VEGAS LEX

Безопасность персональных данных при использовании «облачных» сервисов

WWW.VEGASLEX.RU

ФЕВРАЛЬ 2014

Проблема защиты конфиденциальной информации, в частности, персональных данных (далее – ПДн)[1] является одним из существенных факторов при принятии решения об использовании бизнесом «облачных» технологий[2]. Значимость данного вопроса продиктована, с одной стороны, критической важностью указанной информации для некоторых видов бизнеса, с другой – возросшим в последнее время вниманием регуляторов к этой сфере.

Главный вопрос в связи с этим – не является ли использование «облачных» сервисов для обработки ПДн нарушением российского законодательства? Прежде чем давать оптимистичный ответ на этот вопрос, необходимо учесть ряд важных моментов.

БАЗОВЫЕ ПОЛОЖЕНИЯ

В первую очередь необходимо понимать, что обеспечение безопасности ПДн при их обработке – это обязанность оператора ПДн[3] (далее – Оператор). Для исполнения своей обязанности Оператор выстраивает систему защиты ПДн[4], служащую для нейтрализации актуальных угроз[5], определяемых в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных; Закон).

При этом под «обработкой» Закон о персональных данных понимает любое действие с ПДн, включая сбор, накопление, хранение, передачу, удаление и т. д. Таким образом, операции, совершаемые «облачными» провайдерами с ПДн, в любом случае подпадают под понятие «обработки» и, следовательно, подлежат соответствующему правовому регулированию[6].

Для того чтобы рассматриваемые отношения оставались в рамках существующего правового поля, необходимо учитывать следующие аспекты:

- возможность передачи ПДн для обработки третьим лицам;
- требования к содержанию договора с провайдером «облачного» сервиса;
- условия трансграничной передачи ПДн;
- нормативное регулирование в области сертификации и лицензирования;
- особенности регулирования в части обезличенных данных.

ПЕРЕДАЧА ДАННЫХ ДЛЯ ОБРАБОТКИ ТРЕТЬИМ ЛИЦАМ

В соответствии с частью 3 статьи 6 Закона о персональных данных Оператор вправе поручить обработку ПДн другому лицу (далее – Обработчик) только с согласия субъекта[7]. Такое согласие должен получить именно Оператор ПДн, а не Обработчик.

При этом статус Обработчика, которым и является провайдер «облачного» сервиса, по смыслу Закона, не тождественен статусу самого Оператора, так как в отличие от последнего он осуществляет обработку ПДн с одной единственной целью – исполнить условия договора с Оператором (и получить от него встречное исполнение), и не использует ПДн для взаимодействия с их субъектами или извлечения выгоды путем их коммерциализации. По данному критерию следует отличать от Обработчиков, к примеру, коллекторские агентства, которые, получая ПДн от кредитора, непосредственно используют их в своей деятельности.

Вопросы на практике вызывают требования к форме согласия субъекта на обработку его ПДн третьими лицами. Общие требования к согласию на обработку ПДн определены в статье 9 Закона о персональных данных, согласно которой такое согласие должно быть конкретным, информированным и сознательным. Формальное тре-

[1] При этом не все ПДн являются конфиденциальной информацией. В частности, в отношении общедоступных ПДн у Оператора отсутствует обязанность неразглашения третьим лицам. Тем не менее, с точки зрения обеспечения безопасности именно конфиденциальные ПДн имеют ключевое значение и потому являются основным предметом рассмотрения в настоящем анализе.

[2] Настоящий анализ описывает проблематику, актуальную для частного сектора. Выводы, приведенные здесь, могут не учитывать специфику использования государственных информационных систем, а также требований отраслевого законодательства (банковского и пр).

[3] Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (пункт 2 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

[4] Система защиты персональных данных – организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в информационных системах ПДн (далее – ИСПДн) (абзац второй пункта 2 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119).

[5] Актуальные угрозы безопасности персональных данных – совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия (пункт 6 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119).

