конкретных видах обязательного социального страхования. Так, согласно положениям Федерального закона от 29.11.2010 N 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации", который вступил в силу 01.01.2011 г., Федеральный фонд обязательного медицинского образования вправе обрабатывать данные персонифицированного учета о медицинской помощи, оказанной застрахованным лицам. При этом ведение персонифицированного учета сведений о медицинской помощи, оказанной застрахованным лицам, предполагает сбор, обработку, передачу и хранение следующих данных:

- номер полиса обязательного медицинского страхования застрахованного лица;
- медицинская организация, оказавшая соответствующие услуги;
- виды оказанной медицинской помощи;
- условия оказания медицинской помощи;
- сроки оказания медицинской помощи;
- объемы оказанной медицинской помощи;
- стоимость оказанной медицинской помощи;
- диагноз;
- профиль оказания медицинской помощи;
- медицинские услуги, оказанные застрахованному лицу, и примененные лекарственные препараты;
- примененные медико-экономических стандарты;
- специальность медицинского работника, оказавшего медицинскую помощь;
- результат обращения за медицинской помощью;
- результаты проведенного контроля объемов, сроков, качества и условий предоставления медицинской помощи.

Перечисленные сведения относятся к информации ограниченного доступа и подлежат защите в соответствии с законодательством РФ.

3. Рассматривая п. 3 комментируемой статьи, следует заметить, что Директивой 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" устанавливается, что обработка данных, касающихся правонарушений, уголовного наказания или мер безопасности, может осуществляться только под контролем официального органа, или - если в соответствии с национальным законодательством предусмотрены надлежащие особые гарантии - с учетом частичных исключений, установленных государством-участником в соответствии с национальными нормами, предусматривающими надлежащие особые гарантии. Однако полный реестр уголовных приговоров может вестись только под контролем официального органа. Кроме того государства-участники могут установить, что данные, касающиеся административных санкций или судебных решений по гражданским делам, также могут обрабатываться под контролем официального органа.

В российском законодательстве согласно ст. 37 Федерального закона N 67-ФЗ "Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации" от 12.06.2002 N 67-ФЗ, если у кандидата имеется судимость, эти сведения должны указываться в подписном листе.

4. Ранее объяснялось, что согласно п. 2 ст. 5 комментируемого Закона после достижения цели обработки ПД подлежат уничтожению. В п. 4 комментируемой статьи законодатель уточняет применение этой нормы права для специальной категории ПД. Если обработка таких данных все же велась, то когда цели ее обработки достигнуты, или условия, при которых обработка была разрешена действующим законодательством исчезли, обработка специальной категории ПД должна быть незамедлительно прекращена. Например, если субъект ПД дал письменное разрешение на обработку таких данных, но отозвал свое согласие, обработка упомянутых ПД должна быть закончена.

Статья 11. Биометрические персональные данные

1. Комментируемая статья определяет порядок обработки биометрических ПД. "Биометрические технологии идентификации личности, основанные на распознавании человека по внешним морфологическим признакам, имеют глубокие

исторические корни. Способность людей узнавать друг друга по внешнему виду, голосу, запаху, походке и т.д. есть не что иное, как элементарная биометрическая идентификация"*(7).

Биометрические данные можно разделить на два основных класса:

- физиологические данные - относятся к форме тела (отпечатки пальцев, распознавание лица, ДНК, ладонь руки, сетчатка глаза);
- поведенческие данные связаны с поведением человека (походка, голос).

Из смысла п. 1 комментируемой статьи следует, что биометрические персональные данные - это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Таким образом, к биометрическим ПД, на обработку которых будет распространяться действие комментируемого Закона, можно отнести:

- отпечатки пальцев;
- отпечатки ладони;
- результаты анализа ДНК;
- цифровой образ лица;
- цифровой образ сетчатки глаза;
- фотографии и видеоизображения субъектов ПД и т.п.

Биометрические ПД могут обрабатываться только при наличии согласия субъекта ПД. Причем такое согласие должно быть обязательно оформлено в письменной форме.

Примерный образец согласия на обработку биометрических ПД

В ЗАО "Защита-М",
г. Троицк, ул. Советская,7
от Сергеева Ивана Борисовича,
проживающегося по адресу: г. Троицк, ул. Ленина,1-3,
паспорт 7589 8526321,
выдан ОВД Ленинского р-на г. Троицка 01.10.2001 г.,

Согласие на обработку биометрических персональных данных

Я, Сергеев Иван Борисович, даю свое добровольное согласие ЗАО "Защита-М" для оказания мне услуг по охране моей квартиры на обработку моих биометрических персональных данных, а именно _____ _____.

(перечень биометрических ПД, подлежащих обработки)

Предоставляю ЗАО "Защита-М" право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

В случае неправомерного использования предоставленных мною данных, я имею право в любое время отозвать настоящее согласие.

Данное согласие действует до 31 декабря2010 года.

Дата
Подпись

При использовании материальных носителей, на которые осуществляется запись биометрических ПД, а также при хранении биометрических ПД вне информационных систем ПД операторы должны руководствоваться положениями постановления Правительства РФ от 06.07.2008 N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных". Обращаем внимание, что в этом случае под материальным носителем понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность.

Такой материальный носитель должен обеспечивать:

- защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы ПД;
- возможность доступа к записанным на материальный носитель биометрическим ПД, осуществляемого оператором и лицами, уполномоченными в соответствии с законодательством РФ на работу с биометрическими ПД;
- возможность идентификации информационной системы ПД, в которую была осуществлена запись биометрических ПД, а также оператора, осуществившего такую запись;

- невозможность несанкционированного доступа к биометрическим ПД, содержащимся на материальном носителе.

Следует помнить, что материальный носитель должен использоваться в течение срока, установленного оператором, осуществившим запись биометрических ПД на материальный носитель, но не более срока эксплуатации, установленного изготовителем материального носителя. Тип материального носителя, который будет использован для обработки биометрических ПД, определяет оператор. Однако в ряде случаев нормативными правовыми актами РФ может быть предписано использование материального носителя определенного типа. Например, постановлением Правительства РФ от 25.12.1998 N 1543 "Об утверждении Положения о направлении материальных носителей, содержащих дактилоскопическую информацию, в органы внутренних дел" установлено, что в качестве материальных носителей используются дактилоскопические карты, носители магнитной или иных видов записи, содержащие дактилоскопическую информацию. Материальные носители, направляемые в органы внутренних дел, должны быть подготовлены на основе информационных технологий, используемых при осуществлении оперативно-справочного учета в органах внутренних дел и включать в себя следующие данные:

- фамилия, имя, отчество;
- гражданство;
- пол;
- дата и место рождения;
- сведения о регистрации по месту жительства или по месту пребывания лица, прошедшего обязательную или добровольную государственную дактилоскопическую регистрацию;
- наименование органа, получившего дактилоскопическую информацию;
- основание и дата проведения обязательной или добровольной государственной дактилоскопической регистрации.

Следуем далее. Согласно правилам, прописанным в постановлении Правительства РФ от 06.07.2008 N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", оператор обязан:

- осуществлять учет количества экземпляров материальных носителей;
- осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель.

Если хранение биометрических ПД осуществляется вне информационных систем ПД, то должно быть обеспечено следующее:

- доступ к информации, содержащейся на материальном носителе, для уполномоченных лиц;
- применение средств электронной цифровой подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических ПД, записанных на материальный носитель;
- проверка наличия письменного согласия субъекта ПД на обработку его биометрических ПД или наличия иных оснований обработки ПД, установленных п. 2 комментируемой статьи.

Важно помнить, что в случае если на материальном носителе содержится дополнительная информация, имеющая отношение к записанным биометрическим ПД, то такая информация должна быть подписана электронной цифровой подписью и (или) защищена иными информационными технологиями, позволяющими сохранить целостность и неизменность информации, записанной на материальный носитель. При этом использование шифровальных (криптографических) средств защиты информации осуществляется в соответствии с Федеральным законом от 10.01.2002 N 1-ФЗ "Об электронной цифровой подписи".

В том случае, если хранение биометрических ПД осуществляется вне информационных систем ПД, то должна обеспечиваться регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы ПД.

2. В ряде случаев законодатель позволяет осуществлять обработку биометрических ПД без согласия субъекта ПД. Это возможно, когда:

- обработка данных осуществляется в связи с реализацией международных договоров РФ о реадмиссии;
- обработка данных необходима в связи с осуществлением правосудия;
- обработка данных предусмотрена законодательством РФ о безопасности (например, ФЗ "О безопасности");
- обработка данных предусмотрена законодательством РФ об оперативно-розыскной деятельности (например, ФЗ "Об оперативно-розыскной деятельности);
- обработка данных предусмотрена законодательством РФ о государственной службе (например, Федеральным законом от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации");
- обработка данных предусмотрена уголовно-исполнительным законодательством РФ (например, УИК РФ);
- обработка данных предусмотрена законодательством РФ о порядке выезда из РФ и въезда в РФ (Федеральный закон от 15.08.1996 N 114-ФЗ "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию").

Так, государственные служащие РФ подлежат обязательной государственной дактилоскопической регистрации в случаях и порядке, установленных Федеральным законом от 25.07.1998 N 128-ФЗ "О государственной дактилоскопической регистрации в Российской Федерации".

При этом под государственной дактилоскопической регистрацией нужно понимать деятельность по получению, учету, хранению, классификации и выдаче дактилоскопической информации, установлению или подтверждению личности человека, осуществляемая уполномоченными на то государственными органами. Дактилоскопической информацией является информация об особенностях строения папиллярных узоров пальцев рук человека и о его личности.

Согласно ст. 9 упомянутого нормативного правового акта обязательной государственной дактилоскопической регистрации подлежат граждане РФ, призываемые на военную службу и военнослужащие. Кроме того обязательную государственную дактилоскопическую регистрацию должны пройти граждане РФ, проходящие службу в:

- органах внутренних дел;
- органах по контролю за оборотом наркотических средств и психотропных веществ;
- органах государственной налоговой службы;
- органах по делам гражданской обороны;
- чрезвычайным ситуациям и ликвидации последствий стихийных бедствий;
- органах и подразделениях службы судебных приставов;
- таможенных органах;
- органах государственной охраны;
- учреждениях и органах уголовно-исполнительной системы;
- Государственной противопожарной службе;
- федеральном органе исполнительной власти, уполномоченном на осуществление функций по контролю и надзору в сфере миграции, и его территориальных органах, организациях, подразделениях.

Процедуру дактилоскопической регистрации проходят также:

- федеральные государственные гражданские служащие кадрового состава органов внешней разведки, а также не входящие в кадровый состав федеральные государственные гражданские служащие и работники органов внешней разведки;
- федеральные государственные гражданские служащие и работники органов федеральной службы безопасности, а также граждане, поступающие на военную службу по контракту, федеральную государственную гражданскую службу или работу в органы федеральной службы безопасности;
- спасатели профессиональных аварийно-спасательных служб и профессиональных аварийно-спасательных формирований РФ;
- члены экипажей воздушных судов государственной, гражданской и экспериментальной авиации РФ;
- граждане РФ, иностранные граждане и лица без гражданства, не способные по состоянию здоровья или возрасту сообщить данные о своей личности, если установить указанные данные иным способом невозможно;
- граждане РФ, иностранные граждане и лица без гражданства, подозреваемые в совершении преступления, обвиняемые в совершении преступления либо осужденные за совершение преступления, подвергнутые административному аресту, совершившие административное правонарушение, если установить их личность иным способом невозможно;
- иностранные граждане и лица без гражданства, подлежащие выдворению (депортации) за пределы территории РФ либо подпадающие под действие международных договоров РФ о реадмиссии;
- иностранные граждане и лица без гражданства, прибывшие в РФ в поисках убежища и подавшие ходатайства о предоставлении политического или иного убежища либо о признании их беженцами на территории РФ;
- иностранные граждане и лица без гражданства, незаконно находящиеся на территории РФ;
- иностранные граждане, получившие разрешение на временное проживание;
- граждане, претендующие на получение лицензии на осуществление частной детективной деятельности;
- граждане, претендующие на получение удостоверения частного охранника;
- граждане РФ, постоянно проживающие на территории РФ иностранные граждане и лица без гражданства, в отношении которых принято решение о выдаче удостоверения личности моряка.

Важно учитывать, что право на использование дактилоскопической информации имеют суды; органы прокуратуры; органы предварительного следствия; органы дознания; органы, осуществляющие оперативно-розыскную деятельность; органы уголовно-исполнительной системы; органы, осуществляющие производство по делам об административных правонарушениях; федеральный орган исполнительной власти, уполномоченный на осуществление функций по контролю и надзору в сфере миграции, и его территориальные органы.

Также, например, при идентификации личности с использованием удостоверения личности моряка право на использование дактилоскопической информации, полученной при выдаче удостоверения личности моряка, имеют следующие органы:

- федеральный орган исполнительной власти, осуществляющий функции по оказанию государственных услуг и управлению государственным имуществом в сфере морского и речного транспорта;
- федеральные государственные учреждения, имеющие право выдачи удостоверений личности моряка, в том числе администрации морских портов;
- органы федеральной службы безопасности.

Кроме того, право на получение дактилоскопической информации, содержащейся в информационных массивах органов внутренних дел и федерального органа исполнительной власти, осуществляющего функции по оказанию государственных услуг и управлению государственным имуществом в сфере морского и речного транспорта, может быть предоставлено иностранным государствам в соответствии с международными договорами РФ.

УИК РФ содержит норму права, которая обязывает уголовно-исполнительную инспекцию по месту жительства осужденного к наказанию в виде ограничения свободы поставить его на персональный учет. При этом осужденный подлежит дактилоскопической регистрации и фотографированию (п. 4 ст. 47.1 УИК РФ).

В соответствии со ст. 7 Федерального закона от 15.08.1996 N 114-ФЗ "О порядке выезда из Российской Федерации и

въезда в Российскую Федерацию" основные документы, удостоверяющие личность гражданина РФ, по которым граждане РФ осуществляют выезд из РФ и въезд в РФ, могут содержать электронные носители информации с записанными на них ПД владельца паспорта, включая биометрические ПД. Это такие данные, как номер документа; фамилия и имя владельца документа; гражданство владельца документа; дата рождения владельца документа; пол владельца документа; цветное цифровое фотографическое изображение лица владельца документа (биометрические ПД владельца документа).

Статья 12. Трансграничная передача персональных данных

1. Перед анализом ст. 12 комментируемого Закона необходимо раскрыть понятие "трансграничной передачи ПД". Трансграничная передача ПД - это передача ПД оператором через государственную границу РФ органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Изначально некоторые рекомендации, касающиеся трансграничной передачи ПД давались в Основных положениях о защите неприкосновенности частной жизни и международных обменов персональными данными от 23 сентября 1980 г., принятых Организацией по экономическому сотрудничеству и развитию (ОЭСР). В этом документе странам-членам советовалось учитывать возможные последствия, которые использование ПД внутри страны и их реэкспорт могут иметь для других стран-членов. Странам-членам рекомендовалось принимать разумные и должные меры к обеспечению того, чтобы международные обмены ПД, в том числе их транзит через территорию каждой страны-члена, были непрерывными и безопасными. Необходимо было воздерживаться от введения ограничений на обмены ПД между собой и другой страной-членом, за исключением случаев, когда последняя еще не начала соблюдать большинство пунктов указанного выше документа, а также под угрозой того, что реэкспорт таких данных может привести к нарушению действующих в первой стране внутренних законов о неприкосновенности частной жизни. Также страна-член имела право вводить ограничения в отношении тех категорий ПД, касательно которых ее внутренними законами о неприкосновенности частной жизни предусмотрены конкретные правила, связанные с характером таких данных, в случае если другая страна-член не обеспечивает их эквивалентной защиты. Странам-членам советовалось избегать принятия законов, политических установок и практических правил во имя защиты неприкосновенности частной жизни и индивидуальных свобод, которые могут создать препятствия для международных обменов ПД сверх меры, необходимой для обеспечения такой защиты.*(8)

Далее 28 января 1981 года была принята Конвенция Совета Европы о защите личности в связи с автоматической обработкой персональных данных, положения которой, касающиеся трансграничной передачи ПД, будут рассмотрены ниже.

Затем принцип адекватной защиты ПД при их перемещении через государственные границы был определен в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных".

В связи с вступлением России в 1996 году в Совет Европы возникла необходимость создания условий для выполнения международных обязательств, касающихся обеспечения защиты ПД, и в нашей стране.

В настоящее время в РФ до начала осуществления трансграничной передачи ПД оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПД, обеспечивается адекватная защита прав субъектов ПД. Иными словами, в таком государстве должен действовать закон о защите ПД.

Надо заметить, что нормы комментируемой статьи соответствуют положениям Директивы 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных". Так, согласно ст. 25 упомянутого документа государства-участники обязаны обеспечить, чтобы передача в третьи страны ПД, находящихся в обработке или предназначенных для обработки после передачи, осуществлялась только если соответствующая третья страна - без ущерба для выполнения национальных положений, принятых в соответствии с остальными положениями настоящей Директивы, - обеспечивает адекватный уровень защиты. Адекватность уровня защиты, предоставляемого третьей страной, оценивается в свете всех обстоятельств, в которых производится операция или набор операций по передаче данных. Особое внимание уделяется при этом природе данных, цели и продолжительности предполагаемых операций или операций по обработке данных, стране происхождения и стране окончательного назначения, действующим в соответствующей третьей стране положениям закона, как общим, так и частным, а также профессиональным нормам и мерам безопасности, соблюдаемым в такой стране.

Подписав Директиву 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" государства-участники взяли на себя обязательства информировать друг друга о случаях, когда они считают, что третья страна не обеспечивает адекватного уровня защиты.

В Российской Федерации одним из критериев оценки государства в отношении адекватного уровня защиты может выступать факт ратификации им Конвенции о защите прав физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г., ETS N 108. На сегодняшний день в число стран, подписавших и ратифицировавших указанную Конвенцию, входят Австрия; Андорра; Бельгия; Болгария; Дания; Великобритания; Венгрия; Германия; Греция; Израиль и др.

Так, согласно ст. 14 упомянутой выше Конвенции стороны, подписавшие Конвенцию, должны оказывать помощь любому лицу, проживающему за рубежом, в осуществлении правомочий, предусмотренном его национальным правом, реализующим принципы, изложенные в Конвенции. При этом если такое лицо проживает на территории другой стороны, ему будет предоставлена возможность передать свое ходатайство через посредничество органа, назначенного этой стороной. Ходатайство о помощи должно содержать все необходимые реквизиты, в том числе касающиеся:

- имени, адреса и других относящихся к делу характеристик, позволяющих идентифицировать лицо, подавшее ходатайство;

- автоматизированной базы ПД, к которой относится ходатайство, и ее контролера;

- цели ходатайства.

2. Однако согласно п. 2 комментируемой статьи трансграничная передача ПД на территории иностранных государств, обеспечивающих адекватную защиту прав субъектов ПД, может быть запрещена или ограничена. Это возможно в следующих случаях:

- в целях защиты основ конституционного строя РФ;

- в целях защиты нравственности, здоровья, прав и законных интересов граждан;

- в целях обеспечения обороны страны и безопасности государства.

