Подготовлен для системы КонсультантПлюс

ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ПОЛУЧАЕМЫЕ ЧЕРЕЗ ИНТЕРНЕТ: ПРАКТИЧЕСКИЕ ВОПРОСЫ

Материал подготовлен с использованием правовых актов
по состоянию на 1 июня 2012 года

Р.Д. ЗОРКОЛЬЦЕВ

Зоркольцев Р.Д., адвокат, член адвокатской платы г. Москвы.

В банковском, страховом бизнесе и других сферах деятельности, при создании новой компании или формировании бизнес-проекта, когда предполагается предоставление услуг посредством Интернет, нередко возникают вопросы в работе с персональными данными потенциальных клиентов. Какие сведения будут считаться персональными данными и что является достаточным подтверждением согласия клиента на обработку его данных при заполнении им специальной анкеты в Интернете для последующего оформления страхового полиса, банковской или иной услуги (достаточно ли проставления галочки при заполнении формы на интернет-сайте)? Можно ли хранить персональные данные за пределами России, и допускается ли передача обработки этих данных на аутсорсинг? Эти и другие актуальные для практики проблемы освещаются в статье.

В некоторых сферах деятельности (страхование, банковская деятельность) компании развивают веб-сервисы, при пользовании которыми от потенциальных клиентов, прежде чем оформить с ними правоотношения, требуется заполнение специальной формы на интернет-сайте (анкеты, заявления и т.п.). В этой форме клиент должен отразить информацию, необходимую для заключения договора (оформления страхового полиса, получения банковской или иной услуги).

Будет ли считаться персональными данными та информация, которую предоставляет клиент, заполняя в анкете на интернет-сайте специальные поля, указывая кроме фамилии, имени, отчества, места жительства, паспортных данных также сведения из других документов, относящихся к гражданину опосредованно?

В п. 1 ст. 3 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных, или Закон) определено, что персональные данные - это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Очевидно, что фамилия, имя, отчество, место жительства, реквизиты паспорта являются персональными данными, поскольку они прямо относятся к определенному гражданину. Об этом свидетельствует судебная практика <1>. Полагаю, что также будут являться персональными данными, например, сведения о паспорте транспортного средства, принадлежащего гражданину, сведения из правоустанавливающих документов на принадлежащее ему недвижимое имущество (свидетельство о государственной регистрации права в ЕГРП), вносимые в заявление на страхование или анкету клиента для пользования другого рода услугой, поскольку эти сведения имеют отношение к определенному физическому лицу. Сведения из других документов также могут являться персональными данными, если они, как указывает Закон, прямо или косвенно имеют отношение к определенному или определяемому физическому лицу.

<1> См., например: Постановление Президиума Верховного Суда РФ от 21 июля 2010 г. N 11-ПВ10, Постановление Президиума ВАС РФ от 6 сентября 2011 г. N 1089/11, Определение Кассационной коллегии Верховного Суда РФ от 17 июля 2008 г. N КАС08-347.

Для тех, кто ведет свой бизнес в Интернете, актуален вопрос о месте и стране обработки и хранения персональных данных. Можно ли хранить персональные данные за пределами России?

Допускается ли при этом возможность поручить обработку этих данных третьему лицу (передать на аутсорсинг), в том числе находящемуся за границей?

В п. 2 ст. 3 Закона о персональных данных определено понятие оператора. Им может быть государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

В силу ч. 3 ст. 6 Закона оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (поручение оператора).

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 Закона (в ней приведены меры по обеспечению безопасности персональных данных при их обработке).

Согласно ч. ч. 4 и 5 ст. 6 Закона лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Под обработкой персональных данных понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (п. 3 ст. 3 Закона о персональных данных).

Из этого определения следует, что понятие обработки персональных данных включает в себя хранение и передачу таких данных, а понятие передачи - также их трансграничную передачу, под которой понимается их передача на территорию иностранного государства органу власти иностранного государства, иностранному физическому или юридическому лицу (п. 11 ст. 3 Закона).

В соответствии со ст. 12 Закона допускается трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных <2>, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

<2> Конвенция о защите физических лиц при автоматизированной обработке персональных данных ETS N 108 (Страсбург, 28 января 1981 г.).