[6] Данный момент имеет принципиальное значение, так как существует мнение, что в случае, если у провайдера «облачного» сервиса нет доступа к самим данным, то его действия нельзя считать обработкой ПДн. Однако с данным утверждением нельзя согласиться, если исходить из буквального толкования упомянутой нормы Закона о персональных данных. При этом, как показывает практика, именно буквальное толкование положений законодательства превалирует в решениях российских судов.

[7] В подтверждение см., например, Постановление Кировского областного суда от 24.04.2012 № 7-А-98/2012. Аналогичные выводы можно увидеть в решениях по делам: А32-12882/2010, А04-1037/2012, А27-5075/2013.

бование к такому согласию состоит в том, что оно может быть дано субъектом или его представителем в любой позволяющей подтвердить факт его получения форме. При этом Закон не требует, чтобы такое согласие было письменным. Таким образом, указанное согласие может быть получено Оператором в любой форме, в том числе электронной, при условии, что он впоследствии сможет доказать факт его получения.

Если Оператор поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия этого лица все равно несет Оператор. Обработчик, в свою очередь, несет ответственность перед Оператором.

Подводя итог: прежде чем использовать «облачные» сервисы для обработки ПДн, необходимо получить соответствующее согласие от всех субъектов такой информации.

ДОГОВОР С ПРОВАЙДЕРОМ

Закон о персональных данных также содержит указание на необходимость заключения соответствующего договора с Обработчиком ПДн.

Такой договор в обязательном порядке должен содержать:

1) обязанность провайдера соблюдать принципы и правила обработки ПДн, предусмотренные Законом о персональных данных;
2) перечень действий (операций) с ПДн, которые будут совершаться провайдером, и цели обработки;
3) обязанность провайдера соблюдать конфиденциальность ПДн[8] и обеспечить их безопасность при обработке;
4) требования к защите обрабатываемых ПДн в соответствии со статьей 19 Закона о персональных данных.

При этом обязательность выполнения требований, указанных в пунктах 1 и 4, в случае если провайдер зарегистрирован на территории иностранного государства, вызывает сомнения среди экспертов, ссылающихся на то, что на территории соответствующего государства действуют свои нормы и требования к безопасности ПДн. Однако, как указывалось выше, по смыслу Закона о персональных данных, указанные требования являются обязательными к исполнению не для провайдера сервиса, а для Оператора, который вправе передать соответствующие полномочия на обработку только при условии включения соответствующих положений в текст договора/поручения.

Во избежание различного толкования объема данных, за который провайдер несет ответственность, необходимо включать в договор конкретный перечень ПДн, которые передаются провайдеру или к которым у провайдера есть доступ.

Не лишним также будет включить в SLA-соглашение[9] с провайдером условия, касающиеся безопасности информации, в частности: обязанность использования определенных алгоритмов шифрования данных, порядок исполнения обязанности провайдера по передаче данных оператору в случае расторжения договора, а также по их уничтожению, требования к мерам по изолированной обработке данных разных клиентов/пользователей и др.

ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ДАННЫХ

Исходя из смысла статьи 12 Закона о персональных данных, оператор вправе осуществлять передачу ПДн на территорию любого иностранного государства, обеспечивающего адекватную защиту прав субъектов ПДн, без необходимости получать соответствующее согласие. В соответствии с Законом, к государствам, обеспечивающим такую защиту, относятся:

- государства, являющиеся участниками Конвенции Совета Европы «О защите физических лиц в отношении автоматизированной обработки данных личного характера» (ETS № 108) (Заключена в Страсбурге 28.01.1981)[10] (далее – Конвенция СЕ);
- государства, не являющиеся сторонами Конвенции СЕ, но тем не менее обеспечивающие адекватную защиту ПДн, перечень которых определяет Уполномоченный орган по защите прав субъектов ПДн[11].