Отметим, что согласно ст. 12 Конвенции о защите прав физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г., ETS N 108 государства взяли на себя обязательства не запрещать или не ставить под специальный контроль информационные потоки ПД, идущие на территорию другой страны, исходя исключительно из соображений защиты неприкосновенности личной сферы. Но государству позволяется при этом отступить от этого правила в той мере, в какой законодательство государства устанавливает специальные правила в отношении определенных категорий ПД или автоматизированных баз ПД - кроме случаев, когда правилами другой стороны предусмотрена равноценная защита, а также когда передача осуществляется с территории страны, подписавшей Конвенцию, на территорию государства, не являющегося стороной Конвенции, через территорию другой стороны - с той целью, чтобы такая передача не совершалась в обход законодательства стороны, указанной в начале предложения.

3. В ряде случаев трансграничная передача ПД на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПД возможна. Перечень этих случаев содержится в п. 3 комментируемой статьи. Перед анализом упомянутых случаев, заметим, что согласно Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" передача ПД в третью страну, не обеспечивающую адекватный уровень защиты также может иметь место при условии, что:

- субъект данных дал свое недвусмысленное согласие на предполагаемую передачу;

- или передача является необходимой для исполнения контракта между субъектом данных и контролером (физическим или юридическим лицом, официальным органом, агентством или иным органом, который самостоятельно или совместно с другими определяет цели и средства обработки ПД), или для реализации доконтрактных мер, принятых в ответ на запрос субъекта данных;

- или передача необходима для заключения или исполнения контракта, заключенного в интересах субъекта данных между контролером и третьей стороной;

- или передача необходима или требуется по закону по причинам, представляющим существенный общественный интерес, или для подачи, исполнения судебных исков или защиты по таковым;

- или передача необходима для защиты жизненных интересов субъекта данных;

- или передача производится из реестра, который в соответствии с законами или нормативными актами предназначен для предоставления информации общественности и который открыт для ознакомления либо общественностью в целом, либо любым лицом, проявляющим законный интерес, в той мере, в какой условия, изложенные в законе выполняются в конкретном случае.

Рассмотрим случаи, когда в РФ допускается трансграничная передача ПД на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПД.

Во-первых, это возможно при наличии согласия в письменной форме субъекта ПД.

Напоминаем, что согласно п. 4 ст. 9 комментируемого Закона такое согласие должно включать в себя:

- фамилию, имя, отчество, адрес субъекта ПД, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта ПД;

- цель обработки ПД;

- перечень ПД, на обработку которых дается согласие субъекта ПД;

- перечень действий с ПД, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПД;

- срок, в течение которого действует согласие, а также порядок его отзыва;

- собственноручную подпись субъекта персональных данных.

Во-вторых, допускается трансграничная передача ПД на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПД, в случаях:

- предусмотренных международными договорами РФ по вопросам выдачи виз;

- предусмотренных международными договорами РФ об оказании правовой помощи по гражданским, семейным и уголовным делам;

- предусмотренных международными договорами РФ о реадмиссии.

Так, например, 1 июня 2007 г. вступило в силу Соглашение между РФ и Европейским сообществом об упрощении выдачи виз гражданам РФ и Европейского союза, подписанное 25 мая 2006 г. в городе Сочи. Положения этого документа распространяются, к примеру, на следующие страны Европейского Союза: Австрию; Бельгию; Болгарию; Венгрию; Грецию; Испанию; Италию и др.

Упомянутое выше соглашение регулирует условия оформления деловых, гуманитарных, частных, учебных, транзитных

виз и не применяется для оформления служебных, рабочих, туристических виз, виз временно проживающего лица и визы в целях получения убежища. Напоминаем, что визой называется документ, являющийся одним из оснований въезда иностранного лица на территорию государства.

В качестве примеров международных договоров об оказании правовой помощи можно привести следующие:

- договор между РФ и Эстонской Республикой о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 26 января 1993 г.;

- договор между РФ и Канадой о взаимной правовой помощи по уголовным делам от 20 октября 1997 г.;

- договор между РФ и Соединенными Штатами Америки о взаимной правовой помощи по уголовным делам от 17 июня 1999 г. и другие.

"Сущность соглашений о реадмиссии составляют взаимные обязательства государств принять обратно своих граждан, граждан третьих стран и лиц без гражданства, незаконно прибывших на территорию договаривающейся стороны или остающихся там без законных оснований, если данные лица прибыли с территории этой договаривающейся стороны. Договоры о реадмиссии также предусматривают создание технических возможностей для управления процедурой и операциями по перемещению нелегальных мигрантов, а также установление правил возмещения затрат, защиты данных и соблюдение прочих международных прав и обязательств. Субъектами рассматриваемых соглашений могут являться не только государства, но и группы и объединения государств"*(9).

Согласно ст. 32.2 Федерального закона от 25.07.2002 N 115-ФЗ "О правовом положении иностранных граждан в Российской Федерации" передача иностранного гражданина РФ иностранному государству в соответствии с международным договором РФ о реадмиссии или прием РФ иностранного гражданина, передаваемого иностранным государством РФ в соответствии с международным договором РФ о реадмиссии, осуществляется федеральным органом исполнительной власти в сфере миграции или его территориальным органом на основании решения руководителя указанного федерального органа или его заместителя о реадмиссии указанного иностранного гражданина.

В 2006 г. в городе Сочи прошел саммит Россия-ЕС, где были подписаны соглашения об облегчении визового режима и о взаимной выдаче незаконных мигрантов - реадмиссии.

В-третьих, трансграничная передача ПД на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПД возможна в случаях, предусмотренных федеральными законами, если это необходимо:

- в целях защиты основ конституционного строя РФ;

- в целях обеспечения обороны страны;

- в целях обеспечения безопасности государства.

Под обороной страны понимается система политических, экономических, военных, социальных, правовых и иных мер по подготовке к вооруженной защите и вооруженная защита РФ, целостности и неприкосновенности ее территории. Ко всему прочему организация обороны включает в себя международное сотрудничество в целях коллективной безопасности и совместной обороны. Так, Президент РФ, являясь Верховным Главнокомандующим Вооруженными Силами РФ, ведет переговоры и подписывает международные договоры РФ в области обороны, включая договоры о совместной обороне, коллективной безопасности, сокращении и ограничении вооруженных сил и вооружений, об участии Вооруженных Сил РФ в операциях по поддержанию мира и международной безопасности. Правительство РФ ведет международные переговоры по вопросам военного сотрудничества и заключает соответствующие межправительственные соглашения. В целях защиты интересов РФ и ее граждан, поддержания международного мира и безопасности формирования Вооруженных Сил РФ могут оперативно использоваться за пределами территории РФ в соответствии с общепризнанными принципами и нормами международного права, международными договорами РФ и федеральными законами РФ.

Напоминаем, что угроза безопасности - это совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. Гражданам РФ, находящимся за ее пределами, государством гарантируется защита и покровительство. Одним из принципов обеспечения безопасности РФ является интеграция с международными системами безопасности, а одной из основных функций системы безопасности РФ - участие в мероприятиях по обеспечению безопасности за пределами РФ в соответствии с международными договорами и соглашениями, заключенными или признанными РФ.

Также в соответствии с п. 3 ст. 14 ФЗ "Об оперативно-розыскной деятельности" органы, осуществляющие оперативно-розыскную деятельность обязаны выполнять на основе и в порядке, предусмотренных международными договорами РФ, запросы соответствующих международных правоохранительных организаций, правоохранительных органов и специальных служб иностранных государств. Кроме того ст. 453 УПК РФ установлено, что при необходимости производства на территории иностранного государства допроса, осмотра, выемки, обыска, судебной экспертизы или иных процессуальных действий суд, прокурор, следователь, дознаватель должен внести запрос об их производстве компетентным органом или должностным лицом иностранного государства в соответствии с международным договором РФ, международным соглашением или на основе принципа взаимности. Такой запрос составляется в письменном виде, подписывается должностным лицом, его направляющим, удостоверяется гербовой печатью соответствующего органа и должен содержать:

- наименование органа, от которого исходит запрос;

- наименование и место нахождения органа, в который направляется запрос;

- наименование уголовного дела и характер запроса;

- данные о лицах, в отношении которых направляется запрос, включая данные о дате и месте их рождения, гражданстве, роде занятий, месте жительства или месте пребывания, а для юридических лиц - их наименование и место нахождения;

- изложение подлежащих выяснению обстоятельств, а также перечень запрашиваемых документов, вещественных и других доказательств;

- сведения о фактических обстоятельствах совершенного преступления, его квалификация, текст соответствующей статьи УК РФ, а при необходимости также сведения о размере вреда, причиненного данным преступлением.

В-четвертых, трансграничная передача ПД на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПД, может иметь место при исполнении договора, стороной которого является субъект ПД.

И в-пятых, трансграничная передача ПД на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПД, осуществляется при необходимости защиты жизни, здоровья, иных жизненно важных интересов субъекта ПД или других лиц. Например, при необходимости оказания срочной эффективной медицинской помощи гражданину РФ, который находится за пределами РФ, возможна передача из РФ данных о его прежних заболеваниях. Однако передача таких сведений без согласия субъекта ПД возможна только в тех случаях, когда получения такого согласия по каким-то причинам невозможна.

Статья 13. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных

1. Приступая к анализу этой статьи, напомним, что информационной системой называется совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

При этом согласно ст. 13 ФЗ "Об информации, информационных технологиях и о защите информации" государственными информационными системами называются федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов РФ, на основании правовых актов государственных органов. Муниципальные информационные системы - это информационные системы, созданные на основании решения органа местного самоуправления;

Как известно, ПД граждан распределены по различным базам государственных и муниципальных органов. В качестве примеров, можно привести следующие информационные базы:

- база данных налогоплательщиков, формируемые налоговыми службами;
- базы данных безработных, формируемые службами занятости населения;
- базы данных застрахованных лиц пенсионного фонда, фонда обязательного медицинского и социального страхования;
- базы данных управления внутренних дел;
- базы данных регистрационных служб и т.д.

Так, например, в Регистре получателей государственных услуг в сфере занятости населения - физических лиц, который формируется на основании и в порядке, определенном Законом РФ от 19.04.1991 N 1032-1 "О занятости населения в Российской Федерации" содержится, в частности, следующая информация:

- регистрационный номер учетной записи;
- фамилия, имя, отчество;
- дата рождения;
- пол;
- гражданство;
- адрес места жительства (пребывания), телефон;
- серия и номер паспорта или удостоверения личности, дата выдачи указанных документов и наименование выдавшего их органа;
- дата обращения гражданина и т.д.

При этом уполномоченный Правительством РФ федеральный орган исполнительной власти вправе устанавливать обязательность внесения иной информации в Регистр получателей государственных услуг в сфере занятости населения - физических лиц.

Пенсионный Фонд РФ располагает базой застрахованных лиц, т.е. лиц, на которых распространяется обязательное пенсионное страхование, включая лиц, занятых на рабочем месте с особыми (тяжелыми и вредными) условиями труда, за которых уплачиваются страховые взносы в Пенсионный фонд РФ в соответствии с законодательством РФ. На каждое застрахованное лицо Пенсионный фонд РФ открывает индивидуальный лицевой счет с постоянным страховым номером, содержащим контрольные разряды, которые позволяют выявлять ошибки, допущенные при использовании этого страхового номера в процессе учета.

Индивидуальный лицевой счет застрахованного лица - это документ, хранящийся в форме записи на машинных носителях информации, допускающей обработку с помощью средств вычислительной техники в органах Пенсионного фонда РФ, содержащий сведения о застрахованных лицах, включенные в информационные ресурсы Пенсионного фонда РФ. Так, например, в общей части индивидуального лицевого счета застрахованного лица указываются, в частности: страховой номер; фамилия, имя, отчество, фамилия, которая была у застрахованного лица при рождении; дата рождения; место рождения; пол; адрес постоянного места жительства; серия и номер паспорта; дата регистрации в качестве застрахованного лица и т.д.

2. Пункт 2 комментируемой статьи гласит, что особенности учета персональных данных в государственных и муниципальных информационных системах ПД могут быть определены федеральными законами. При этом может разрешаться использование различных способов обозначения принадлежности ПД, содержащихся в соответствующей государственной или муниципальной информационной системе ПД, конкретному субъекту ПД.

В настоящее время в соответствии с НК РФ налоговыми службами создаются базы данных налогоплательщиков - физических лиц, где каждому налогоплательщику присваивается единый по всем видам налогов и сборов, в том числе подлежащих уплате в связи с перемещением товаров через таможенную границу РФ, и на всей территории РФ идентификационный номер налогоплательщика (ИНН). Порядок и условия присвоения, применения, а также изменения идентификационного номера налогоплательщика установлены приказом МНС РФ от 03.03.2004 N БГ-3-09/178 "Об утверждении Порядка и условий присвоения, применения, а также изменения идентификационного номера налогоплательщика и форм документов, используемых при постановке на учет, снятии с учета юридических и физических лиц". Идентификационный номер налогоплательщика формируется как цифровой код, состоящий из последовательности цифр, характеризующих слева направо следующее:

- код налогового органа, который присвоил идентификационный номер налогоплательщика (NNNN);

- собственно порядковый номер записи о лице в территориальном разделе единого государственного реестра налогоплательщиков налогового органа, осуществившего постановку на учет: для физических лиц - 6 знаков (XXXXXX);

- контрольное число, рассчитанное по специальному алгоритму, установленному Министерством Российской Федерации по налогам и сборам: для физических лиц - 2 знака (CC).

Идентификационный номер налогоплательщика присваивается налоговым органом по месту жительства физического лица при постановке на учет физического лица или учете сведений о физическом лице. В случае если физическое лицо, которому принадлежит недвижимое имущество и (или) транспортные средства, не имеет места жительства на территории РФ, ИНН присваивается налоговым органом по месту нахождения имущества и (или) транспортного средства при постановке на учет физического лица в вышеназванном налоговом органе. Для физических лиц - иностранных граждан или лиц без гражданства, зарегистрированных в качестве индивидуальных предпринимателей и имеющих разрешение на временное проживание в РФ, адрес временного проживания приравнивается к адресу места жительства.

На официальном сайте Федеральной налоговой службы каждый гражданин может воспользоваться указанной выше базой данных налогоплательщиков. Так, введя свой ИНН и сведения о фамилии, имени и отчестве, гражданин может получить информацию о наличии или отсутствии у него задолженности по налогам на доходы физических лиц, имущественному, транспортному, земельному налогу.

3. Законодатель устанавливает особые требования к государственным и муниципальным информационным системам ПД.:

- права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки ПД или обозначения принадлежности ПД конкретному субъекту ПД;

- не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности ПД конкретному субъекту ПД.

4. Пункт 4 комментируемой статьи позволяет создание государственного регистра населения, правовой статус которого устанавливаются федеральными законами.

Еще в 1999 г. Правительством РФ было поручено Минтруду России совместно с МНС России, МВД России, Минфином России, Госкомстатом России, ФАПСИ, Пенсионным фондом РФ, Фондом социального страхования РФ, Федеральным фондом обязательного медицинского страхования и Минюстом России разработать проект Федерального закона "О государственном регистре населения Российской Федерации". Проект закона разрабатывался в целях повышения уровня социальной защиты населения РФ и предусматривал введение единого персонифицированного учета социального страхования граждан и концепцию создания автоматизированной системы "Государственный регистр населения", технические решения которой должны были быть взаимоувязаны с техническими решениями автоматизированных систем заинтересованных федеральных органов исполнительной власти и организаций.

В настоящее время опытные проекты реализуется в некоторых субъектах РФ. Так, государственный регистр населения (ГРН Спб) создается в Санкт-Петербурга. "Это государственный информационный ресурс Санкт-Петербурга, который содержит основные идентификационные (персональные) сведения о населении Санкт-Петербурга, (включая всех граждан, зарегистрированных по месту постоянного проживания или временного пребывания на территории города). Основным назначением ГРН СПб является обеспечение необходимой информационной поддержки деятельности органов государственной власти Санкт-Петербурга и органов местного самоуправления в Санкт-Петербурге, а также формирование условий для организации информационного взаимодействия между указанными органами на основе использования современных информационных технологий. Формирование и использование ГРН СПб обеспечивается на основе функционирования межведомственной автоматизированной информационной системы - АИС "ГРН СПб". Значение ГРН, в первую очередь, определяется его интегрирующей ролью по отношению к системе баз данных, содержащих персональные данные различных категорий населения. Одной из основных задач АИС "ГРН СПб" является обеспечение организаций, которые занимаются учетом отдельных категорий граждан, достоверной и актуальной информацией о персональных данных граждан.

Центральная, системообразующая роль ГРН по отношению к информационным ресурсам территории, содержащим персональные данные граждан, определяется рядом факторов, основными из которых являются:

- ГРН СПб содержит сведения обо всем населении Санкт-Петербурга;

- в ГРН содержатся основные идентификационные данные гражданина, используемые в других системах учета населения, в которых к основной идентификационной информации о человеке добавляется специфическая, для соответствующего ведомства, информация;

- информация в ГРН СПб поступает из официальных первоисточников (где она легитимно зарождается) и подлежит

своевременному (ежедневному) обновлению, что гарантирует ее достоверность и актуальность (паспортно-визовые органы, органы ЗАГС)"*(10).

Подобный опыт имеет и Московская область. Там в 2006-2009 году была реализована программа "Электронное Подмосковье" в рамках которой велась работа по созданию и внедрению автоматизированной системы персонального учета населения (СПУН. "Например, в Климовске официальным разработчиком СПУН по Московской области - компанией "ИНСОФТ" была установлена автоматизированная информационная система муниципального регистра населения, позволяющая вести базу данных жителей. По словам специалистов, это позволило не только автоматизировать работу в указанном направлении, но и обеспечить эффективное взаимодействие информационных систем учета различных категорий граждан, а на уровне области - наладить информационное обслуживание органов государственной власти, местного самоуправления, организаций и предприятий"*(11).

По мнению авторов, создание подобных государственных регистров населения поможет избегать дублирования информации в работе различных служб по сбору одних и тех же сведений о гражданине, ускорит процедуры, связанные со сбором и представлением гражданами справок из разных инстанций.

Глава 3. Права субъекта персональных данных

Статья 14. Право субъекта персональных данных на доступ к своим персональным данным

Комментируемой статьей начинается новая глава Закона, определяющая права субъекта ПД.

Итак, субъект ПД обладает следующими правами:

- правом на получение сведений об операторе, о месте его нахождения;
- правом на получение сведений о наличии у оператора ПД, относящихся к соответствующему субъекту ПД;
- правом на ознакомление со своими ПД, находящимися у оператора (кроме случаев как доступ к ПД ограничен - см. комментарии к п. 5 Закона);
- правом требовать от оператора уточнения своих ПД, их блокирования или уничтожения в случае, если ПД являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- правом принимать предусмотренные законом меры по защите своих прав.

Право доступа к своим ПД предоставляет и Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных". Так, согласно ст. 12 указанного документа государства-участники гарантируют право каждого субъекта данных получать от контролера (физического или юридического лица, официального органа, агентства или иного органа, который самостоятельно или совместно с другими определяет цели и средства обработки ПД):

- подтверждение того, были ли или нет в обработке относящиеся к нему данные, и информацию по меньшей мере о целях обработки, категории используемых данных, получателях или категориях получателей, которым сообщаются данные;
- сообщение об обрабатываемых данных и о любой доступной информации, касающейся их источника;
- сведения о логике, используемой в любой автоматической обработке данных, касающихся его;
- уточнение, стирание или блокировку данных, не соответствующих положениям Директивы, в частности, в связи с неполным или неточным характером данных;
- уведомление третьих лиц, которым раскрываются данные, о любых уточнениях, стирании или блокировках данных, если это не оказывается невозможным или требующим непропорциональных усилий.