Оператор, работающий с персональными данными, до начала осуществления трансграничной передачи персональных данных обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

Понятия "адекватной защиты" в российском законодательстве не содержится,

следовательно, это понятие оценочное. По всей видимости, с юридической точки зрения, об адекватности защиты прав субъектов персональных данных на территории иностранного государства может свидетельствовать, во-первых, сам факт присоединения этого государства к Конвенции <3>, во-вторых (это касается стран, не присоединившихся к Конвенции), наличие в государстве юридических и практических мер (национальных законов, подзаконных актов и административных распоряжений), обеспечивающих полную, своевременную и реальную защиту прав субъектов персональных данных. Для стран - членов ЕС, например, в числе принципов передачи персональных данных в третьи страны, изложенных в ст. 25 Директивы Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, предусмотрено, что достаточность уровня защиты, предоставляемого третьей страной, оценивается в свете всех обстоятельств, связанных с операцией по передаче или с последовательностью операций по передаче данных; особое внимание уделяется характеру данных, цели и продолжительности предлагаемой операции или операций по обработке, стране происхождения и стране конечного назначения, законодательным правилам, как общим, так и отраслевым, действующим в соответствующей третьей стране, а также профессиональным правилам и мерам безопасности, соблюдаемым в этой стране.

<3> Об этом см.: письмо Министерства связи и массовых коммуникаций РФ от 13 мая 2009 г. N ДС-П11-2502 "Об осуществлении трансграничной передачи персональных данных" (ответ на запрос Ассоциации российских банков от 23 марта 2009 г. N А-01/5-140).

В ряде случаев, перечисленных в ч. 4 ст. 12 Закона, трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, все же возможна. Она может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Как видно, нормы Закона о персональных данных не запрещают передачу персональных данных за пределы России и не запрещают передачу обработки персональных данных на аутсорсинг за границу. При должном соблюдении всех прав субъектов персональных данных это поможет также снизить риски бизнесменов, поскольку в ряде случаев в практике реализации интернет-проектов у них отсутствует доверие к качеству хостинга, предоставляемого российскими провайдерами (хостинг-провайдерами, хостерами), которые допускают так называемые "обвалы сайтов".

Исходя из ч. 4 ст. 9 Закона согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности, перечень действий с персональными данными, на совершение которых дается согласие и общее описание используемых оператором способов обработки персональных данных. В связи с этим, если речь идет о поручении обработки персональных данных на аутсорсинг за границу, рекомендуется получить согласие гражданина на обработку его персональных данных в данном конкретном иностранном государстве.

Еще более важной для практики ведения бизнеса в Интернете является проблема, связанная с формой выражения согласия субъекта персональных данных на их обработку. Что является достаточным подтверждением согласия субъекта на обработку его персональных данных?

Является ли таким согласием проставление им галочки при заполнении специальной анкеты на интернет-сайте для последующего оформления страхового полиса, банковской или иной услуги?

Исходя из ст. 9 Закона о персональных данных субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Таким образом, в целом допускается проставление галочки в документе, который подписывается субъектом персональных данных, либо формулирование в документе фразы о том, что субъект персональных данных подписанием этого документа дает свое согласие оператору или другому лицу, определяемому оператором, на обработку персональных данных. Однако если речь идет о согласии в форме электронного документа, то оно должно сопровождаться электронной подписью, т.е. обязательным реквизитом.

Между тем в одном из судебных актов <4> указано, что обработка персональных данных может осуществляться с согласия субъектов персональных данных, при этом Законом о персональных данных определено два способа получения указанного согласия: путем принятия субъектом персональных данных решения на обработку своих данных своей волей и в своем интересе, а также путем получения согласия субъекта персональных данных в письменной форме. В этом судебном споре, в котором рассматривалась ситуация получения ипотечного кредита, выводы суда были следующими: "Физические лица - потенциальные клиенты на получение ипотечного кредита, заполняя анкету-запрос в письменном электронном виде на веб-ресурсах www.krediтuem.com и www.creditsbrf.ru, последовательно отвечали на вопросы анкеты, содержащей сведения о персональных данных; цель предоставления данных - получение ипотечного кредита и обработка персональных данных, поскольку в анкете было указано, что кредит предоставляется банком... Затем данные физические лица отправляли анкету в электронном виде ООО "Кредитмарт", которое непосредственно имело доступ в административную часть порталов указанных веб-ресурсов под профилем "Руководитель офиса"... Отправив свои данные по указанному алгоритму заполнения анкеты, физические лица фактически выразили свое согласие на передачу своих персональных данных, то есть при обработке персональных данных указанных лиц ООО "Авторим" получало их письменное согласие в смысле, определенном пунктом 4 статьи 9 Закона о персональных данных".

<4> Постановление ФАС Северо-Западного округа от 13 декабря 2010 г. N Ф07-13220/2010 по делу N А56-73636/2009.

Исходя из такого толкования проставление галочки в полях специально отведенной электронной формы на интернет-сайте допускается. Такая практика может применяться, например, при заключении договора страхования. В этом случае получается, что заполнение в электронной форме на интернет-сайте заявления на страхование, анкеты и т.п., где, помимо прочего, предусматривается необходимость заказчика услуги (страхователя) проставить в отведенном для этого месте галочку в подтверждение своего согласия с обработкой его персональных данных, означает как заключение самого договора страхования, так и предоставление согласия на обработку персональных данных. Если предположить, что сразу после этого клиент внесет необходимую сумму (оплатит полис или другую услугу) посредством безналичных расчетов, то договор будет считаться заключенным, согласие на обработку персональных данных - полученным.