Передача ПДн на территорию государства, не обеспечивающего адекватную защиту прав субъектов ПДн, возможна в следующих случаях[12]:

1) наличие согласия в письменной форме субъекта

[8] Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (пункт 7 статьи 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

[9] Service Level Agreement (SLA) – «соглашение об уровне обслуживания», ключевой документ, определяющий и (или) детализирующий обязательства и ответственность провайдера.

[10] Согласно информации СПС «КонсультантПлюс», к государствам, подписавшим Конвенцию СЕ по состоянию на 23 января 2014 года, являются: Австрия, Азербайджан, Албания, Андорра, Армения, Бельгия, Болгария, Босния и Герцеговина, Великобритания, Венгрия, Германия (ФРГ), Греция, Грузия, Дания, Ирландия, Исландия, Испания, Италия, Кипр, Латвия, Литва, Лихтенштейн, Люксембург, Македония, Мальта, Молдавия, Монако, Нидерланды, Норвегия, Польша, Португалия, Россия, Румыния, Сербия, Словакия, Словения, Турция, Украина, Уругвай, Финляндия, Франция, Хорватия, Черногория, Чехия, Швейцария, Швеция, Эстония.

[11] См. Приказ Роскомнадзора от 15.03.2013 № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

[12] Здесь указаны три из пяти упомянутых в Законе случаев, так как остальные два не имеют отношения к обработке ПДн с использованием «облачных» сервисов. Полный перечень содержится в части 4 статьи 12 Закона о персональных данных.

персональных данных на трансграничную передачу его ПДн;

2) случаи, предусмотренные международными договорами Российской Федерации (например, при оформлении визы);
3) исполнение договора, стороной которого является субъект ПДн (например, при осуществлении трансграничных банковских операций).

Таким образом, при использовании «облачных» сервисов необходимо требовать от соответствующих провайдеров предоставления информации о местонахождении их центров хранения и обработки данных и, в зависимости от предоставленной информации, принимать решение о необходимости запрашивать согласие у субъектов ПДн.

СЕРТИФИКАТЫ И ЛИЦЕНЗИИ

В зависимости от того, на территории какого государства зарегистрирован провайдер «облачного» сервиса, следует различать две принципиально различные ситуации.

Так, в случае если провайдером является иностранное лицо, то оно осуществляет свою деятельность, в том числе связанную с обработкой ПДн, в соответствии с национальным законодательством соответствующего государства и, таким образом, не обязано соблюдать требования российских регуляторов. Отсюда следует, что в данной ситуации для оператора, по крайней мере, с точки зрения соблюдения требований регуляторов, не имеет значения, обладает ли такой провайдер соответствующими сертификатами, лицензиями и т. п.

С российскими провайдерами дело обстоит несколько сложнее.

В части 2 статьи 19 Закона о персональных данных приведен перечень мер, с помощью которых достигается обеспечение безопасности ПДн. Данный перечень содержит в числе прочих мер «применение прошедших в установленном порядке процедуру оценки соответствия» средств защиты информации (далее – СЗИ)[13].

Указанное положение говорит об «оценке соответствия» СЗИ, которая в соответствии с абзацем вторым части 3 статьи 7 Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании» (далее – Закон о техрегулировании) помимо сертификации включает в себя еще целый ряд возможных способов такой оценки (государственный контроль (надзор), испытание, регистрацию и др.) и может носить как обязательный характер (декларирование соответствия или обязательная сертификация), так и добровольный (добровольная сертификация).

Следует также учитывать, что Закон о техническом регулировании устанавливает принцип недопустимости применения обязательного подтверждения соответствия к объектам, в отношении которых не установлены требования технических регламентов[14].

Из всего этого мы можем сделать вывод, что на сегодняшний момент законодательство не устанавливает обязанности операторов использовать сертифицированные СЗИ, а лишь указывает на возможность их использования в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПДн[15]. Оператор самостоятельно определяет, необходимо ли использование сертифицированных СЗИ в каждом конкретном случае или нет. В рассматриваемом случае Оператор вправе пользоваться услугами провайдера независимо от того, сертифицированы ли СЗИ, применяемые последним при оказании услуг, или нет[16].