Права субъекта ПД на доступ к своим данным закреплены, например, в Положении о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденном Указом Президента РФ от 30.05.2005 г. N 609. Так, гражданские служащие имеют право:

- получать полную информацию о своих ПД и обработке этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим ПД, включая право получать копии любой записи, содержащей ПД гражданского служащего, за исключением ряда случаев, предусмотренных федеральными законами;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства о ПД (при этом гражданский служащий при отказе представителя нанимателя или уполномоченного им лица исключить или исправить ПД гражданского служащего имеет право заявить в письменной форме представителю нанимателя или уполномоченному им лицу о своем несогласии, обосновав соответствующим образом такое несогласие);
- требовать от представителя нанимателя или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные ПД гражданского служащего, обо всех произведенных в них изменениях или исключениях из них;
- обжаловать в суд любые неправомерные действия или бездействие представителя нанимателя или уполномоченного им лица при обработке и защите ПД гражданского служащего.

Следуя требованиям п. 1 комментируемой статьи, операторам ПД целесообразно определить процедуру оперативного уточнения данных. Если кроме основной базы ПД в организации существует несколько резервных копий, то соответствующие уточнения должны вноситься во все из них. Если это возможно, то обязанность уточнения информации может распространяться

и на сведения, которые были переданы третьим лицам. Обязанность уточнения данных можно закрепить за отдельным ответственным сотрудником. Этот же сотрудник может фиксировать изменение статуса ПД в случае их блокирования и отвечать за своевременное уничтожение ПД в случае отказа субъекта ПД от обработки его данных, удалять из базы данных информацию об умерших субъектах ПД. Необходимо учитывать, что если исправление ПД технически невозможно, например, когда данные записаны на CD или DVD, оператор ПД обязан гарантировать, что неточные данные не будут использоваться.*(12)

2. Итак, оператор должен предоставить возможность субъекту ПД ознакомиться со своими данными. При этом доступ к данным может быть предоставлен в любой форме, в зависимости от того, как хранятся данные. Например, с содержанием электронной базы данных можно познакомиться как посмотрев ее на мониторе компьютера, так и получив соответствующую распечатку. Доступ к ПД, которые хранятся в Интернете, может быть обеспечен путем предоставления ссылки на страницу. Доступ к истории болезни гражданина в поликлинике или больнице может быть предоставлен путем передачи истории болезни на руки пациенту или его законному представителю. Во всех случаях оператор ПД должен позаботиться о том, чтобы в информации или документах, передаваемых гражданину, не содержались данные, относящиеся к другому субъекту ПД.

Примерный образец заявления о выдаче истории болезни

Заведующему поликлиникой N __
_____
(Ф.И.О. заведующего)
от _____
(Ф.И.О. заявителя)
проживающего по адресу: _____
паспортные данные _____

"___" _____ 20 __ г.

Заявление о выдаче истории болезни

Прошу выдать мне на руки мою историю болезни в соответствии со ст. 14 ФЗ "О персональных данных" и ст. 31 "Основ законодательства Российской Федерации об охране здоровья граждан"

Подпись

Примерный образец жалобы прокурору на действия заведующего поликлиникой

Прокурору
г. _____
_____
(Ф.И.О. прокурора)
от _____
(Ф.И.О. заявителя)
проживающего по адресу: _____
паспортные данные _____

"___" _____ 20 __ г.

Жалоба
на действия заведующего поликлиникой N___

"__" _____ 20 ___ г. я обратился к заведующему поликлиникой N ___ _____ (Ф.И.О. заведующего) с просьбой выдать мне на руки мою историю болезни (копия запроса прилагается).

Однако "__" _____ 20 __ г. я получил по почте письменный отказ в выдаче моей истории болезни.

Руководствуясь ст. 14 ФЗ "О персональных данных", ст. 31 "Основ законодательства Российской Федерации об охране здоровья граждан", ст. 26-28 ФЗ "О прокуратуре РФ"
прошу обязать заведующего поликлиники N ___ выдать мою историю болезни мне на руки.

Приложение:

- копия запроса к заведующему поликлиникой N __ от "___" _____ г.;
- копия ответа на запрос.

Подпись

Гражданам также следует знать, что согласно ст. 8 Федерального закона от 30.12.2004 N 218-ФЗ "О кредитных историях" субъект кредитной истории вправе в каждом бюро кредитных историй, в котором хранится кредитная история о нем, один раз в год бесплатно и любое количество раз за плату без указания причин получить кредитный отчет по своей кредитной истории, в том числе с накопленной информацией об источниках формирования кредитной истории и о пользователях кредитной истории, которым выдавались кредитные отчеты. Кроме того субъект кредитной истории вправе полностью или частично оспорить информацию, содержащуюся в его кредитной истории, подав в бюро кредитных историй, в котором хранится указанная кредитная история, заявление о внесении изменений и (или) дополнений в эту кредитную историю. При этом бюро кредитных историй в течение 30 дней со дня получения такого заявления, обязано, провести дополнительную проверку информации, входящей в состав кредитной истории, запросив ее у источника формирования кредитной истории. На время проведения такой проверки в кредитной истории делается соответствующая пометка. Далее бюро кредитных историй в случае подтверждения заявления субъекта кредитной истории обновляет кредитную историю в оспариваемой части или оставляет кредитную историю без изменения. О результатах рассмотрения указанного заявления бюро кредитных историй обязано в письменной форме сообщить субъекту кредитной истории по истечении 30 дней со дня его получения. Отказ в удовлетворении указанного заявления должен быть мотивированным. Субъект кредитной истории вправе обжаловать в судебном порядке отказ бюро кредитных историй в удовлетворении заявления о внесении изменений и (или) дополнений в кредитную историю, а также непредставление в установленный срок письменного сообщения о результатах рассмотрения его заявления.

Примерный образец запроса в бюро кредитных историй

Руководителю
_____
от _____
(Ф.И.О. заявителя)
проживающего по адресу: _____
паспортные данные _____

"_"__" _____ 20 __ г.

Запрос о предоставлении отчета по кредитной истории

Прошу в соответствии с ч. 2 ст. 8 ФЗ "О кредитных историях" предоставить полный кредитный отчет по моей кредитной истории.

Подпись

Примерный образец заявления в бюро кредитных историй об исправлении персональных данных

Руководителю
_____
от _____
(Ф.И.О. заявителя)
проживающего по адресу: _____
паспортные данные _____

"___" _____ 20 __ г.

Заявление об исправлении персональных данных в кредитной истории

Прошу в соответствии с ч. 3 ст. 8 ФЗ "О кредитных историях" исправить в моей кредитной истории мои персональные данные, а именно _____.

(перечислить персональные данные, которые требуется исправить)

Подпись

3. Как следует из смысла п. 3 комментируемой статьи, доступ к своим ПД предоставляется субъекту ПД или его законному представителю либо в случае устного обращения к оператору с соответствующей просьбой, либо в случае получения оператором запроса субъекта ПД или его законного представителя.

Авторы рекомендуют в положении о защите персональных данных, разрабатываемом оператором ПД, указывать также перечень информации, которая может быть направлена субъекту ПД по почте либо предоставляться лично.

Отделам кадров в организациях нужно вести журнал учета, в который будут заноситься все факты ознакомления с ПД работников, а также информация о движении документов, включенных в личные дела, и самих личных дел. В таком журнале необходимо фиксировать:

- дату выдачи и возврата документов (личных дел);
- срок пользования документами;
- цель выдачи документов;
- наименовании выдаваемых документов (личных дел).

Далее в присутствии лица, возвращающего личное дело, необходимо сверить по описи наличие всех документов. Лица, получающие документы во временное пользование, должны быть предупреждены о том, что нельзя делать пометки в таких документах, вносить новые записи, извлекать документы из личного дела или помещать в него новые.

Авторы напоминают, что согласно ст. 89 ТК РФ работники организации имеют право на:

- полную информацию об их ПД и обработке этих данных;
- свободный бесплатный доступ к своим ПД, включая право на получение копий любой записи, содержащей ПД работника;
- определение своих представителей для защиты ПД;
- доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;
- требование об исключении или исправлении неверных или неполных ПД, а также данных, обработанных с нарушением требований законодательства о ПД. (при отказе работодателя исключить или исправить ПД работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные ПД работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его ПД.

Сотрудники организации, получившее право работать с ПД, обязаны принять на себя обязательства не разглашать доверенные им сведения, неукоснительно выполнять правила работы с ПД, обеспечивать надежное хранение носителей конфиденциальной информации.

Итак, запрос или обращение о доступе к своим ПД могут исходить как от самого субъекта ПД, так и от его законного представителя. В комментарии к п. 6 ст. 9 Закона разъяснялось понятие "законного представителя". Напомним, что законные представители действуют на основании документов, удостоверяющие их статус и полномочия.

Дееспособный субъект ПД для представления его интересов у оператора ПД может выдать доверенность своему представителю. Согласно ст. 185 ГК РФ доверенностью признается письменное уполномочие, выдаваемое одним лицом другому лицу для представительства перед третьими лицами. Доверенность на совершение сделок, требующих нотариальной формы, должна быть нотариально удостоверена, за исключением случаев, предусмотренных законом. Нотариус удостоверяет доверенности от имени одного или нескольких лиц, на имя одного или нескольких лиц. К нотариально удостоверенным доверенностям приравниваются:

- доверенности военнослужащих и других лиц, находящихся на излечении в госпиталях, санаториях и других военно-лечебных учреждениях, удостоверенные начальником такого учреждения, его заместителем по медицинской части, старшим или дежурным врачом;
- доверенности военнослужащих, а в пунктах дислокации воинских частей, соединений, учреждений и военно-учебных заведений, где нет нотариальных контор и других органов, совершающих нотариальные действия, также доверенности рабочих и служащих, членов их семей и членов семей военнослужащих, удостоверенные командиром (начальником) этих части, соединения, учреждения или заведения;
- доверенности лиц, находящихся в местах лишения свободы, удостоверенные начальником соответствующего места лишения свободы;
- доверенности совершеннолетних дееспособных граждан, находящихся в учреждениях социальной защиты населения,

удостоверенные администрацией этого учреждения или руководителем (его заместителем) соответствующего органа социальной защиты населения.

Обращаем внимание, что срок действия доверенности не может превышать трех лет. Если срок в доверенности не указан, она сохраняет силу в течение года со дня ее совершения. Доверенность, в которой не указана дата ее совершения, ничтожна.

Следует помнить, что лицо, которому выдана доверенность на получение доступа к ПД, должно лично совершать те действия, на которые оно уполномочено. Оно может передоверить их совершение другому лицу, если уполномочено на это доверенностью либо вынуждено к этому силою обстоятельств для охраны интересов лица, выдавшего доверенность. Действие доверенности на получение доступа к ПД прекращается вследствие:

- истечения срока доверенности;
- отмены доверенности лицом, выдавшим ее;
- отказа лица, которому выдана доверенность;
- смерти гражданина, выдавшего доверенность, признания его недееспособным, ограниченно дееспособным или безвестно отсутствующим;
- смерти гражданина, которому выдана доверенность, признания его недееспособным, ограниченно дееспособным или безвестно отсутствующим.

Субъект ПД, выдавший доверенность, может во всякое время отменить доверенность или передоверие, а лицо, которому доверенность выдана, - отказаться от нее.

Законодатель установил, что запрос на получении доступа к ПД должен содержать следующую обязательную информацию:

- номер основного документа, удостоверяющего личность субъекта ПД или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- собственноручную подпись субъекта ПД или его законного представителя.

Согласно постановлению Правительства РФ от 08.07.1997 N 828 "Об утверждении Положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации" основным документом, удостоверяющим личность гражданина РФ на территории РФ является паспорт гражданина РФ. Паспорт обязаны иметь все граждане РФ, достигшие 14-летнего возраста и проживающие на территории РФ. В паспорт вносятся следующие сведения о личности гражданина: фамилия, имя, отчество;

- пол;
- дата рождения;
- место рождения.

Кроме того в паспорте производятся следующие отметки:

- о регистрации гражданина по месту жительства и снятии его с регистрационного учета - соответствующими органами регистрационного учета;
- об отношении к воинской обязанности граждан, достигших 18-летнего возраста;
- о регистрации и расторжении брака;
- о детях;
- о ранее выданных основных документах, удостоверяющих личность гражданина РФ на территории РФ;
- о выдаче основных документов, удостоверяющих личность гражданина РФ за пределами РФ.

По желанию гражданина в паспорте также производятся отметки:

- о его группе крови и резус-факторе;
- об идентификационном номере налогоплательщика.

Срок действия паспорта гражданина:

- от 14 лет - до достижения 20-летнего возраста;
- от 20 лет - до достижения 45-летнего возраста;
- от 45 лет - бессрочно.

По достижении гражданином (за исключением военнослужащих, проходящих службу по призыву) 20-летнего и 45-летнего возраста паспорт подлежит замене. Военнослужащим, проходящим военную службу по призыву, паспорта выдаются или заменяются по окончании установленного срока военной службы по призыву.

Кроме того, в соответствии со ст. 7 Федерального закона от 15.08.1996 N 114-ФЗ "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию" основными документами, удостоверяющими личность гражданина РФ, по которым граждане РФ осуществляют выезд из РФ и въезд в РФ, признаются:

- паспорт;
- дипломатический паспорт;
- служебный паспорт;
- паспорт моряка (удостоверение личности моряка).

Также документами, удостоверяющими личность иностранного гражданина в РФ, согласно положениям Федерального закона от 25.07.2002 N 115-ФЗ "О правовом положении иностранных граждан в Российской Федерации" являются паспорт иностранного гражданина либо иной документ, установленный федеральным законом или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина. Документами, удостоверяющими личность лица без гражданства в РФ, являются:

- документ, выданный иностранным государством и признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность лица без гражданства;

- разрешение на временное проживание;

- вид на жительство;

- иные документы, предусмотренные федеральным законом или признаваемые в соответствии с международным договором РФ в качестве документов, удостоверяющих личность лица без гражданства.

Запрос на доступ к своим ПД может быть составлен как в простой письменной форме на бумажном носители, так и направлен в электронной форме и подписан электронной цифровой подписью. Напоминаем, что особенности использования цифровой подписи определяются ФЗ "Об электронной цифровой подписи". Так, электронным документом признается документ, в котором информация представлена в электронно-цифровой форме. Электронная цифровая подпись - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Владелец сертификата ключа подписи - это физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы). Под средствами электронной цифровой подписи понимаются аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

- создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи;

- подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

- создание закрытых и открытых ключей электронных цифровых подписей.

Закрытый ключ электронной цифровой подписи - это уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Открытый ключ электронной цифровой подписи - это уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Сертификат ключа подписи - это документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Следует помнить, что электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

- подтверждена подлинность электронной цифровой подписи в электронном документе;

- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Согласно ст. 11 ФЗ "Об информации, информационных технологиях и о защите информации" электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе. Таким образом, комментируемая статья Закона признает запрос о доступе к ПД, созданный в электронной форме и подписанный электронной цифровой подписью, равнозначным бумажному документу, подписанному собственноручно субъектом ПД.

4. В п. 4 комментируемой статьи уточняется, получение какой информации может требовать субъект ПД при обращении к оператору ПД с соответствующим запросом. Таким образом, по запросу субъекта ПД оператор обязан предоставить гражданину следующую информацию о его данных, хранящихся у оператора:

- подтверждение факта обработки ПД оператором, а также цель такой обработки;

- способы обработки ПД, применяемые оператором;

- сведения о лицах, которые имеют доступ к ПД или которым может быть предоставлен такой доступ;

- перечень обрабатываемых ПД и источник их получения;

- сроки обработки ПД, в том числе сроки их хранения;

- сведения о том, какие юридические последствия для субъекта ПД может повлечь за собой обработка его ПД.

Примерный образец запроса на предоставлении информации о персональных данных

Руководителю ООО "_____"
г-ну _____
от _____ (Ф.И.О.)
проживающего по адресу: _____
паспортные данные _____
выдан _____

Запрос на получение информации о персональных данных

С мая 2010 года я регулярно получаю именные рекламные материалы Вашей организации на свой адрес.
В соответствии со ст. 14 Закона "О персональных данных" прошу предоставить мне следующие сведения:
- из каких источников Вами были получены мои персональные данные;
- с какой целью они хранятся и используются;
- как обрабатываются (хранятся, систематизируются и распространяются) мои персональные данные;
- кто имеет доступ к данным в настоящее время и кому он может быть предоставлен в будущем;
- каковы сроки хранения данных и порядок их уничтожения.

В соответствии с ч. 1 ст. 14 Закона "О персональных данных", прошу предоставить мне копию всех находящихся в Вашем распоряжении данных, которые имеют ко мне отношение, либо разъяснить мне порядок ознакомления с находящимися у Вас персональными данными.

Дата
Подпись

5. В ряде случаев право субъекта ПД на доступ к своим данным может быть ограничено. Рассмотрим эти случаи.

Во-первых, ограничивается доступ к ПД, если их обработка осуществлялась в целях обороны страны, безопасности государства и охраны правопорядка. Такие данные, как правило, бывают получены в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности.

Во-вторых, ограничивается доступ к ПД, если обработка ПД производится органами, осуществившими задержание субъекта ПД по подозрению в совершении преступления, либо предъявившими субъекту ПД обвинение по уголовному делу, либо применившими к субъекту ПД меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством РФ случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПД. Напоминаем, что задержанием подозреваемого называется мера процессуального принуждения, применяемая органом дознания, дознавателем, следователем на срок не более 48 часов с момента фактического задержания лица по подозрению в совершении преступления. Обвинение - это утверждение о совершении определенным лицом деяния, запрещенного уголовным законом, выдвинутое в порядке, установленном УПК РФ. Мерами пресечения являются:
- подписка о невыезде;
- личное поручительство;
- наблюдение командования воинской части;
- присмотр за несовершеннолетним обвиняемым;
- залог;
- домашний арест;
- заключение под стражу.

Мера пресечения может быть избрана в отношении подозреваемого в исключительных случаях. При этом обвинение должно быть предъявлено подозреваемому не позднее 10 суток с момента применения меры пресечения, а если подозреваемый был задержан, а затем заключен под стражу - в тот же срок с момента задержания.

В-третьих, доступ субъекта ПД к своим данным может быть ограничен, если предоставление ПД нарушает конституционные права и свободы других лиц.

Статья 15. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации

1. Организации, чьими услугами когда-либо пользовались граждане, иногда высылают им свои рекламные материалы. В период выборов в органы государственной власти, органы местного самоуправления граждане также получают адресную агитационную продукцию. Законно ли это?

В п. 1 комментируемой статьи определяются условия обработки ПД путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи:
- в целях продвижения товаров, работ, услуг на рынке (например, рассылка рекламных буклетов);
- в целях политической агитации.

Как упоминалось ранее, согласно абз. 28 ст. 2 ФЗ "О связи" под средствами связи понимаются технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений

электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи.