В законодательстве регламентированы случаи, когда факт оплаты услуг будет свидетельствовать об акцепте, следовательно, о заключении договора. Согласно ст. 434 ГК РФ письменная форма договора считается соблюденной, если письменное предложение заключить договор принято в порядке, предусмотренном п. 3 ст. 438 ГК РФ: совершение лицом, получившим

оферту, в срок, установленный для ее акцепта, действий по выполнению указанных в ней условий договора (отгрузка товаров, предоставление услуг, выполнение работ, уплата соответствующей суммы и т.п.) считается акцептом, если иное не предусмотрено законом, иными правовыми актами или не указано в оферте.

Однако есть и иное толкование Закона о персональных данных судебными инстанциями.

В другом судебном деле <5> вывод суда был таким: "Само по себе заключение от имени фирмы публичных договоров с гражданами не свидетельствует о согласии последних на распространение их персональных данных третьим лицам". Хотя нужно учитывать специфику этого спора: публичная оферта была выражена в письменной форме в печатном издании, а не в электронной форме на интернет-сайте. В этом деле речь тоже шла о кредитовании. Обществом в средствах массовой информации ("Российская газета") были опубликованы условия договора (публичной оферты), согласно которому пользователь согласен на представление сведений о нем третьим лицам, в том числе его персональных данных, юридическим лицам, осуществляющим формирование, обработку, хранение и выдачу информации об исполнении должником принятых на себя договорных обязательств, включая бюро кредитных историй. Ссылка общества на то, что, подписав договор, граждане фактически согласились с возможностью распространения их персональных данных третьим лицам, была признана необоснованной. По мнению судов апелляционной и кассационной инстанций, рассматривавших спор, действующим законодательством установлены специальные требования к письменному согласию субъекта персональных данных, и само по себе заключение публичных договоров между обществом и гражданами не свидетельствует о согласии последних на распространение их персональных данных третьим лицам.

<5> Постановление ФАС Уральского округа от 18 марта 2010 г. N Ф09-1736/10-С1 по делу N А34-5785/2009.

Исходя из такого толкования получается, что заполнение документа (заявления, анкеты и т.п.) в электронной форме на интернет-сайте, где предусматривается необходимость клиента поставить галочку, а значит, согласиться с обработкой его персональных данных, означает лишь заключение самого договора (при условии совершения иных конклюдентных действий), но не освобождает оператора от обязанности получить согласие субъекта персональных данных в установленной форме - либо в письменной, либо в электронной форме, последняя должна сопровождаться электронной подписью клиента.

Думаю, что вопрос может быть разрешен следующим образом.

Согласно ч. 4 ст. 9 Закона в случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Следовательно, если в специальном законодательстве нет прямо выраженного запрета на то, чтобы согласие на обработку таких данных давалось не в письменной форме (т.е. не на бумажном носителе), то допускается любая другая форма выражения этого согласия, в том числе посредством проставления галочки при заполнении заявления или анкеты в электронной форме на интернет-сайте. Например, в Законе РФ от 27 ноября 1992 года N 4015-1 "Об организации страхового дела в Российской Федерации" нет запрета на то, чтобы согласие на обработку таких данных давалось не в письменной форме. Значит, для этой сферы допускается любая другая форма выражения такого согласия. Вероятно, тот же вывод можно сделать и в отношении других сфер деятельности с учетом их правового регулирования. Главное, чтобы решение на обработку своих данных было выражено субъектом персональных данных, как требует закон, свободно, своей волей и в своем интересе (и именно этим субъектом, а не другим лицом), и такое согласие должно быть конкретным, информированным и сознательным. Однако этот вывод, конечно, относится к случаям, когда вслед за предоставлением согласия в такой форме клиент совершил другие действия, позволяющие считать, что он вступил в правоотношения с контрагентом (например, заключил договор). Во всяком случае, при рассмотрении возможного судебного спора будут учитываться все фактические обстоятельства взаимоотношений сторон.

Не менее важным для практиков является то, каковы технические требования к обеспечению безопасности персональных данных при их обработке в автоматизированных

системах (специальные требования к серверам и каналам передачи данных), в каких нормативных актах они закреплены, нужно ли иметь специальное сертифицированное оборудование и кто осуществляет его сертификацию.

В силу ст. 19 Закона оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Согласно подп. 7 п. 3.1 Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных ФСБ РФ 21 февраля 2008 г. N 149/54-144, для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации) криптосредства.

В п. 5 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17 ноября 2007 г. N 781, предусмотрено, что средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

В соответствии с п. 18 указанного Положения результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю (ФСТЭК) и ФСБ в пределах их полномочий.