В свою очередь, реклама - это информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу лиц и направленная на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке. Объектом рекламирования может быть товар, средства индивидуализации юридического лица и (или) товара, изготовитель или продавец товара, результаты интеллектуальной деятельности либо мероприятие (в том числе спортивное соревнование, концерт, конкурс, фестиваль, основанные на риске игры, пари), на привлечение внимания к которым направлена реклама. Товаром называется продукт деятельности (в том числе работа, услуга), предназначенный для продажи, обмена или иного введения в оборот.

Политическая агитация - это устная, печатная или наглядная политическая деятельность, воздействующая на сознание и настроение людей. Цель такой агитации - побудить граждан к определенным политическим действиям.

Пунктом 1 комментируемой статьи законодатель обязывает операторов ПД, обрабатывать данные граждан в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации, только при наличии предварительного согласия субъекта ПД. При чем оператор должен будет доказать, что такое согласие ему было предоставлено субъектом ПД. Поэтому, если организация, получающая ПД гражданина в целях исполнения договора, заключенного между организацией и этим гражданином, планирует в дальнейшем обрабатывать его ПД для продвижения своих услуг, следует позаботиться о получении письменного согласия на то субъекта ПД. По мнению авторов, только письменная форма согласия поможет избежать возникновения спорных ситуаций. Напоминаем, что требования к содержанию письменного согласия на обработку ПД определены в п. 4 ст. 9 комментируемого Закона.

Примерный образец согласия на обработку ПД в целях продвижения товаров, работ или услуг

_____
Наименование (Ф.И.О.) оператора

_____
Адрес оператора

_____
Ф.И.О. субъекта персональных данных

_____
Адрес, где зарегистрирован субъект персональных данных

_____
Номер основного документа, удостоверяющего его личность

_____
Дата выдачи указанного документа

_____
Наименование органа, выдавшего документ

Согласие на обработку персональных данных в целях продвижения товаров и услуг

Я, _____ (Ф.И.О.) даю свое согласие на обработку следующих моих персональных данных:

- Ф.И.О.;
- Почтового адреса;
- Адреса электронной почты.

для рассылки мне рекламной продукции от _____.
(наименование оператора)

Для указанных целей я предоставляю _____
(наименование оператора)

право осуществлять все действия с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

В случае неправомерного использования предоставленных данных настоящее согласие может быть в любое время отозвано мной.

Данное соглашение действует с "__" _____ 20__ г. по "__" _____ 20__ г.

Дата _____
Подпись

Интересно, что в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" закрепляются похожие права субъектов ПД. Так, согласно ст. 14 упомянутого выше документа государства-участники обязаны предоставить субъекту данных право бесплатно высказывать возражение против обработки касающихся его ПД, которые, по мнению контролера, обрабатываются для целей прямого маркетинга, или получать уведомление прежде, чем ПД будут впервые раскрыты третьим сторонам, или использованы по их поручению в целях прямого маркетинга, и в явной форме получать право бесплатно высказывать возражение против такого раскрытия или использования.

2. Из смысла п. 2 комментируемой статьи следует, что гражданин имеет право в любое время отказаться от получения рекламных или агитационных материалов, независимо от формы их получения - по обычной или электронной почте, по факсу или по телефону. Для этого следует уведомить отправителя о несогласии на получение подобных материалов и попросить удалить соответствующие ПД из его базы данных. Законодатель не устанавливает в какой именно форме субъект ПД должен предъявить оператору ПД требование о прекращении обработки его данных. По мнению авторов, такое обращение может быть как письменным, отправленным по месту нахождения оператора ПД, так и устным, заявленным при личной встрече. Пункт 3 ст. 21 комментируемого Закона обязывает оператора ПД в срок, не превышающий трех рабочих дней с даты выявления неправомерных действий с ПД, устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПД, обязан уничтожить такие данные. Об устранении допущенных нарушений или об уничтожении ПД оператор обязан уведомить субъекта ПД или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПД, - также указанный орган.

Примерный образец обращения к руководителю организации, рассылающей рекламную продукцию

Директору ЗАО "_____"
г-ну _____
_____
(Ф.И.О. заявителя)
проживающий по адресу
_____

Требование
о прекращении обработки персональных данных для продвижения товаров и услуг

На мой адрес, а именно _____
(адрес субъекта ПД)
регулярно приходят рекламные проспекты от Вашей организации. Свое согласие на получение рекламной продукции я не давал, поэтому прошу прекратить использование моих персональных данных в соответствии со ст. 14 ФЗ "О персональных данных" для продвижения Ваших товаров и услуг.

В противном случае я буду вынужден обратиться в суд за защитой своих прав и взысканием суммы компенсации за причиненный моральный ущерб. Также предупреждаю Вас об административной ответственности согласно ст. 13.11 КоАП РФ и ответственности в случае немотивированного отказа.

Дата
Подпись

Если несмотря на обращение, оператор не отвечает на требование о прекращении обработки ПД, субъект ПД имеет право подать исковое заявление в суд или обратиться с жалобой в Уполномоченный орган по защите прав субъектов персональных данных.

При обращении в суд с жалобой на неправомерные действия оператора ПД гражданин вправе требовать компенсации причиненного ему морального вреда в соответствии с положениями ст. 151 ГК РФ, поскольку он причинен действиями, которые нарушают личные неимущественные права гражданина (ст. 150 ГК РФ), а именно право на неприкосновенность частной жизни и право на защиту ПД. Так, согласно ст. 151 ГК РФ если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда. При определении размеров компенсации морального вреда суд принимает во внимание степень вины нарушителя и иные заслуживающие внимания обстоятельства.

Примерный образец искового заявления в суд

В _____ районный суд
г. _____
Истец: _____
Адрес:_____
Ответчик: _____
Адрес:_____

Исковое заявление

С "___" _____ 20 __ г. на мой домашний адрес, а именно _____ стали регулярно поступать рекламные буклеты от ЗАО "_____". При этом своего согласия на получение рекламных материалов я не давал.

"__" _____ 20 __ г. я отправил обращение на имя директора ЗАО "_____" с требованием прекратить присылать мне рекламную продукцию. Но никакого ответа не последовало, и рекламная рассылка не прекратилась.

Считаю, что такими действиями ЗАО "_____" причинила мне моральный ущерб на сумму _____ рублей.

На основании вышеизложенного и руководствуясь ст. 6, 14 ФЗ "О персональных данных", ст. 151 ГК РФ, ст. 3 ГПК РФ прошу:

- обязать ЗАО "_____" прекратить присылать рекламную продукцию на мой адрес _____ и исключить мой адрес из базы данных адресов ЗАО "_____";
- взыскать с ЗАО "_____" компенсацию за причиненный мне незаконными действиями моральный вред в сумме _____ рублей.

Приложение:

- квитанция об оплате государственной пошлины
- копия обращение на имя директора ЗАО "_____".

Дата
Подпись

Статья 16. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

1. Комментируемая статья определяет перечень прав субъекта ПД при принятии решений на основании исключительно автоматизированной обработки его данных.

Обратимся к Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных". В ст. 15 указанного документа указываются обязанности государств-участников при принятии ими автоматизированных решений в отношении частных лиц. Так, государства-участники взяли на себя обязательства предоставить каждому лицу право не оказаться под воздействием решения, порождающего юридические последствия в отношении него или существенно воздействующего на него, и основанного исключительно на автоматической обработке данных, предназначенной для оценки некоторых касающихся его личных аспектов, таких как выполнение им своей работы, кредитоспособность, надежность, поведение и т.п.

Важным документом, защищающим права граждан при автоматизированной обработке их данных, является Конвенции Совета Европы о защите личности в связи с автоматической обработкой персональных данных от 28.01.1981 г., в соответствии с которой все ПД, проходящие автоматическую обработку:

- должны быть получены и обработаны добросовестным и законным образом;
- должны накапливаться для точно определенных и законных целей и не использоваться в противоречии с этими целями;
- должны быть адекватными, относящимися к делу и не быть избыточными применительно к целям, для которых они накапливаются;
- должны быть точными и в случае необходимости обновляться и т.д.

Пунктом 1 комментируемой статьи законодатель запрещает принятие на основании исключительно автоматизированной обработки ПД следующих решений в отношении субъекта ПД:

- решений, порождающих юридические последствия в отношении субъекта ПД;

- решений каким-либо образом затрагивающих права и законные интересы субъекта ПД.

Исключение составляют только некоторые случаи, которые будут прокомментированы ниже

2. Итак, решение, порождающее юридические последствия в отношении субъекта ПД или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПД только в следующих случаях:

- при наличии согласия в письменной форме субъекта ПД;

- в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПД.

В п. 2 ст. 15 Директивы 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24.10. 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" также устанавливается, что лицо может оказаться под воздействием решения, принятого на основании обработки его ПД, только если такое решение:

- принято в ходе заключения или исполнения контракта, при условии, что запрос на заключение или исполнение контракта, хранящийся у субъекта данных, был удовлетворен, или что приняты надлежащие меры для обеспечения его законных интересов, такие, как соглашения, позволяющие ему высказать свою точку зрения;

- или санкционировано законом, также устанавливающим меры для обеспечения законных интересов субъекта данных.

Здесь также следует отметить, что согласно ст. 11 Федерального закона от 09.02.2007 N 16-ФЗ "О транспортной безопасности", в целях осуществления мер по обеспечению транспортной безопасности федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере информационных технологий и связи, создается единая государственная информационная система обеспечения транспортной безопасности, являющаяся собственностью РФ. Эта информационная система состоит, в том числе из автоматизированных централизованных баз персональных данных о пассажирах. Такие базы формируются при осуществлении следующих видов перевозок:

- внутренних и международных воздушных перевозок;

- железнодорожных перевозок в дальнем следовании;

- международных перевозок морским, внутренним водным и автомобильным транспортом;

- перевозок железнодорожным, морским, внутренним водным и автомобильным транспортом по отдельным маршрутам, определенным уполномоченным Правительством РФ федеральным органом исполнительной власти по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности РФ и федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере внутренних дел.

Указанные выше автоматизированные централизованные базы ПД пассажиров формируются на основании информации, предоставленной:

- пассажирами и перевозчиками;

- федеральными органами исполнительной власти;

- иностранными государствами и организациями в рамках международного сотрудничества по вопросам обеспечения транспортной безопасности.

Согласно ФЗ "О транспортной безопасности" информационные ресурсы единой государственной информационной системы обеспечения транспортной безопасности являются информацией ограниченного доступа. При этом в базы данных вносятся следующая информация о пассажирах и перевозках:

- фамилия, имя, отчество;

- дата и место рождения;

- вид и номер документа, удостоверяющего личность, по которому приобретается проездной документ (билет);

- пункт отправления, пункт назначения, вид маршрута следования (беспересадочный, транзитный);

- дата поездки.

Необходимо также упомянуть, что порядок формирования и ведения автоматизированных централизованных баз ПД о пассажирах, а также предоставления содержащихся в них данных устанавливается уполномоченным Правительством РФ федеральным органом исполнительной власти. При этом контроль за соблюдением порядка передачи таких сведений в автоматизированные централизованные базы ПД о пассажирах осуществляется федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере транспорта.

Также в ст. 85.1 Воздушного кодекса РФ указывается, что в целях обеспечения авиационной безопасности перевозчики обеспечивают передачу ПД пассажиров воздушных судов в автоматизированные централизованные базы персональных данных о пассажирах в соответствии с ФЗ "О транспортной безопасности" и законодательством РФ в области ПД. Порядок передачи ПД пассажиров воздушных судов в автоматизированные централизованные базы ПД о пассажирах также устанавливается Правительством РФ.

3. Пунктом 3 комментируемой статьи законодатель определяет обязанности оператора ПД в отношении субъекта ПД при принятии решения на основании исключительно автоматизированной обработки его ПД. Таким образом, на оператора ПД возлагаются следующие обязанности:

- обязанность разъяснить субъекту ПД порядок принятия решения на основании исключительно автоматизированной

обработки его ПД;

- обязанность разъяснить субъекту ПД возможные юридические последствия такого решения;
- обязанность предоставить субъекту ПД возможность заявить возражение против такого решения;
- обязанность разъяснить порядок защиты субъектом ПД своих прав и законных интересов.

Надо отметить, что Конвенция Совета Европы о защите личности в связи с автоматической обработкой персональных данных от 28.01.1981 г. предоставляет любому лицу следующие права:

- быть осведомленным о существовании автоматизированной базы ПД, о ее главных целях, а также о контролере базы данных, его месте жительства либо юридическом адресе;
- периодически и без излишних затрат времени или средств обращаться с запросом о том, накапливаются ли в автоматизированной базе данных касающиеся его ПД, и получать информацию о таких данных в доступной форме;
- требовать уточнения или уничтожения таких данных, если они были обработаны с нарушением положений национального права, реализующих основные принципы, изложенные в статьях Конвенции;
- прибегнуть к судебной защите нарушенного права, если его запрос либо требование о предоставлении информации, уточнении или уничтожении данных не были удовлетворены.

4. В п. 4 комментируемой статьи определяется порядок рассмотрения оператором ПД возражения против принятия решения на основании исключительно автоматизированной обработки ПД, направленного ему субъектом ПД. Таким образом, по смыслу анализируемой нормы права такое возражение должно быть оформлено в письменном виде. Таким образом, порядок действий оператора ПД при получении возражения следующий:

- возражение рассматривается оператором в течение семи рабочих дней со дня его получения;
- далее субъекту ПД предоставляется уведомления о результатах рассмотрения такого возражения.

Статья 17. Право на обжалование действий или бездействия оператора

1. Норма, содержащаяся в п. 1 комментируемой статьи, предоставляет право субъекту ПД обжаловать действия или бездействие оператора ПД, если тот осуществляет обработку данных с нарушением требований законодательства о ПД.

Субъект ПД может защитить свои права путем направления жалобы по своему выбору:

- в уполномоченный орган по защите прав субъектов персональных данных;
- в суд.

В настоящее время уполномоченным органом по защите прав субъектов ПД является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Как указывается в постановлении Правительства РФ от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций", Роскомнадзор является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки ПД требованиям законодательства РФ в области ПД, а также функции по организации деятельности радиочастотной службы. Кроме того, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций является уполномоченным федеральным органом исполнительной власти по защите прав субъектов ПД.

Таким образом, с жалобами о нарушении прав граждан в отношении их ПД можно обратиться по адресу: 109074, г. Москва, Китайгородский проезд, д. 7, стр. 2 или по факсу (495) 987-6801. В Роскомнадзор можно направить жалобу заказным письмом или заполнить соответствующую форму на сайте организации, расположенной в Интернете по адресу: http://www.rsoc.ru/treatments/ask-question/.

Жалоба должна содержать:

- фамилию, имя, отчество;
- почтовый и электронный адрес заявителя;
- описание ситуации, при которой были нарушены права заявителя.

Ответ на запрос направляется заявителю на указанный им адрес - почтовый или электронный. Срок рассмотрения обращения, как правило, составляет 30 дней. Обращаем внимание, что вместе с жалобой нужно предоставить максимальный объем имеющейся информации в отношении сложившейся ситуации:

- контактная информация нарушителя;
- время и дата получения сообщения;
- копия сообщения;
- информация о наличии и характере предыдущих контактов с отправителем (например, копии обращений в организацию с требованием прекратить информационные рассылки).

Контактную информацию территориального отделения Роскомнадзора в своем регионе можно найти в Интернете по адресу http://www.rsoc.ru/about/territorial/.

Согласно ст. 3 ГПК РФ заинтересованное лицо вправе обратиться в суд за защитой нарушенных либо оспариваемых прав, свобод или законных интересов.

При обращении в суд субъектам ПД следует учитывать, что исковое заявление подается в письменной форме и в нем должны быть указаны:

- наименование суда, в который подается заявление;
- наименование истца, его место жительства или, если истцом является организация, ее место нахождения, а также

наименование представителя и его адрес, если заявление подается представителем;

- наименование ответчика, его место жительства;
- в чем заключается нарушение либо угроза нарушения прав, свобод или законных интересов истца и его требования;
- обстоятельства, на которых истец основывает свои требования, и доказательства, подтверждающие эти обстоятельства;
- цена иска, если он подлежит оценке, а также расчет взыскиваемых или оспариваемых денежных сумм;
- сведения о соблюдении досудебного порядка обращения к ответчику, если это установлено федеральным законом или предусмотрено договором сторон;
- перечень прилагаемых к заявлению документов.

В заявлении могут быть указаны номера телефонов, факсов, адреса электронной почты истца, его представителя, ответчика, иные сведения, имеющие значение для рассмотрения и разрешения дела, а также изложены ходатайства истца. Исковое заявление подписывается истцом или его представителем при наличии у него полномочий на подписание заявления и предъявление его в суд.

Кроме того к исковому заявлению должны быть приложены:

- его копии в соответствии с количеством ответчиков и третьих лиц;
- документ, подтверждающий уплату государственной пошлины;
- доверенность или иной документ, удостоверяющие полномочия представителя истца;
- документы, подтверждающие обстоятельства, на которых истец основывает свои требования, копии этих документов для ответчиков и третьих лиц, если копии у них отсутствуют;
- текст опубликованного нормативного правового акта в случае его оспаривания;
- доказательство, подтверждающее выполнение обязательного досудебного порядка урегулирования спора, если такой порядок предусмотрен федеральным законом или договором;
- расчет взыскиваемой или оспариваемой денежной суммы, подписанный истцом, его представителем, с копиями в соответствии с количеством ответчиков и третьих лиц.

2. Субъект ПД в судебном порядке может требовать также возмещения убытков; компенсации морального вреда.

Так, ст. 12 ГК РФ установлено, что защита гражданских прав осуществляется путем:

- признания права;
- восстановления положения, существовавшего до нарушения права, и пресечения действий, нарушающих право или создающих угрозу его нарушения;
- признания оспоримой сделки недействительной и применения последствий ее недействительности, применения последствий недействительности ничтожной сделки;
- признания недействительным акта государственного органа или органа местного самоуправления;
- самозащиты права и т.д.

Убытками называются расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода). При этом если лицо, нарушившее право, получило вследствие этого доходы, лицо, право которого нарушено, вправе требовать возмещения наряду с другими убытками упущенной выгоды в размере не меньшем, чем такие доходы.

Кроме того субъект ПД вправе требовать возмещения убытков, причиненных ему в результате незаконных действий (бездействия) государственных органов, органов местного самоуправления или должностных лиц этих органов в отношении обработки ПД этого субъекта. Такие убытки подлежат возмещению РФ, соответствующим субъектом РФ или муниципальным образованием.

Как упоминалось ранее, если субъекту ПД причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его права при обработке ПД, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда.

Примерный образец искового заявления в суд от имени работника организации

В _____ районный суд
г. _____
Истец: _____
Адрес:_____
Ответчик: _____
Адрес:_____

Исковое заявление

Я работаю в ЗАО "_____" с "___" _____ 20 __ г. При

заключении трудового договора я передал в отдел кадров этой организации свои персональные данные, а именно:_____
_____.
(перечислить персональные данные)

"___" _____ 20 __ г. я обнаружил свои персональные данные в общедоступном корпоративном справочнике. Однако своего согласия на включение моих персональных данных в общедоступный источник информации я не давал. Поэтому "__" _____ 20 __ г. я обратился к руководителю нашей организации _____ (Ф.И.О. руководителя) с требованием исключить мои персональные данные из справочника, но он проигнорировал мою просьбу.

Считаю, что такими действиями ЗАО "_____" причинило мне моральный ущерб на сумму _____ рублей.

На основании вышеизложенного и руководствуясь ст. 88-90 ТК РФ, ст. 6, 8 ФЗ "О персональных данных", ст. 151 ГК РФ, ст. 3 ГПК РФ прошу:

- обязать ЗАО "_____" исключить мои персональные данные из корпоративного справочника;
- взыскать с ЗАО "_____" компенсацию за причиненный их незаконными действиями моральный вред в сумме _____ рублей;
- взыскать с ЗАО "_____" расходы по оплате мною государственной пошлины в сумме _____ рублей и услуг юриста в сумме _____ рублей.

Приложение:

- квитанция об оплате государственной пошлины;
- копия обращение на имя директора ЗАО "_____" от "___" _____ 20 __ г.
- квитанцию об оплате услуг юридического агентства.

Дата
Подпись

Глава 4. Обязанности оператора

Статья 18. Обязанности оператора при сборе персональных данных

1. Со ст. 18 начинается новая глава комментируемого Закона, устанавливающая обязанности оператора ПД.

Пунктом 1 комментируемой статьи законодатель закрепляет за оператором ПД обязанность предоставить субъекту ПД по его просьбе следующую информацию:

- подтверждение факта обработки ПД оператором, а также цель такой обработки;
- способы обработки ПД, применяемые оператором;
- сведения о лицах, которые имеют доступ к ПД или которым может быть предоставлен такой доступ;
- перечень обрабатываемых ПД и источник их получения;
- сроки обработки ПД, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта ПД может повлечь за собой обработка его ПД.

Законодатель не устанавливает, в какой форме (письменной или устной) оператор ПД должен предоставить субъекту данных вышеуказанную информацию. Следовательно ответ на такой запрос может быть выдан в любой форме, согласованной сторонами.

Примерный образец ответа на запрос субъекта ПД о предоставлении информации о его данных

Г-ну _____,
проживающему по адресу: _____.

Ответ на запрос о предоставлении информации
от "___" _____ 20 __ г.

Уважаемый _____!

На Ваш запрос от "___" _____ 20 __ г. сообщаем следующее:

1) Ваши персональные данные, а именно _____,
(перечень персональных данных)
получены нашей организацией _____
(наименование организации, адрес)
из общедоступного источника информации, а именно _____
_____
(указать источник информации)
и обрабатываются с целью _____;
(указать цель обработки);

2) способы обработки Ваших персональных данных _____
_____;

3) к вашим персональным данным имеют доступ следующие лица, с которыми заключены соглашения о неразглашении конфиденциальной информации: _____ (ф.и.о. лиц);

4) предполагаемый срок обработки Ваших персональных данных: _____
_____. По окончании указанного срока Ваши персональные данные будут уничтожены.

В случае Вашего несогласия на обработку нашей организацией Ваших данных, вы можете заявить об этом по адресу: _____.

Дата
Подпись должностного лица организации

Напоминаем, что данная информация должна быть предоставлена оператором ПД при устном обращении к нему субъекта ПД или при получении от субъекта ПД соответствующего письменного запроса.

2. Как упоминалось в комментарии к п. 2 ст. 9 комментируемого Закона в ряде случаев требуется обязательное предоставление субъектом ПД своих данных. Это может быть:

- в целях защиты основ конституционного строя;
- в целях защиты нравственности, здоровья, прав и законных интересов других лиц;
- в целях обеспечения обороны страны и безопасности государства.

Например, ст. 308 УПК РФ предусмотрено наказание за отказ свидетеля или потерпевшего от дачи показаний по уголовному делу в виде штрафа в размере до сорока тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до трех месяцев. Однако лицо не подлежит уголовной ответственности за отказ от дачи показаний против себя самого, своего супруга или своих близких родственников. Следователь, привлекая к участию в следственных действиях участников уголовного судопроизводства:

- удостоверяется в их личности;
- разъясняет им права, ответственность, а также порядок производства.

Согласно ст. 189 УПК РФ по инициативе следователя или по ходатайству допрашиваемого лица в ходе допроса могут быть проведены фотографирование, аудио- и (или) видеозапись, киносъемка, материалы которых хранятся при уголовном деле и по окончании предварительного следствия опечатываются.

3. В п. 3 комментируемой статьи законодатель определяет обязанности оператора ПД при обработке данных, которые были получены у третьих лиц.

Обратимся к Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных". Похожая норма права закреплена в ст. 11 этого документа. На государств-участников возлагается обязанность обеспечить, чтобы контролер (физическое или юридическое лицо, официальный орган, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных) или его представитель на момент документирования данных, которые были получены не у субъекта данных, или в случае, когда предполагается разглашение данных третьей стороне, не позднее времени, когда данные впервые разглашаются, предоставили субъекту данных следующую информацию:

- личность контролера или его представителя, если таковой имеется;
- цели обработки;
- категории используемых данных;
- получатели или категории получателей данных;
- наличие права доступа и права уточнять касающиеся его данные в той мере, в какой требуется дополнительная

информация, касающаяся конкретных обстоятельств, при которых собираются данные;

- гарантии корректной обработки применительно к субъекту данных.

Однако эти правила не применяется в тех случаях, когда для обработки в статистических целях или же в целях исторических или научных исследований, предоставление такой информации оказывается невозможным или может повлечь непропорциональные усилия, или же если документирование или разглашение прямо определяются законом.

Возвратимся к анализу содержания п. 3 комментируемой статьи. До начала обработки тех данных, которые были получены не у субъекта ПД, оператор обязан предоставить гражданину уведомление о планируемой обработке. Законодатель предъявляет определенные требования к содержанию такого уведомления, стремясь максимально защитить права и интересы субъекта ПД.

Примерный образец уведомления об обработке ПД, полученных у третьих лиц

Уважаемый _____!

Уведомляем Вас, что наша организация планирует получить дополнительную информацию о Вас, а именно _____
_____
(перечень персональных данных, которые планируется получить)
из организации, в которой Вы ранее работали _____.
(наименование организации)

В соответствии с п. 3 ст. 18 ФЗ "О персональных данных" сообщаем Вам следующую информацию:

- Наименование организации-оператора "_____", адрес: _____, контактный телефон _____, руководитель организации: _____.
- Цель обработки персональных данных: _____;
- Предполагаемые пользователи персональных данных: _____
_____.

В случае Вашего несогласия на обработку нашей организацией Ваших данных, вы можете заявить об этом по адресу: _____
_____.

Дата
Подпись должностного лица организации

Настоящее уведомление на руки получил:
_____ подпись субъекта персональных данных

Законодатель установил исключения из правила, содержащегося в п. 3 комментируемой статьи. Так, предоставления указанного выше уведомления не требуется:

- если ПД были предоставлены оператору на основании федерального закона;
- если ПД являются общедоступными.

Так, например, уполномоченные государственные органы, осуществляющие оперативно-розыскную деятельность или обеспечение безопасности РФ, могут на основании ст. 64 ФЗ "О связи" получать у операторов связи информацию о пользователях услугами связи и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач. Из общедоступных источников информации, т.е. из баз, содержащих ПД, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта данных, операторы также могут получать данные без уведомления субъекта ПД об обработке такой информации.

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

1. Законодатель возлагает на оператора ПД обязанность принимать необходимые организационные и технические меры для защиты данных:

- от неправомерного или случайного доступа к ним;
- от уничтожения, изменения, блокирования, копирования, распространения;
- от иных неправомерных действий.

При этом обеспечение безопасности ПД должно осуществляться в соответствии с методическими документами Федеральной службы по техническому и экспортному контролю (далее по тексту - ФСТЭК России), такими как:

- "Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных" от 15 февраля 2008 г.;

- "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 г.;

- "Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 г.;

- "Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 г.

Следует отметить, что Федеральным законом от 27.12.2009 N 363-ФЗ "О внесении изменений в статьи 19 и 25 Федерального закона "О персональных данных" в п. 1 комментируемой статьи были внесены изменения, которые вступили в силу 29.12.2009 года. Ранее на операторов ПД также возлагалась обязанность использования криптосредств для защиты ПД в соответствии с:

- приказом ФСБ России от 09.02.2005 N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации";

- постановлением Правительства РФ от 29.12.2007 N 957 "Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами";

- методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, от 21.02.2008 N 149/54-144);

- типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, от 21.02.2008 N 149/6/6-622).

Но практика показала, что выполнение всех этих требований операторами ПД является очень дорогостоящей и практически невыполнимой задачей. Первоначально комментируемый Закон обязывал операторов ПД привести свои информационные системы в соответствии с требованиями нового законодательства в срок до 1 января 2010 года. Однако, как отмечают многие исследователи, даже крупные организации, обрабатывающие ПД, такие как государственные и муниципальные органы, банки и т.п. не смогли вовремя это выполнить. Поэтому Федеральный закон от 27.12.2009 N 363-ФЗ "О внесении изменений в статьи 19 и 25 Федерального закона "О персональных данных" продлил упомянутый выше срок до 01.01.2011 года. Кроме того с операторов ПД сняли обязанность использовать шифровальные (криптографические) средства. Федеральным законом от 23.12.2010 N 359-ФЗ указанный срок был дополнительно продлен до 1 июля 2011 года.

Требования об обеспечении мер защиты ПД содержатся и в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных". Согласно ст. 17 этого документа государства-участники обязаны обеспечить, чтобы контролер (физическое или юридическое лицо, официальный орган, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных) реализовал надлежащие технические и организационные меры для защиты ПД от случайного или незаконного уничтожения или случайной утраты, изменения, неправомерного раскрытия или доступа, в частности, когда обработка влечет передачу данных по сети, а также от всех иных незаконных форм обработки. С учетом состояния и стоимости их реализации такие меры должны обеспечить надлежащий уровень безопасности для рисков, представленных обработкой и природой защищаемых данных. Также государства-участники должны обеспечить, чтобы контролер - в случае, если обработка осуществляется по его поручению - избрал обработчика, предоставляющего достаточные гарантии в отношении мер технической безопасности и организационных мер, регулирующих осуществляемую обработку, и обеспечил соблюдение таких мер.

На основании анализа комментируемого Закона выделим некоторые требования, которые должен учитывать оператор ПД для обеспечения безопасности и защиты данных в процессе их обработки.

Во-первых, всем операторам ПД необходимо закрепить документально основные понятия обработки ПД, такие как цель обработки; способы обработки; сведения о лицах, имеющих доступ к ПД; перечень обрабатываемых ПД; источник получения; сроки обработки и хранения ПД.

Необходимость анализа всех обрабатываемых организацией ПД и аккумулирования этой информации в едином документе обусловлена требованием к технической защите обрабатываемых оператором ПД. Приказом ФСТЭК России, ФСБ России и Мининформсвязи от 13.02.2008 N 55/86/20 "Об утверждении порядка проведения классификации информационных систем персональных данных" при классификации информационных систем с целью определения уровня их защиты и степени расходования средств организации на техническую защиту ПД субъектов учитываются категории обрабатываемых ПД и их объем. Поэтому и возникает необходимость такую информацию фиксировать и документировать

Во-вторых, организациям следует установить сроки хранения ПД. При этом необходимо заранее продумать обоснование выбранных сроков хранения.

В-третьих, мероприятия по обеспечению безопасности ПД при их обработке в информационных системах должны включать в себя учет лиц, допущенных к работе с ПД в информационных системах. Нужно помнить, что лица, доступ которых к ПД, обрабатываемым в информационной системе, необходим для выполнения служебных обязанностей, должны допускаться к таким данным на основании списка, утвержденного уполномоченным лицом оператора ПД.

В-четвертых, оператором ПД должны быть реализованы следующие механизмы защиты:

- регистрация и учет;

- обеспечение целостности;
- обеспечение антивирусной защиты.

Функционал, который должны выполнять данные механизмы, определен в методических документах ФСБ России и ФСТЭК России по защите ПД. Такие механизмы призваны предотвращать несанкционированный доступ к ПД и обеспечивать своевременное обнаружение фактов несанкционированного доступа к ним.

В-пятых, оператору ПД следует разработать ряд локальных документов, таких как:

- приказ о создании комиссии по защите ПД с наделением ее полномочий по проведению всех мероприятий, касающихся организации защиты ПД;
- положение о ПД и их защите;
- инструкцию о порядке обеспечения конфиденциальности при обращении с информацией, содержащей ПД;
- приказы о возложении персональной ответственности за защиту ПД;
- форму согласия субъекта ПД на их обработку, в случаях определенных комментируемым Законом;
- перечень информационных систем, обрабатывающих ПД;
- регламент допуска сотрудников к обработке ПД;
- перечень сотрудников, допущенных к обработке ПД;
- должностные инструкции сотрудников, имеющих отношение к обработке ПД.

В-шестых, должна быть осуществлена классификация информационных систем ПД на основании приказа ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных". При этом модель угроз создается, на основании методических документов ФСТЭК России и ФСБ России, а также актуальных угроз безопасности ПД при их обработке в информационных системах данных.

2. Основные требования к обеспечению безопасности ПД при их обработке в информационных системах содержатся в Постановлении Правительства РФ от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных". Рассмотрим основные положения этого документа.

Обращаем внимание, что требования указанного выше Постановления распространяются на обработку ПД, если данные обрабатываются в информационных системах ПД, представляющих собой совокупность ПД, содержащихся в базах данных, и информационных технологий и технических средств, позволяющих осуществлять обработку таких данных с использованием средств автоматизации.

Следует знать, что техническими средствами, позволяющими осуществлять обработку ПД, называются:

- средства вычислительной техники;
- информационно-вычислительные комплексы и сети;
- средства и системы звукозаписи, звукоусиления, звуковоспроизведения;
- переговорные и телевизионные устройства;
- средства изготовления, тиражирования документов;
- технические средства обработки речевой, графической, видео- и буквенно-цифровой информации;
- программные средства (операционные системы, системы управления базами данных и т.п.);
- средства защиты информации, применяемые в информационных системах.

Идем дальше. Безопасность ПД при их обработке в информационных системах должна достигаться следующими способами:

- путем исключения несанкционированного, в том числе случайного, доступа к ПД, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПД, а также иных несанкционированных действий;
- должны применяться средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПД, а также используемые в информационной системе информационные технологии;
- технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям Федерального закона от 27.12.2002 N 184-ФЗ "О техническом регулировании";
- должна быть обеспечена защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Также необходимо учитывать, что методы и способы защиты информации в информационных системах установлены приказом ФСТЭК РФ от 05.02.2010 N 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных". Достаточность принятых мер по обеспечению безопасности ПД при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

Итак, для выбора и реализации методов и способов защиты информации в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности ПД. Также позволяется привлекать организацию, имеющую оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Обращаем внимание, что выбор и реализация методов и способов защиты информации в информационной системе

осуществляются на основе определяемых оператором (уполномоченным лицом) угроз безопасности ПД (модели угроз) и в зависимости от класса информационной системы, определенного в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 N 55/86/20.

Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с п. 2 постановления Правительства РФ от 17.11.2007 N 781. Следует помнить, что выбранные и реализованные методы и способы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности ПД при их обработке в информационных системах в составе создаваемой оператором (уполномоченным лицом) системы защиты ПД.

Рассмотрим некоторые методы и способы защиты ПД.

Методы и способы защиты ПД от несанкционированного доступа:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПД, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку ПД, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку ПД;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

Операторам ПД необходимо помнить, что методы и способы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия в зависимости от класса информационной системы определяются оператором (уполномоченным лицом) в соответствии с Приложением к Положению о методах и способах защиты информации в информационных системах ПД, утвержденным приказом ФСТЭК РФ от 05.02.2010 N 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных".

В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (например, к базам данных, размещенным в сети Интернет) или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты. При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (Интернет) кроме вышеперечисленных методов и способов защиты информации от несанкционированного доступа следует использовать следующую защиту:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защита информации при ее передаче по каналам связи;
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
- использование средств антивирусной защиты;
- централизованное управление системой защиты персональных данных информационной системы.

Особое внимание авторы обращают на то, что подключение информационных систем, обрабатывающих государственные информационные ресурсы, к информационно-телекоммуникационным сетям международного информационного обмена осуществляется в соответствии с Указом Президента РФ от 17.03.2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена".

Методы и способы защиты информации от утечки по техническим каналам.

Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, осуществляется в случаях, когда при определении угроз безопасности персональных данных и формировании модели угроз применительно к информационной системе являются актуальными угрозы утечки акустической речевой информации, угрозы утечки видовой информации и угрозы утечки информации по каналам побочных

электромагнитных излучений и наводок, определенные на основе методических документов, утвержденных в соответствии с п. 2 постановления Правительства РФ от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".

Напоминаем, что порядок проведения классификации информационных систем устанавливается приказом Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13.02.2008 N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" (см. комментарий к ст. 3 Закона). Таким образом, для исключения утечки ПД за счет побочных электромагнитных излучений и наводок в информационных системах 1 класса могут применяться следующие методы и способы защиты информации:

- использование технических средств в защищенном исполнении;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- размещение объектов защиты в соответствии с предписанием на эксплуатацию;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;
- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

В информационных системах 2 класса для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники. При применении в информационных системах функции голосового ввода ПД в информационную систему или функции воспроизведения информации акустическими средствами информационных систем для информационной системы 1 класса реализуются методы и способы защиты акустической (речевой) информации.

Необходимо учитывать, что методы и способы защиты акустической (речевой) информации заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе ПД в информационной системе или воспроизведении информации акустическими средствами. При этом величина звукоизоляции определяется оператором исходя из характеристик помещения, его расположения и особенностей обработки ПД в информационной системе. Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

Идем дальше. Как упоминалось в комментарии к ст. 3 Закона, средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Информационные системы классифицируются органами и лицами, осуществляющими обработку ПД, а также определяющими цели и содержание обработки данных, т.е. операторами ПД, а именно:

- государственными органами;
- муниципальными органами;
- юридическими или физическими лицами.

Классификация осуществляется в зависимости от объема обрабатываемых ими ПД и угроз безопасности жизненно важным интересам личности, общества и государства.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с ПД, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПД и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц. Возможные каналы утечки информации при обработке ПД в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности РФ в пределах их полномочий.

Важно учитывать, что безопасность ПД при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку ПД. Существенным условием такого договора является обязанность уполномоченного лица обеспечить конфиденциальность и безопасность ПД при их обработке в информационной системе.

Таким образом, при обработке ПД в информационной системе должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПД и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к ПД;
- недопущение воздействия на технические средства автоматизированной обработки ПД, в результате которого может быть нарушено их функционирование;

- возможность незамедлительного восстановления ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- постоянный контроль за обеспечением уровня защищенности ПД.

Мероприятия по обеспечению безопасности ПД при их обработке в информационных системах в соответствии с требованиями постановления Правительства РФ от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" должны включать в себя:

- определение угроз безопасности ПД при их обработке, формирование на их основе модели угроз;

- разработку на основе модели угроз системы защиты ПД, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПД, предусмотренных для соответствующего класса информационных систем;

- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

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

- учет лиц, допущенных к работе с ПД в информационной системе;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПД, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПД или другим нарушениям, приводящим к снижению уровня защищенности ПД, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание системы защиты ПД.

Как разъяснялось ранее, обработка ПД может осуществляться как в информационных системах ПД, таки без использования средств автоматизации. Часто операторы ПД, владея большими базами данных, все же не могут определиться, обрабатывать ли им данные вручную или с помощью средств автоматизации. Из содержания комментируемого Закона улавливается, что оператор должен самостоятельно принимать решение о форме обработки ПД.