К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с ФСТЭК и ФСБ в пределах их полномочий. Изменение условий применения средств защиты информации, предусмотренных указанными правилами, согласовывается с этими федеральными органами исполнительной власти в пределах их полномочий. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров, перечень которых определяется ФСТЭК и ФСБ в пределах их полномочий. Особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах устанавливаются ФСБ (п. п. 19 - 21 Положения).

Согласно п. 2.1 Типовых требований 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, утвержденных ФСБ РФ 21 февраля 2008 г. N 149/6/6-622, безопасность обработки персональных данных с использованием криптосредств организуют и обеспечивают операторы, а также лица, которым на основании договора оператор поручает обработку персональных данных и (или) лица, которым на основании договора оператор поручает оказание услуг по организации и обеспечению безопасности обработки в информационной системе персональных данных с использованием криптосредств.

Обеспечение безопасности персональных данных с использованием криптосредств должно осуществляться также в соответствии с Приказом ФСБ России от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"; Постановлением Правительства РФ от 29 декабря 2007 г. N 957 "Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами".

Согласно п. 46 Положения ПКЗ-2005 средства криптографической защиты информации (СКЗИ) эксплуатируются в соответствии с правилами пользования ими. Все изменения условий использования СКЗИ, указанных в правилах пользования ими, должны согласовываться с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.

Имеются другие нормативные документы, в которых содержатся требования к защите персональных данных при их автоматизированной обработке в информационных системах и иные требования, связанные с обработкой и хранением персональных данных, режимом работы с персональными данными в организации оператора, например: Положение о методах и способах защиты информации в информационных системах персональных данных, утвержденное Приказом ФСТЭК России от 5 февраля 2010 г. N 58; Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК 14 февраля 2008 г.; Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК 15 февраля 2008 г.

Работа с персональными данными вызывает необходимость сохранения их конфиденциальности. Так, согласно ст. 7 Закона о персональных данных операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных. Существует ли необходимость в особом способе организации доступа к персональным данным уполномоченных сотрудников и каковы требования к таким сотрудникам?

В силу ст. 18.1 Закона оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения этих обязанностей. К таким мерам могут, в частности, относиться:

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

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со ст. 19 Закона;

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

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом;

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

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

Оператор обязан представить документы и локальные акты по вопросам, связанным с мерами, необходимыми и достаточными для обеспечения выполнения указанных выше обязанностей, и (или) иным образом подтвердить принятие этих мер по запросу уполномоченного органа по защите прав субъектов персональных данных. Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <6>.

<6> Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденное Постановлением Правительства РФ от 16 марта 2009 г. N 228.

Исходя из ст. 22.1 Закона оператор, являющийся юридическим лицом, назначает ответственного за организацию обработки персональных данных. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему. Ответственный за организацию обработки персональных данных, в частности, обязан:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Представляют интерес имеющиеся в законодательстве санкции за нарушение установленных требований в работе с персональными данными.

Прежде всего, существуют гражданско-правовые способы защиты прав.

Согласно ст. 17 Закона, если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Закона 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. 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.

В силу ст. 24 Закона о персональных данных лица, виновные в нарушении требований данного Закона, несут предусмотренную законодательством Российской Федерации ответственность. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Законом, а также требований к защите персональных данных, установленных в соответствии с ним, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Существует административная ответственность за нарушение установленных требований. Напрямую к нарушениям в сфере обработки персональных данных относится ст. 13.11 КоАП РФ, в силу которой 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 300 до 500 руб.; на должностных лиц - от 500 до 1 тыс. руб.; на юридических лиц - от 5 тыс. до 10 тыс. руб.

Прочие виды административных правонарушений предусмотрены следующими статьями КоАП РФ: отказ в предоставлении информации (ст. 5.39); нарушение правил защиты информации (ст. 13.12); незаконная деятельность в области защиты информации (ст. 13.13); разглашение информации с ограниченным доступом (ст. 13.14).

Предусмотрены и уголовно-правовые санкции за совершение преступлений в этой сфере. Так, статьей 137 УК РФ к уголовно наказуемому деянию относится нарушение неприкосновенности частной жизни, а именно 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. В ст. 140 УК РФ установлена ответственность за отказ в предоставлении гражданину информации, а в ст. 272 УК РФ - ответственность за неправомерный доступ к компьютерной информации.

Как видно, при ведении бизнеса посредством Интернета возникает ряд трудностей, преодоление которых во многом связано с надлежащим правоприменением и толкованием права уполномоченными органами и частными лицами. В силу наличия принципа соблюдения баланса частных и публичных интересов важно, чтобы при их преодолении не возникал "крен" в какую-то одну сторону, поскольку это может отразиться на распространении и развитии тех или иных услуг в стране, а ими, как известно, пользуются не только частные лица, но и государственные служащие.