Согласно п. 2 комментируемой статьи особые требования предъявляются законодателем и к материальным носителям биометрических ПД, а также к технологиям хранения таких данных вне информационных систем ПД. Такие требования установлены в постановлении Правительства РФ от 06.07.2008 N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных" и анализировались авторами в комментарии к ст. 11 Закона.

3. Законодатель определяет органы, контролирующие выполнение операторами ПД требований, установленных п. 2 комментируемой статьи. Такими органами в настоящее время являются:

- Федеральная служба безопасности Российской Федерации (далее по тексту - ФСБ России);

- Федеральная служба по техническому и экспортному контролю (далее по тексту - ФСТЭК России).

Как указывается в Указе Президента РФ от 11.08.2003 N 960 "Вопросы Федеральной службы безопасности Российской Федерации", ФСБ России кроме всего прочего является федеральным органом исполнительной власти, в пределах своих полномочий обеспечивающим информационную безопасность РФ.

Из основных функций и задач ФСБ России можно выделить, к примеру, следующие:

- организация в пределах своих полномочий и во взаимодействии с органами внешней разведки РФ добывания и обработки разведывательной информации;

- формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности;

- организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в РФ и ее учреждениях за рубежом и т.д.

ФСБ России также координирует деятельность:

- федеральных органов исполнительной власти и организаций по обеспечению криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в РФ и ее учреждениях за рубежом;

- федеральных органов исполнительной власти в области разработки, производства, закупки, ввоза в РФ и вывоза из РФ специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, а также их оперативных подразделений по выявлению нарушений установленного порядка разработки, производства, реализации, приобретения в целях продажи, ввоза в РФ и вывоза из РФ специальных технических средств, предназначенных для негласного получения информации.

Кроме того согласно постановлению Правительства РФ от 26.01.2006 N 45 "Об организации лицензирования отдельных видов деятельности" ФСБ России осуществляет лицензирование следующих видов деятельности:

- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)

- деятельность по распространению шифровальных (криптографических) средств;

- деятельность по техническому обслуживанию шифровальных (криптографических) средств;

- предоставление услуг в области шифрования информации

- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности, например, обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов РФ информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям.

Кроме того, ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля. Также ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну, организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.

Среди основных задач ФСТЭК России можно назвать следующие:

- реализация в пределах своей компетенции государственной политики в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации;

- осуществление государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

- обеспечение в пределах своей компетенции безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов РФ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ, органах местного самоуправления и организациях;

- прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации;

- противодействие добыванию информации техническими средствами разведки, техническая защита информации.

Приведем в качестве примера некоторые полномочия ФСТЭК России:

- разрабатывает стратегию и определяет приоритетные направления деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации;

- разрабатывает и вносит в установленном порядке Президенту РФ и в Правительство РФ проекты законодательных и иных нормативных правовых актов РФ по вопросам своей деятельности;

- осуществляет межотраслевую координацию деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов РФ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ, органах местного самоуправления и организациях;

- осуществляет в пределах своей компетенции контроль за состоянием работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации и т.д. (подробнее см. Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю").

Согласно постановлению Правительства РФ от 26.01.2006 N 45 "Об организации лицензирования отдельных видов деятельности" ФСТЭК России осуществляет лицензирование следующих видов деятельности:

- деятельность по технической защите конфиденциальной информации;

- деятельность по разработке и (или) производству средств защиты конфиденциальной информации (совместно с ФСБ России).

4. Пункт 4 комментируемой статьи определяет условия использования и хранения биометрических ПД вне информационных систем ПД. Такими условиями являются:

- использование биометрических ПД может осуществляться только на материальных носителях информации;

- должна применяться технологии хранения информации, которая будет обеспечивать защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

Напоминаем, что порядок использования и хранения биометрических ПД вне информационных систем ПД закреплен также в постановлении Правительства РФ от 06.07.2008 N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных" и анализировался в комментарии к ст. 11 Закона.

Статья 20. Обязанности оператора при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

1. Комментируемая статья по своей сути дополняет ст. 14, 18 Закона. Так, в ответ на запрос субъекта ПД или его представителя о предоставлении информации о ПД, относящихся к этому субъекту, оператор ПД обязан:

- сообщить субъекту ПД или его законному представителю информацию о наличии данных, относящихся к соответствующему субъекту ПД;

- предоставить возможность ознакомления с этими данными.

Предоставление возможности ознакомления с ПД должно быть организовано оператором:

- при обращении субъекта ПД или его законного представителя;

- либо в течение десяти рабочих дней с даты получения запроса субъекта ПД или его законного представителя.

Согласно постановлению Правительства РФ от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" запросы пользователей информационной системы на получение ПД, а также факты предоставления ПД по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора или уполномоченного лица. При обнаружении нарушений порядка предоставления ПД оператор или уполномоченное лицо незамедлительно приостанавливают предоставление информации пользователям информационной системы до выявления причин нарушений и устранения этих причин.

2. Как разъяснялось в комментарии к п. 5 ст. 14 Закона в ряде случаев субъекту ПД оператором ПД может быть отказано в предоставлении информации об этих данных.

Это возможно если:

- обработка ПД, в том числе данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

- обработка ПД осуществляется органами, осуществившими задержание субъекта ПД по подозрению в совершении преступления, либо предъявившими субъекту данных обвинение по уголовному делу, либо применившими к субъекту ПД меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством РФ случаев, если допускается ознакомление подозреваемого или обвиняемого с такими данными;

- предоставление ПД нарушает конституционные права и свободы других лиц.

Отказ в предоставлении информации о ПД должен быть:

- мотивированным;

- оформленным в письменном виде;

- содержать ссылку на положение п. 5 ст. 14 комментируемого Закона или иного федерального закона, являющееся основанием для такого отказа;

- должен быть передан субъекту ПД или его законному представителю в срок, не превышающий семи рабочих дней со дня обращения субъекта ПД или его законного представителя либо с даты получения запроса субъекта ПД или его законного представителя.

Примерный образец мотивированного отказа в предоставлении информации о ПД субъекту ПД

Г-ну _____,
проживающему по адресу: _____.

Ответ на запрос о предоставлении информации
от "___" _____ 20 __ г.

Уважаемый _____!

На Ваш запрос от "___" _____ 20 __ г. сообщаем, что вам отказывается в предоставлении такой информации на основании п. 5 ст. 14

ФЗ "О персональных данных" и ФЗ "Об оперативно-розыскной деятельности".

Дата
Подпись должностного лица организации

3. В соответствии с п. 3 комментируемой статьи оператор обязан:

- безвозмездно предоставить субъекту ПД или его законному представителю возможность ознакомления с данными, относящимися к соответствующему субъекту ПД;
- в случае необходимости внести в данные необходимые изменения, уничтожить или блокировать соответствующие ПД;
- уведомить субъекта ПД или его законного представителя и третьих лиц, которым ПД этого субъекта были переданы, о внесенных изменениях и предпринятых мерах.

Законодатель определяет условия, при которых на оператора ПД возлагается обязанность внести в данные необходимые изменения, уничтожить или блокировать их. Это должно произойти в случае предоставления субъектом ПД или его законным представителем сведений, подтверждающих, что ПД, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются:

- неполными;
- устаревшими;
- недостоверными;
- незаконно полученными;
- не являются необходимыми для заявленной цели обработки.

Примерный образец уведомления об уничтожения персональных данных

Г-ну _____,
проживающему по адресу: _____.

Уведомление об уничтожении персональных данных

Уважаемый _____!

Сообщаем Вам, что в связи с _____
_____
(указать причины уничтожения персональных данных)
обработка Ваших персональных данных, а именно _____
_____
(перечислить персональные данные)
прекращена, и Ваши персональные данные будут уничтожены
"___" _____ 200_г.

Дата
Подпись должностного лица организации

Настоящее уведомление на руки получил:
_____ подпись субъекта персональных данных

4. В том случае, если оператором получен запрос от Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), то оператор обязан предоставить информацию, необходимую для осуществления деятельности этого органа, в течение семи рабочих дней с даты получения такого запроса.

Статья 21. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных

1.В п. 1 комментируемой статьи законодатель определяет порядок действий оператора ПД при обращении или по запросу субъекта данных или его законного представителя либо Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в случаях:

- выявления недостоверных ПД;
- выявления неправомерных действий с ПД.

Оператор обязан осуществить блокирование ПД, относящихся к соответствующему субъекту данных, с момента такого обращения или получения такого запроса на весь период проверки. Напоминаем, что под блокированием ПД подразумевается

временное прекращение сбора, систематизации, накопления, использования, распространения ПД, в том числе их передачи.

2. Идем дальше. Итак, получив информацию о недостоверности ПД в соответствии с п. 1 комментируемой статьи оператор обязан:

- блокировать ПД;
- на основании документов, представленных субъектом ПД или его законным представителем либо Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), осуществить проверку данных на предмет подтверждения (опровержения) факта недостоверности ПД;
- уточнить ПД на основании документов, представленных субъектом ПД или его законным представителем либо Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);
- снять блокирование с ПД.

Примерный образец заявления об исправление ПД в личном деле работника

Руководителю
ЗАО "_____"
Адрес: _____
_____ (Ф.И.О. заявителя)
проживающего по адресу:
_____
паспортные данные _____

"___" _____ 20 __ г.

Заявление об исправлении персональных данных в личном деле

Прошу Вас в соответствии со ст. 89 Трудового кодекса Российской Федерации, а также ст. 21 ФЗ "О персональных данных" исправить в моем личном деле мои персональные данные, а именно, удалить сведения о судимости в связи с тем, что судимость была погашена в январе 2010 года.

Приложение
- справка из Главного информационно-аналитического центра МВД России об отсутствии судимости

Подпись

Примерный образец заявления об исправлении персональных данных в истории болезни

Заведующему поликлиникой N __
_____
(Ф.И.О. заведующего)
От _____ (Ф.И.О. заявителя)
проживающего по адресу: _____
паспортные данные _____

"___" _____ 20 __ г.

Заявление об исправлении персональных данных в истории болезни

"__" _____ 20 __ г. врач _____ (Ф.И.О. врача)
ошибочно внес в мою историю болезни запись о том, что _____
_____.
(указать допущенные неточности)

Я обратился к врачу _____ с просьбой удалить ошибочную запись в моей истории болезни, но получил немотивированный отказ.

В соответствии со ст. 21 ФЗ "О персональных данных" и ст. 30 Основ законодательства Российской Федерации об охране здоровья граждан" прошу

внести исправления в мою историю болезни и удалить ошибочную запись о _____ от "___" _____ 20 __ г.

Подпись

3. Пунктом 3 комментируемой статьи законодатель устанавливает сроки, в течение которых оператор ПД обязан устранить допущенные нарушения в случае выявления неправомерных действий с ПД. Оператор ПД обязан это сделать в течение трех рабочих дней с даты выявления неправомерных действий. Если устранить допущенные нарушения по каким-либо причинам не представляется возможным, оператор обязан в вышеуказанный срок уничтожить ПД. Напоминаем, чтоб уничтожение ПД - это действия, в результате которых невозможно восстановить содержание ПД в информационной системе данных или в результате которых уничтожаются материальные носители ПД.

После устранения допущенных нарушений или после уничтожения ПД оператор обязан об этом уведомить субъекта ПД или его законного представителя, а в случае, если обращение или запрос были направлены Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), то также указанный орган.

Примерный образец уведомления об уничтожении ПД

Г-ну _____,
проживающему по адресу: _____.

Уведомление об уничтожении персональных данных

Уважаемый _____!
Сообщаем Вам, что не удалось устранить допущенные нарушения в процессе обработки Ваших ПД, а именно: _____
_____
(перечислить выявленные неправомерные действия с ПД)
в связи с _____
_____.
(указать причины, по котором невозможно устранить допущенные нарушения)
Поэтому в соответствии с п. 3 ст. 21 ФЗ "О персональных данных"
Ваши данные _____
(перечислить персональные данные)
были уничтожены "__" _____ г.

Дата
Подпись должностного лица организации

Настоящее уведомление на руки получил:
_____ подпись субъекта персональных данных

4. Пункт 4 комментируемой статьи конкретизирует один из принципов обработки ПД, изложенный в п. 2 ст. 5 Закона. Авторы напоминают, что согласно вышеупомянутой статье Закона ПД подлежат уничтожению в случае:

- достижения целей обработки;
- в случае утраты необходимости в достижении целей обработки.

Таким образом, законодатель возлагает на оператора ПД обязанность в случае достижения цели обработки ПД:

- незамедлительно прекратить обработку ПД;
- уничтожить соответствующие ПД в срок, не превышающий трех рабочих дней с даты достижения цели обработки ПД, кроме ряда случаев специально предусмотренных федеральными законами;
- уведомить об уничтожении ПД субъекта данных или его законного представителя, а в случае, если обращение или запрос были направлены Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), то также указанный орган.

Так, например, если гражданин обратился в кадровое агентство с целью содействия в трудоустройстве и с этой целью предоставил свои ПД, то после получения гражданином работы кадровое агентство обязано удалить его данные.

Примерный образец уведомления об уничтожении ПД

Г-ну _____,
проживающему по адресу: _____.

Уведомление об уничтожении персональных данных в связи с достижением целей их обработки

Уважаемый _____!
Сообщаем Вам, что в связи с достижением целей обработки Ваших персональных данных, а именно _____
(указать достигнутые цели обработки данных)
Ваши данные _____
(перечислить персональные данные)
были уничтожены "__" _____ г.

Дата
Подпись должностного лица организации

Настоящее уведомление на руки получил:
_____ подпись субъекта персональных данных

5. Согласно п. 1 ст. 9 комментируемого Закона согласие на обработку ПД может быть отозвано субъектом ПД. В том случае, если согласие на обработку ПД предоставлялось в письменной форме, порядок отзыва согласия должен был фиксироваться в содержании этого документа. Пунктом 5 комментируемой статьи законодатель регламентирует дальнейшие действия оператора ПД после получения им отзыва субъектом данных согласия на обработку своих данных. Оператор ПД обязан:

- прекратить обработку данных;
- уничтожить данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных;
- уведомить субъекта ПД о таком уничтожении данных.

Вместе с тем буквальный анализ представленной нормы позволяет отметить, что законодатель позволяет оператору ПД и субъекту ПД самостоятельно определять порядок действий с ПД на основании соглашения, заключенного сторонами.

Примерный образец уведомления об уничтожении ПД

Г-ну _____,
проживающему по адресу: _____.

Уведомление об уничтожении персональных данных в связи с отзывом согласия на обработку персональных данных

Уважаемый _____!
Уведомляем Вас, что в связи с отзывом Вашего согласия на обработку Ваших персональных данных, поступившим в нашу организацию "___" _____ г. Ваши данные _____
(перечислить персональные данные)
были уничтожены "__" _____ г.

Дата
Подпись должностного лица организации

Настоящее уведомление на руки получил:
_____ подпись субъекта персональных данных

Статья 22. Уведомление об обработке персональных данных

1. Первоначально обязанность уведомлять уполномоченный орган о начале обработки ПД была закреплена в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных". Согласно ст. 18 упомянутого выше документа государства-участники обязаны обеспечить, чтобы контролер (физическое или юридическое лицо, официальный

орган, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных) или его представитель, если таковой имеется, уведомили уполномоченный орган перед осуществлением полностью или частично любой операции по автоматической обработке данных, либо набора таких операций, предназначенных служить единой цели или нескольким связанным целям.

Как упоминалось выше в Российской Федерации таким уполномоченным органом, который обязаны уведомить операторы ПД перед началом обработки данных, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

2. В ряде случаев законодатель позволяет осуществлять обработку ПД без предварительного уведомления о том Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Рассмотрим эти случаи.

Во-первых, оператор вправе осуществлять без уведомления Роскомнадзора обработку ПД, относящихся к субъектам ПД, которых связывают с оператором трудовые отношения. Таким образом, если организация обрабатывает только ПД своих сотрудников, уведомлять Роскомнадзор ей не потребуется. Однако, по мнению авторов, в этом контексте речь не идет о гражданско-правовых отношениях. Поэтому в отношении лиц, которые работают в организации по договорам подряда или возмездного оказания услуг, воспользоваться данной нормой нельзя.

Во-вторых, оператор вправе не уведомлять Роскомнадзор, если он обрабатывает ПД, полученные в связи с заключением договора, стороной которого является субъект ПД. Но здесь существует ряд ограничений. Воспользоваться этой нормой права оператор может лишь при выполнении ряда условий:

- ПД не должны распространяться;
- ПД не должны предоставляться третьим лицам без согласия субъекта ПД;
- ПД должны использоваться оператором исключительно для исполнения указанного договора и заключения договоров с субъектом ПД.

Например, если организация заключает с рядом работников договоры гражданско-правового характеры и выполняет вышеперечисленные условия, уведомлять уполномоченный орган также не потребуется.

В-третьих, не обязаны уведомлять Роскомнадзор общественные объединения или религиозные организации, действующие в соответствии с законодательством РФ, если:

- они обрабатывают только данные своих членов (участников) для достижения законных целей, предусмотренных их учредительными документами;
- такие ПД не распространяются без согласия в письменной форме субъектов ПД.

Согласно ст. 5 ФЗ "Об общественных объединениях" под общественным объединением понимается добровольное, самоуправляемое, некоммерческое формирование, созданное по инициативе граждан, объединившихся на основе общности интересов для реализации общих целей, указанных в уставе общественного объединения. Учредителями общественного объединения являются физические лица и юридические лица - общественные объединения, созвавшие съезд (конференцию) или общее собрание, на котором принимается устав общественного объединения, формируются его руководящие и контрольно-ревизионный органы. Общественные объединения могут создаваться в одной из следующих организационно-правовых форм: общественная организация; общественное движение; общественный фонд; общественное учреждение; орган общественной самодеятельности; политическая партия.

Так, общественной организацией является основанное на членстве общественное объединение, созданное на основе совместной деятельности для защиты общих интересов и достижения уставных целей объединившихся граждан.

Общественным движением является состоящее из участников и не имеющее членства массовое общественное объединение, преследующее социальные, политические и иные общественно полезные цели, поддерживаемые участниками общественного движения.

Общественный фонд - это один из видов некоммерческих фондов, представляющий собой не имеющее членства общественное объединение, цель которого заключается в формировании имущества на основе добровольных взносов, иных не запрещенных законом поступлений и использовании данного имущества на общественно полезные цели. Учредители и управляющие имуществом общественного фонда не вправе использовать указанное имущество в собственных интересах.

Общественным учреждением является не имеющее членства общественное объединение, ставящее своей целью оказание конкретного вида услуг, отвечающих интересам участников и соответствующих уставным целям указанного объединения.

Органом общественной самодеятельности является не имеющее членства общественное объединение, целью которого является совместное решение различных социальных проблем, возникающих у граждан по месту жительства, работы или учебы, направленное на удовлетворение потребностей неограниченного круга лиц, чьи интересы связаны с достижением уставных целей и реализацией программ органа общественной самодеятельности по месту его создания.

Политическая партия - это общественное объединение, созданное в целях участия граждан РФ в политической жизни общества посредством формирования и выражения их политической воли, участия в общественных и политических акциях, в выборах и референдумах, а также в целях представления интересов граждан в органах государственной власти и органах местного самоуправления.

Религиозным объединением в РФ признается добровольное объединение граждан Российской Федерации, иных лиц, постоянно и на законных основаниях проживающих на территории РФ, образованное в целях совместного исповедания и распространения веры и обладающее соответствующими этой цели признаками:

- вероисповедание;

- совершение богослужений, других религиозных обрядов и церемоний;

- обучение религии и религиозное воспитание своих последователей.

В свою очередь религиозные объединения могут создаваться в форме религиозных групп и религиозных организаций.

Религиозной группой признается добровольное объединение граждан, образованное в целях совместного исповедания и распространения веры, осуществляющее деятельность без государственной регистрации и приобретения правоспособности юридического лица.

Религиозной организацией признается добровольное объединение граждан РФ, иных лиц, постоянно и на законных основаниях проживающих на территории РФ, образованное в целях совместного исповедания и распространения веры и в установленном законом порядке зарегистрированное в качестве юридического лица.

В-четвертых, не требуется уведомлять Роскомнадзор, если оператор обрабатывает только общедоступные персональные данные, т.е. такие данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПД или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

В-пятых, требования об уведомлении Роскомнадзора перед началом обработки ПД не распространяются на операторов, обрабатывающих данные, содержащие только фамилии, имена и отчества субъектов ПД. Так, например, если ресторан резервируя столики за посетителями, просит у граждан сообщить их фамилию, имя и отчество, то такая обработка данных может осуществляться без уведомления Роскомнадзора.

В-шестых, в целях однократного пропуска субъекта ПД на определенную территорию, на которой находится оператор (например, в гостиницу), или в иных аналогичных целях (например, при выдаче гражданину пропуска для разового посещения организации) уведомлять уполномоченный орган также не нужно.

В-седьмых, требование, указанное в п. 1 комментируемой статьи не распространяется на обработку данных включенных в:

- информационные системы ПД, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем;

- в государственные информационные системы ПД, созданные в целях защиты безопасности государства и общественного порядка.

И, в-восьмых, возможна обработка ПД без предварительного уведомления Роскомнадзора, если обработка осуществляется без использования средств автоматизации в соответствии с требованиями постановления Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации". Содержание этого документа анализировалось в комментарии к ст. 1 Закона.

Комментируемая статья своим содержанием похожа на положение, закрепленное в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных". Так, государствам-участникам позволяется освободить операторов ПД от уведомления надзорного органа об обработке ПД в следующих случаях:

- если обработка данных без уведомления не может существенно нарушить права и свободы субъекта данных;

- если контролер (физическое или юридическое лицо, официальный орган, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных), в соответствии с национальным законом, регулирующим его деятельность, назначает должностное лицо по защите персональных данных, ответственное за обеспечение применения национальных положений, принятых на Директивы и за ведение реестра операций по обработке, проводимых контролером, таким образом гарантируя, что права и свободы субъекта данных едва ли могут быть существенно нарушены операциями по обработке.

Кроме того государствам-участникам разрешается оговорить, что об отдельных либо всех неавтоматизированных операциях по обработке, касающихся ПД, должно делаться уведомление, либо установить для таких операций упрощенное уведомление

3. Пунктом 3 комментируемой статьи законодателем устанавливаются требования к содержанию уведомления, которое в соответствии с п. 1 направляется оператором ПД в Роскомнадзор.

Согласно ст. 19 Директивы 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" государства-участники имеют право самостоятельно определить информацию, указываемую в уведомлении. Однако уведомление в обязательном порядке должно содержать:

- имя (наименование) и адрес контролера и его представителя, если таковой имеется;

- цель или цели обработки;

- описание категории или категорий субъекта данных и данных, или категории относящихся к ним данных;

- получателей или категории получателей, которым могут раскрываться данные;

- предполагаемую передачу в третьи страны;

- общее описание, позволяющее произвести предварительную оценку правомерности мер, принятых для обеспечения безопасности обработки.

Образец уведомления об обработке ПД в РФ утвержден приказом Роскомнадзора от 16.07.2010 N 482 "Об утверждении образца формы уведомления об обработке персональных данных". Этот же нормативный правовой акт содержит рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) ПД.

Примерный образец заполнения уведомления об обработке ПД для оператора, являющегося юридическим лицом

Руководителю Управления
Федеральной службы по надзору
в сфере связи, информационных
технологий и массовых коммуникаций
по Челябинской области
А.А. Балакину

Пр. Карла Маркса, д. 18
г. Челябинск, 454003

Уведомление
об обработке персональных данных

1. Тип оператора: юридическое лицо.
2. Наименование, адрес оператора:
полное наименование с указанием организационно-правовой формы: Общество с ограниченной ответственностью "Салют".
сокращенное наименование юридического лица (оператора), осуществляющего обработку персональных данных: ООО "Салют".
наименование филиала (представительства) юридического лица (оператора), осуществляющего обработку персональных данных: Филиал ООО "Салют" в городе Магнитогорске.
место нахождения: 454000, Российская Федерация, Челябинская область, город Челябинск, пр. Карла Маркса, дом 11.
ИНН: 7400000000.
ОГРН: 74000000.
ОКВЭД: 560000.
ОКПО: 430000.
ОКОГУ: 8500000.
ОКОП: 360000.
ОКФС: 890000.
3. Цель обработки персональных данных:
- кадровый и бухгалтерский учет сотрудников;
- заключение договорных отношений с физическими лицами на оказание услуг в сфере трудоустройства.
4. Категории персональных данных:
непосредственно персональные данные:
- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- семейное, социальное положение;
- образование, профессия;
- паспортные данные;
- данные трудовой книжки;
- данные военного билета;
- сведения о пенсионном страховании;
- ИНН.
специальные категории персональных данных:
- состояние здоровья;
- национальная принадлежность.
биометрические персональные данные: нет
5. Категории субъектов, персональные данные которых обрабатываются:
- работники организации, состоящие в трудовых отношениях с юридическим лицом (оператором);
- физические лица (клиенты) состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором).
6. Правовое основание:
- ст. 23, 24 Конституции Российской Федерации;
- ст. 85-90 Трудового кодекса Российской Федерации;
- ст.ст 2, 5, 6, 7, 9, 18-22 ФЗ "О персональных данных" от 27 июля 2006 г. N 152-ФЗ,
- устав ООО "Салют", Положение о защите персональных данных работников и клиентов ООО "Салют" от 10 мая 2009 г.

N 12;

- Федеральный закон от 08.02.1998 N 14-ФЗ "Об обществах с ограниченной ответственностью".

7. Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных:

смешанная обработка персональных данных:

неавтоматизированная обработка:

- ведение трудовых книжек;
- ведение личных дел на работников ООО "Салют";
- учет и хранение договоров, заключенными с физическими лицами (клиентами).
- автоматизированная: в ходе обработки информация доступна лишь для строго определенных сотрудников юридического лица, информация не передается с использованием сети общего пользования Интернет.

8. Описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных:

- соблюдение положений Трудового кодекса Российской Федерации; Федерального закона "О персональных данных" от 27 июля 2006 г. N 152-ФЗ;
- технические меры:
- использование программного обеспечение _____ (производитель _____) серийный номер N 55000, заводской N 22200);
- электронный ключ для ограничения доступа к автоматизированным рабочим местам, на которых осуществляется обработка персональных данных (_____);
- присвоение персональных паролей для каждого рабочего места (конкретного работника);
- установлена защита Антивирус Касперского версия 6.0. лиц. соглашение N 5230000;
- класс информационной системы персональных данных _____, уровень криптографической защиты ___, уровень специальной защиты от утечки по каналам побочных излучений ___, уровень защиты от несанкционированного доступа ___.
- установлены сейфы для хранения личных дел работников ООО "Салют" и персональных данных обрабатываемых клиентов;
- установлена охранная сигнализация.

9. Дата начала обработки персональных данных: 10 мая2010 года.

10. Срок или условие прекращения обработки персональных данных:

прекращение договорных отношений с работниками организации и клиентами.

ликвидация ООО "Салют".

11. Территория обработки: г. Челябинск г. Магнитогорск,

12. Трансграничная передача персональных данных: нет

Директор А.А. Шмелев
Подпись, печать

Следует помнить, что уведомление должно быть составлено исключительно в письменной или электронной форме и подписано соответственно уполномоченным лицом или электронной цифровой подписью. Напоминаем, что согласно ФЗ "Об электронной цифровой подписи" электронный документ - это документ, в котором информация представлена в электронно-цифровой форме, а электронная цифровая подпись - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. При этом электронная цифровая подпись в электронном документе будет равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Таким образом, уведомление, присланное посредством факсимильной связи не принимается Роскомнадзором.

4. Уведомление об обработке ПД, направляемое в Роскомнадзор, должно быть оформлено на бланке оператора. Документ должен быть зарегистрирован и иметь исходящий номер и дату. Кроме полного наименования оператора требуется указывать и сокращенное, причем в точном соответствии с учредительными документами. Обязательно указание адреса юридического лица. Кроме указания ИНН, желательно указывать и ОГРН (основной государственный номер организации). При заполнении поля "правовое обеспечение обработки персональных данных" должны быть как минимум указаны:

- ст. 85-90 Трудового кодекса РФ;
- устав;
- положение об обработке ПД в организации;
- номер, дата лицензии;

- статьи ФЗ "О персональных данных";

- отраслевые нормативно-правовые акты, которыми руководствуется юридическое лицо, обрабатывая персональные данные, с указанием статей и пунктов.

Обращаем внимание, что "цель обработки" указана в учредительных документах организации. Это цель деятельности оператора. При заполнении поля "категории обрабатываемых персональных данных" необходимо указать именно те категории, которые обрабатывается непосредственно оператором. При заполнении поля "категории субъектов, персональные данные которых обрабатываются" указываются категории субъектов (физические лица) и виды отношений с ними. Например: работники (субъекты), состоящие в трудовых отношениях с юридическим лицом (оператором), физические лица, состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором). *(13)

В поле "перечень действий и способы обработки" помимо самого перечня, необходимо указывать способ обработки: неавтоматизированная, исключительно автоматизированная, смешанная. При автоматизированной или смешанной обработке, обязательно необходимо указать, передается ли полученная в ходе обработки персональных данных информация по внутренней сети юридического лица (информация доступна лишь для строго определенных сотрудников) либо информация передается с использованием сети общего пользования Интернет либо без передачи полученной информации. В поле "описание мер по обеспечению безопасности" указываются организационные и технические меры. В том числе необходимо обязательно указывать, используются ли шифровальные (криптографические) средства. Кроме того, обращаем ваше внимание на то, что в уведомлении следует обязательно указывать, имеет ли место трансграничная передача персональных данных.

При заполнении поля "дата начала обработки персональных данных" необходимо за дату начала обработки брать дату, когда были произведены последние изменения по одному из пунктов уведомления (возможно, это реорганизация, смена наименования).

В поле "срок или условие прекращения обработки персональных данных" следует указать конкретную дату или основание (условие), наступление которого повлечет прекращение обработки ПД. Данное основание тесным образом связано с целями обработки, при достижении целей обработка должна быть прекращена.

В течение 30 дней оператор включается в реестр операторов ПД. Сведения, содержащиеся в реестре, за исключением сведений о средствах обеспечения безопасности ПД при их обработке, являются общедоступными.*(14)

5. Операторы ПД должны помнить, что на них не могут быть возложены расходы, связанные с рассмотрением уведомления об обработке ПД и внесением изменений в реестр операторов ПД. Так в Постановлении Правительства РФ от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" указывается, что Роскомнадзор не вправе оказывать платные услуги в установленной сфере ведения, кроме случаев, установленных федеральными законами, указами Президента РФ и постановлениями Правительства РФ.

6. В случае если уведомление содержит неполную или недостоверную информацию, оно принимается к обработке, но временно отклоняется. Оператору направляется соответствующее письмо о необходимости предоставления недостающей информации.

Роскомнадзор вправе, по результатам анализа обработанного уведомления:

- осуществлять проверку достоверности предоставленной оператором информации, содержащейся в уведомлении об обработке ПД;

- привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

- запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию, в том числе в случае необходимости уточнения или дополнения недостающих сведений.

Кроме того операторы ПД могут быть привлечены к административной ответственности в соответствии со ст. 19.7 КоАП РФ в случае непредставления или несвоевременного представление в Роскомнадзор уведомления об обработке ПД. Напоминаем, что такое уведомление должно быть предоставлено в уполномоченный орган до начала обработки ПД.

7. В случае изменения сведений, содержащихся в представленном ранее уведомлении, оператор ПД обязан уведомить территориальное управление Роскомнадзора об изменениях в течение 10 рабочих дней с даты возникновения таких изменений. Уведомление об изменении сведений предоставляется оператором в виде информационного письма с указанием причин внесения изменений. Вместе с информационным письмом оператор обязан представить в качестве приложения уведомление с измененными сведениями в письменной форме, подписанное уполномоченным лицом или в электронной форме, подписанное электронной цифровой подписью. На основании результатов проверки сведений, содержащихся в полученном уведомлении Роскомнадзор в течение 30 дней, с даты поступления уведомления издает приказ о внесении изменений в реестр операторов. Внесение изменений в реестр может быть обжаловано в порядке, установленном законодательством РФ.

Получить информацию о данных реестра операторов можно в Интернете по адресу: http://pd.rsoc.ru/operators-registry/operators-list/.

Глава 5. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований настоящего федерального закона

Статья 23. Уполномоченный орган по защите прав субъектов персональных данных

1. Комментируемой статьей начинается последняя глава Закона, определяющая порядок контроля и надзора за

обработкой ПД, а также устанавливающая ответственность за нарушение требований Закона.

Как упоминалось ранее, в настоящее время уполномоченным органом по защите прав субъектов ПД на который возлагается обеспечение контроля и надзора за соответствием обработки ПД требованиям комментируемого Закона, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Положение о Роскомнадзоре утверждено постановлением Правительства РФ от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций".

Таким образом, Роскомнадзор является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки ПД требованиям законодательства РФ в области ПД, а также функции по организации деятельности радиочастотной службы. Также Роскомнадзор является уполномоченным федеральным органом исполнительной власти по защите прав субъектов ПД. Роскомнадзор находится в ведении Министерства связи и массовых коммуникаций РФ.

Роскомнадзор руководствуется в своей деятельности:

- Конституцией РФ;
- федеральными конституционными законами;
- федеральными законами;
- актами Президента РФ и Правительства РФ;
- международными договорами РФ;
- нормативными правовыми актами Министерства связи и массовых коммуникаций РФ;
- упомянутым выше положением о Роскомнадзоре.

Обращаем внимание, что Роскомнадзор осуществляет свою деятельность непосредственно и через свои территориальные органы во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ, органами местного самоуправления, общественными объединениями и иными организациями.

Официальный сайт Роскомнадзора находится в сети Интернет по адресу: http://www.rsoc.ru/. Список и контактную информацию территориальных органов Роскомнадзора можно посмотреть здесь: http://www.rsoc.ru/about/territorial/.

Рассмотрим некоторые полномочия Роскомнадзора. Итак, Роскомнадзор кроме всего прочего осуществляет государственный контроль и надзор за соблюдением законодательства РФ в сфере информационных технологий:

- за соблюдением требований обязательной сертификации или декларирования соответствия информационных технологий, предназначенных для обработки государственного банка данных о детях, оставшихся без попечения родителей;
- за соответствием обработки ПД требованиям законодательства РФ в области ПД;
- за представлением обязательного федерального экземпляра документов в установленной сфере деятельности Службы.

Роскомнадзор ведет следующие реестры:

- реестр операторов, занимающих существенное положение в сети связи общего пользования;
- единые общероссийские реестры средств массовой информации;
- реестры лицензий;
- реестр операторов, осуществляющих обработку ПД.

Роскомнадзор организует также формирование и ведение реестра федеральных государственных информационных систем, осуществляет прием граждан и обеспечивает своевременное и полное рассмотрение устных и письменных обращений граждан, принятие по ним решений и направление заявителям ответов в установленный законодательством РФ срок, обеспечивает защиту сведений, составляющих государственную тайну, в процессе деятельности Службы, а также контроль за деятельностью ее территориальных органов и подведомственных организаций.

Роскомнадзор взаимодействует в установленном порядке с органами государственной власти иностранных государств и международными организациями в установленной сфере ведения, осуществляет в соответствии с законодательством РФ работу по комплектованию, хранению, учету и использованию архивных документов, образовавшихся в процессе деятельности Службы.

Отметим также, что Роскомнадзор возглавляет руководитель, назначаемый на должность и освобождаемый от должности Правительством РФ по представлению Министра связи и массовых коммуникаций РФ. Руководитель Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций несет персональную ответственность за осуществление возложенных на Службу полномочий. Руководитель Службы имеет заместителей, назначаемых на должность и освобождаемых от должности Министром связи и массовых коммуникаций РФ по представлению руководителя Службы. Количество заместителей руководителя Службы устанавливается Правительством РФ.

Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" также содержит нормы, подразумевающие создание органа надзора. Так, согласно ст. 28 каждое государство-участник должно назначить один или несколько государственных органов для надзора за соблюдением на своей территории положений, принятых государствами-участниками во исполнение Директивы. При выполнении возложенных на них обязанностей указанные органы должны действовать в условиях полной независимости. При этом каждое государство-участник должно создать условия для проведения консультаций с органами надзора при разработке административных мер или правил, касающихся защиты прав и свобод индивидуумов в отношении обработки их ПД. Согласно Директиве каждый орган надзора должен наделяется следующими полномочиями:

- полномочиями для проведения расследований, в том числе правом доступа к данным, являющимся предметом операций по обработке данных, а также правом получения любой информации, необходимой для исполнения его обязанностей по надзору;

- реальными полномочиями для вмешательства в процесс обработки, в том числе правом вынесения суждений до начала операций по обработке данных, а также обеспечения надлежащего уровня гласности в отношении таких суждений;

- правом отдавать распоряжения относительно блокирования, стирания или уничтожения данных, налагать временный или постоянный запрет на обработку данных, выносить предупреждения и налагать взыскания на контрольный орган, а также передавать такого рода дела на рассмотрение национальных парламентов или иных политических структур;

- полномочиями для возбуждения юридических дел в случаях нарушения национальных положений, принятых во исполнение Директивы, а также для привлечения внимания судебных органов к упомянутым нарушениям.

2. Одной из основных функций Роскомнадзора является рассмотрение обращений субъектов ПД о соответствии содержания ПД и способов обработки их целям. В результате рассмотрения таких обращений Роскомнадзор принимает соответствующее решение.

Комментируемая норма права является развитием нормы, содержащейся в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных", согласно которой каждый орган надзора обязан рассматривать жалобы, поданные любым лицом или представляющей это лицо ассоциацией касательно защиты его прав и свобод в отношении обработки ПД. Заинтересованное лицо должно быть проинформировано о результатах рассмотрения жалобы. Каждый орган надзора обязан, в частности, рассматривать иски любого лица о проверке законности обработки данных в случаях, когда действуют национальные положения, принятые во исполнение Директивы. При этом податель иска должен быть проинформирован о факте проведения проверки.

Порядок подачи субъектом ПД обращения или заявления в Роскомнадзор рассматривался в комментарии к ст. 17 Закона.

3. Пункт 3 комментируемой статьи определяет основные права Роскомнадзора, которыми он обладает, осуществляя контроль и надзор в сфере обеспечения защиты ПД.

Следует также учитывать, что Роскомнадзор обладает следующими правами, перечисленными в постановлении Правительства РФ от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций". Итак, Роскомнадзор имеет право:

- запрашивать и получать в установленном порядке сведения, необходимые для принятия решений по вопросам, отнесенным к компетенции Службы;

- проводить необходимые расследования, испытания, экспертизы, анализы и оценки, а также научные исследования по вопросам, отнесенным к компетенции Службы;

- привлекать в установленном порядке для проработки вопросов, отнесенных к компетенции Службы, научные и иные организации, а также ученых и специалистов;

- давать государственным органам, органам местного самоуправления, юридическим и физическим лицам разъяснения по вопросам, отнесенным к компетенции Службы;

- в порядке и случаях, которые установлены законодательством РФ, применять в установленной сфере ведения меры профилактического и пресекательного характера, направленные на недопущение нарушений юридическими лицами и гражданами обязательных требований в этой сфере и (или) ликвидацию последствий таких нарушений;

- создавать совещательные и экспертные органы (советы, комиссии, группы и коллегии), в том числе межведомственные, в установленной сфере ведения;

- осуществлять контроль за деятельностью территориальных органов Службы, а также за деятельностью подведомственных организаций;

- утверждать образцы служебных удостоверений.

Обеспечивая контроль и надзор за выполнение операторами ПД действующего законодательства в области защиты ПД и комментируемого Закона Роскомнадзор обладает следующими правами:

- правом запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию (при получении обращения субъекта ПД о нарушении его прав Роскомнадзор может потребовать оператора ПД, жалоба в отношении которого поступила, представить некоторые документы для проведения проверки);

- правом осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий (например, при получении уведомления об обработке ПД, направленного в Роскомнадзор оператором ПД и содержащее неполные сведении, Роскомнадзор может потребовать оператора представить дополнительную информацию о себе);

- правом требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных (такое требование может быть отправлено операторам ПД в форме предписания);

- правом принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки ПД, осуществляемой с нарушением требований комментируемого Закона (виновные лица могут быть привлечены к административной и уголовной ответственности, деятельность организаций может быть приостановлена).

- правом обращаться в суд с исковыми заявлениями в защиту прав субъектов ПД и представлять интересы субъектов ПД в суде (например, после получения жалобы от субъекта ПД и проведения соответствующей проверки Роскомнадзор может

обратиться в суд за защитой прав этого субъекта данных).

Кроме того Роскомнадзор обладает правом направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством РФ порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу ПД третьим лицам без согласия в письменной форме субъекта ПД. Авторы напоминают, что в соответствии со ст. 13 Федерального закона от 08.08.2001 N 128-ФЗ "О лицензировании отдельных видов деятельности" приостановление действия лицензии осуществляется лицензирующим органом в случае привлечения лицензиата за нарушение лицензионных требований и условий к административной ответственности в порядке, установленном КоАП РФ. В случае вынесения судьей решения об административном приостановлении деятельности лицензиата за нарушение лицензионных требований и условий лицензирующий орган в течение суток со дня вступления данного решения в законную силу приостанавливает действие лицензии на срок административного приостановления деятельности лицензиата. Далее лицензиат обязан уведомить в письменной форме лицензирующий орган об устранении им нарушения лицензионных требований и условий, повлекшего за собой административное приостановление деятельности лицензиата. В этом случае действие лицензии возобновляется лицензирующим органом со дня, следующего за днем истечения срока административного приостановления деятельности лицензиата, или со дня, следующего за днем досрочного прекращения исполнения административного наказания в виде административного приостановления деятельности лицензиата. В случае если в установленный судьей срок лицензиат не устранил нарушение лицензионных требований и условий, повлекшее за собой административное приостановление деятельности лицензиата, лицензирующий орган обязан обратиться в суд с заявлением об аннулировании лицензии. Лицензия аннулируется решением суда на основании рассмотрения заявления лицензирующего органа.

Роскомнадзор также вправе направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПД, в соответствии с подведомственностью.

Прокуратура РФ - это единая федеральная централизованная система органов, осуществляющих от имени РФ надзор за соблюдением Конституции РФ и исполнением законов, действующих на территории РФ (ст. 1 Федеральный закон от 17.01.1992 N 2202-I "О прокуратуре Российской Федерации"). В целях обеспечения верховенства закона, единства и укрепления законности, защиты прав и свобод человека и гражданина, а также охраняемых законом интересов общества и государства прокуратура РФ осуществляет:

- надзор за исполнением законов федеральными министерствами, государственными комитетами, службами и иными федеральными органами исполнительной власти, представительными (законодательными) и исполнительными органами субъектов РФ, органами местного самоуправления, органами военного управления, органами контроля, их должностными лицами, субъектами осуществления общественного контроля за обеспечением прав человека в местах принудительного содержания и содействия лицам, находящимся в местах принудительного содержания, органами управления и руководителями коммерческих и некоммерческих организаций, а также за соответствием законам издаваемых ими правовых актов;

- надзор за соблюдением прав и свобод человека и гражданина федеральными министерствами, государственными комитетами, службами и иными федеральными органами исполнительной власти, представительными (законодательными) и исполнительными органами субъектов РФ, органами местного самоуправления, органами военного управления, органами контроля, их должностными лицами, субъектами осуществления общественного контроля за обеспечением прав человека в местах принудительного содержания и содействия лицам, находящимся в местах принудительного содержания, а также органами управления и руководителями коммерческих и некоммерческих организаций и т.д. (подробнее см. указанный Федеральный закон).

Под правоохранительной деятельностью в РФ понимается вид государственной деятельности, которая осуществляется с целью охраны права путем применения юридических мер воздействия в строгом соответствии с законом и при неуклонном соблюдении установленного им порядка.

К государственным правоохранительным органам можно отнести:

- суд;
- прокуратуру;
- органы юстиции;
- органы внутренних дел;
- органы предварительного расследования;
- таможенные органы;
- службу по контролю за наркотическими средствами и психотропными веществами;
- органы обеспечения безопасности.

К негосударственным органам, осуществляющим правоохранительную деятельность можно отнести:

- адвокатуру;
- частный нотариат;
- частные детективные и охранные службы.

Следуем дальше. Роскомнадзор обладает правом вносить в Правительство РФ предложения о совершенствовании нормативного правового регулирования защиты прав субъектов ПД. Напоминаем, что в соответствии с Федеральным конституционным законом от 17.12.1997 N 2-ФКЗ "О Правительстве Российской Федерации" Правительство РФ является

органом государственной власти РФ, осуществляет исполнительную власть РФ, в пределах своих полномочий организует исполнение Конституции РФ, федеральных конституционных законов, федеральных законов, указов Президента РФ, международных договоров РФ, осуществляет систематический контроль за их исполнением федеральными органами исполнительной власти и органами исполнительной власти субъектов РФ, принимает меры по устранению нарушений законодательства РФ.

Роскомнадзор вправе привлекать к административной ответственности лиц, виновных в нарушении комментируемого Закона. В РФ административным правонарушением признается противоправное, виновное действие (бездействие) физического или юридического лица, за которое КоАП РФ или законами субъектов РФ об административных правонарушениях установлена административная ответственность. Юридическое лицо признается виновным в совершении административного правонарушения, если будет установлено, что у него имелась возможность для соблюдения правил и норм, за нарушение которых КоАП РФ или законами субъекта РФ предусмотрена административная ответственность, но данным лицом не были приняты все зависящие от него меры по их соблюдению. Порядок привлечения к административной ответственности за невыполнение норм комментируемого Закона будет рассмотрен подробно ниже.

4. Законодатель обязывает сотрудников Роскомнадзора обеспечивать конфиденциальность ПД. Норма, идентичная изложенной в п. 4 комментируемой статьи, содержится и в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных". Так, государства-участники взяли на себя обязательства обеспечить соблюдение членами и сотрудниками органов надзора профессиональной тайны в отношении конфиденциальной информации, к которой они имеют доступ, даже после окончания срока их службы в указанных органах.

5. В п. 5 комментируемой статьи законодатель устанавливает обязанности Роскомнадзора, как уполномоченного органа по защите прав субъектов ПД. Таким образом, Роскомнадзор обязан:

- организовывать в соответствии с требованиями комментируемого Закона и других федеральных законов защиту прав субъектов ПД;

- рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой ПД, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений (с жалобами о нарушении прав граждан в отношении их ПД можно обратиться по адресу: 109074, г. Москва, Китайгородский проезд, д. 7, стр. 2 или по факсу (495) 987-6801, направив жалобу заказным письмом, или заполнить соответствующую форму на сайте организации, расположенной в Интернете по адресу: http://www.rsoc.ru/treatments/ask-question.)

- вести реестр операторов (доступ к реестру операторов ПД находится в Интернете по адресу: http://www.rsoc.ru/personal-data/register/);

- осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных (27 октября 2010 г. по инициативе Роскомнадзора и при поддержке Минкомсвязи РФ состоялась I Международная конференция "Защита персональных данных", в которой приняли участие представители Минкомсвязи России, Министерства юстиции России, ФСБ, ФСТЭК, других заинтересованных министерств и ведомств, Государственной думы, Исполнительного комитета СНГ, Организации Договора коллективной безопасности, специалисты в области информационной безопасности).

- принимать в установленном законодательством РФ порядке по представлению ФСБ России или ФСТЭК России меры по приостановлению или прекращению обработки ПД;

- информировать государственные органы, а также субъектов ПД по их обращениям или запросам о положении дел в области защиты прав субъектов ПД;

- выполнять иные предусмотренные законодательством РФ обязанности.

6. Законодатель установил, что решения Роскомнадзора могут быть обжалованы в судебном порядке. Отметим, что согласно Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" решения органа надзора, повлекшие за собой подачу жалоб, также могут быть опротестованы в судебном порядке.

7. В соответствии с положениями Директивы 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" каждый орган надзора обязан составлять регулярные отчеты о своей деятельности. В директиве указывается также, что такие отчеты должны подлежать опубликованию.

Комментируемый Закон содержит подобную норму. На Роскомнадзор возлагается обязанность направлять отчет о своей деятельности Президенту РФ, в Правительство РФ и Федеральное Собрание РФ. Такой отчет подлежит опубликованию в средствах массовой информации.

8. В соответствии с постановлением Правительства РФ от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" финансовое обеспечение расходов на содержание центрального аппарата Роскомнадзора и территориальных органов осуществляется в пределах бюджетных ассигнований, предусмотренных в федеральном бюджете. Роскомнадзор является юридическим лицом, имеет печать с изображением Государственного герба РФ и со своим наименованием, иные печати, штампы и бланки установленного образца, а также лицевые счета, открываемые в соответствии с бюджетным законодательством РФ в Федеральном казначействе и его территориальных органах в валюте РФ, а также счета в кредитных организациях, открываемые для учета операций в соответствии с валютным законодательством РФ.

9. Пунктом 9 комментируемой статьи законодатель устанавливает, что при Роскомнадзоре создается на общественных

началах консультативный совет. Порядок формирования и порядок деятельности этого органа определяются Роскомнадзором. В настоящее время Положение о консультационном совете утверждено приказом Роскомнадзора от 14.09.2009 N 465. Консультативный совет не является экспертным учреждением. Его члены могут выступать в качестве экспертов в порядке, предусмотренном действующим законодательством РФ. Консультативный совет создается и прекращает свою деятельность на основании приказа Роскомнадзора.

Основными задачами Консультативного совета являются подготовка предложений и рекомендаций по вопросам:

- гармонизации законодательства РФ в области защиты ПД с учетом общественного мнения и опыта правоприменительной практики;
- обеспечения соблюдения законодательства РФ в области защиты ПД;
- методического обеспечения правоприменительной деятельности в области защиты ПД;
- содействия распространению положительного опыта по организации защиты прав субъектов ПД;
- содействия формированию позитивного общественного мнения, способствующего созданию и развитию эффективной системы защиты прав субъектов ПД;
- создания условий для повышения правового уровня и активной гражданской позиции общества.

К функциям Консультативного совета относятся следующие:

- изучение и оценка информации о состоянии дел в области ПД на основе научных и социологических исследований и разработок, профессиональных знаний и международного опыта;
- изучение, обобщение и распространение опыта организации деятельности по защите прав субъектов ПД;
- выработка предложений по внесению изменений, дополнений в действующее законодательство РФ в области ПД;
- обсуждение проектов законодательных и иных нормативных правовых актов в области ПД;
- рассмотрение и разработка научно обоснованных рекомендаций по совершенствованию комментируемого Закона;
- содействие реализации мер, направленных на защиту прав субъектов ПД;
- содействие реализации мер, направленных на расширение международного сотрудничества по вопросам защиты прав субъектов ПД.

Консультативный совет формируется из представителей федеральных органов государственной власти, объединений операторов, осуществляющих обработку ПД в установленной сфере деятельности, общественных организаций, специалистов в области ПД, информационной безопасности. Консультативный совет создается в составе председателя, заместителя председателя, ответственного секретаря и иных членов Консультативного совета. Консультативный совет возглавляет его председатель, который является заместителем руководителя Роскомнадзора.

При Консультативном совете, в целях эффективного осуществления возложенных на него функций, могут создаваться рабочие группы по основным направлениям его деятельности. Количество рабочих групп, их руководители и персональный состав определяются и утверждаются председателем Консультативного совета. Рабочие группы:

- организуют по поручению Консультативного совета изучение вопросов в области ПД и разработку проектов документов, связанных с деятельностью Консультативного совета;
- обеспечивают реализацию мероприятий, связанных с подготовкой заседаний Консультативного совета;
- вносят предложения в план работы Консультативного совета;
- отчитываются перед Консультативным советом о проделанной работе.

К работе рабочих групп могут привлекаться представители федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, общественных и иных организаций.

Согласно Положению о консультационном совете, утвержденному приказом Роскомнадзора от 14 сентября 2009 года N 465, Консультативный совет проводит свои заседания по мере необходимости, но не реже 1 раза в три месяца. Решения, принимаемые Консультативным советом, носят рекомендательный характер. На заседания Консультативного совета могут приглашаться представители федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, общественных и иных организаций, а также организаций, осуществляющих деятельность по обработке ПД.

Статья 24. Ответственность за нарушение требований настоящего Федерального закона

Законодатель определяет виды ответственности за нарушение комментируемого Закона.

Уголовная ответственность.

Так, за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации виновные лица наказываются в соответствии со ст. 137 УК РФ штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет. Если это преступление совершено лицом с использованием своего служебного положения, то наказание будет еще строже.

Должностные лица могут быть привлечены к уголовной ответственности по ст. 140 УК РФ, если неправомерно откажут гражданину в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставят гражданину неполную или заведомо ложную информацию, если эти деяния

причинили вред правам и законным интересам граждан.

За неправомерный доступ к компьютерной информации также предусмотрена уголовная ответственность. Виновные лица будут наказаны по ст. 272 УК РФ, если ими будет незаконно получена информация, содержащаяся на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, при условии, что это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

За нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений виновные лица наказываются штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года. Также подвергаются уголовному преследованию лица, осуществляющие незаконные производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации.

Административная ответственность.

За неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации виновное лицо будет привлечено к ответственности по ст. 5.39 КоАП РФ и наказано штрафом в размере от одной тысячи до трех тысяч рублей.

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей в соответствии со ст. 13.11 КоАП РФ.

Кроме того административная ответственность предусмотрена за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей. В этом случае виновный будет наказан в соответствии со ст. 13.14 КоАП РФ.

Операторам ПД также следует учитывать, что использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от одной тысячи до двух тысяч рублей; на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой. Административная ответственность в этом случае наступает в соответствии со ст. 13.12 КоАП РФ.

Статьей 13.13 КоАП РФ предусматривается ответственность за незаконную деятельность в области защиты информации. Так, занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц - от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой.

Дисциплинарная ответственность.

Статья 192 ТК РФ предусматривает следующие виды дисциплинарных взысканий: замечание; выговор; увольнение по соответствующим основаниям.

Как разъяснялось ранее, с работниками организации, имеющими доступ к ПД сотрудников, партнеров или клиентов организации следует заключать соглашения об обеспечении конфиденциальности данных. В случае нарушения взятых на себя обязательств работник, имеющий доступ к чужим ПД, может быть уволен по основаниям пункта "в" ст. 81 ТК РФ - за разглашение охраняемой законом тайны, в т.ч. разглашение ПД другого работника.

Глава 6. Заключительные положения

Статья 25. Заключительные положения

1. Пунктом 1 комментируемой статьи законодатель определяет срок вступления в силу Закона. Комментируемый Закон вступил в силу по истечении ста восьмидесяти дней после дня его официального опубликования, то есть с 26 января 2007 года.

Первоначальный текст документа опубликован в следующих изданиях:

- "Российская газета", N 165, 29.07.2006;
- "Собрание законодательства РФ", 31.07.2006, N 31 (1 ч.), ст. 3451;
- "Парламентская газета", N 126-127, 03.08.2006.

2. Пунктом 2 комментируемой статьи законодатель устанавливает, что обработка тех ПД, которые были включены в информационные системы ПД до дня вступления в силу данного Закона, также должна осуществляться в соответствии с положениями комментируемого Закона.

3. Пунктом 3 комментируемой статьи законодатель устанавливает дополнительные требования к информационным системам ПД. В первоначальной редакции Закона устанавливалось, что информационные системы ПД, созданные до дня

вступления в силу комментируемого Закона, должны быть приведены в соответствие с требованиями Закона не позднее 1 января 2010 года. Как упоминалось ранее, большинство операторов ПД не смогли выполнить эти требования в срок. Федеральным законом от 27.12.2009 N 363-ФЗ "О внесении изменений в статьи 19 и 25 Федерального закона "О персональных данных" указанный срок был продлен до 1 января 2011 года. Следует учитывать, что в течение 2010 год в статьи анализируемого Закона был внесен ряд изменений и дополнений. Таким образом, операторы ПД должны привести информационные системы ПД, созданные до 1 января 2011 года, в соответствие со всеми требованиями комментируемого Закона не позднее 1 июля 2011 года.

4. Пункт 4 комментируемой статьи регламентирует действия оператора ПД, которые начали осуществлять обработку ПД до вступления в силу рассматриваемого Закона. На таких операторов Закон возлагал обязанность направить не позднее 1 января 2008 г. уведомление об обработке ПД в уполномоченный орган в соответствии со ст. 22 комментируемого Закона.

Список использованных ресурсов удаленного доступа (internet)

1. В Московской области реализуется программа "Электронное Подмосковье на период 2006-2009 годов" (Электронный ресурс) - Правительство Московской области - Режим доступа: http://www.mosreg.ru/news/29755.html

2. Государственный регистр населения Санкт-Петербурга (Электронный ресурс) - Официальный портал администрации Санкт-Петербурга - Режим доступа: http://www.gov.spb.ru/gov/admin/otrasl/c_information/gos_registr

3. Законодательство в области персональных данных (Электронный ресурс) - Официальный интернет-ресурс Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций - Режим доступа: http://63.rsoc.ru/law/p966/

4. На саммите в Сочи лидеры России и ЕС подписали соглашения об облегчении визового режима и реадмиссии (Электронный ресурс) - Newsru.com - Режим доступа: http://www.newsru.com/russia/25may2006/summit.html