В соответствии с пунктами 1, 5, 36 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» лицензированию подлежат следующие виды деятельности, осуществление которых связано с предоставлением «облачных» сервисов и обеспечением безопасности ПДн:

1) деятельность по технической защите информации;
2) распространение средств, информационных и телекоммуникационных систем, защищенных шифрованием; выполнение работ и услуг в области шифрования информации; обслуживание средств, информационных и телекоммуникационных систем, защищенных шифрованием;
3) оказание услуг связи (а именно телематических услуг связи).

Указанные регуляторные требования необходимо учитывать при выборе российского провайдера «облачного» сервиса.

ОБЕЗЛИЧЕННЫЕ ДАННЫЕ

В соответствии с Законом о персональных данных персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. То есть для признания за той или иной информацией статуса ПДн необходимо, кроме прочего, чтобы данную информацию можно было бы соотнести с конкретным физическим лицом.

[13] Исходя из формулировки данной статьи, нельзя сделать однозначный вывод об обязательности применения всех перечисленных мер для защиты ПДн, так как в статье указан лишь примерный перечень соответствующих мер.

[14] См. часть 1 статьи 19 Закона о техрегулировании.

[15] См. пункт 4 «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Приказом ФСТЭК России от 18.02.2013 № 21.

[16] При этом нельзя полностью исключить риск предъявления соответствующих претензий со стороны контролирующих органов в силу упомянутой неоднозначности правового регулирования и отсутствия судебной практики по данному вопросу.

В то же время Закон о персональных данных содержит определение «обезличивания ПДн». Согласно данному определению, под обезличиванием понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту. Обезличивание также упоминается в части 7 статьи 5 Закона о персональных данных в качестве мероприятия, которое обязан произвести Оператор по достижении целей обработки ПДн или в случае утраты необходимости в достижении этих целей. Таким образом, исходя из системного толкования положений Закона о персональных данных, а также с учетом зарубежного опыта[17] регулирования данного вопроса, можно сделать вывод о том, что в отношении обезличенных ПДн вышеназванные требования не действуют.

Однако необходимо учитывать, что, в случае если какое-либо третье лицо по вине Оператора получит доступ к указанным данным и сможет соотнести эти данные с конкретными лицами, Оператор все равно будет нести ответственность за разглашение ПДн, так как он не предпринял достаточных мер для обеспечения безопасности соответствующей информации.

В качестве рекомендаций для осуществления обезличивания ПДн частные организации могут руководствоваться положениями, указанными в Требованиях и методах обезличивания ПДн, утвержденных Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996, распространяющими свое действие на Операторов, являющихся государственными или муниципальными органами. В частности, указанный документ содержит следующие методы обезличивания ПДн:

- метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);
- метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);
- метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);
- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

Таким образом, использование того или иного метода обезличивания ПДн может оказаться при определенных условиях наиболее целесообразным выходом для Оператора, прибегающего к помощи «облачных» сервисов.

ЗАКЛЮЧЕНИЕ

В заключение хотелось бы отметить значительное отставание правового регулирования в этой области от развития ИТ-сектора. Соответствующая нормативная база находится еще на этапе формирования[18]. Существующее же законодательство рассчитано на использование традиционных технологий, в нем почти отсутствует дифференцированный подход к регулированию услуг в ИТ-сфере, наконец, ощущается нехватка судебной практики. Все это, с одной стороны, образует неопределенность в части юридической квалификации соответствующих отношений, однако в то же время создает предпосылки для формирования позиции, отражающей цели законодательства в сфере защиты персональных данных.

[17] См., например, пункт 26 преамбулы к Директиве № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (Принята в Люксембурге 24.10.1995).

[18] На дату подготовки настоящего материала на рассмотрении Государственной Думы находится законопроект № 416052-6 «О внесении изменений в Федеральный закон «О персональных данных» и статью 28.3 Кодекса Российской Федерации об административных правонарушениях», в том числе, нацеленный на сокращение отставания правового регулирования от реально складывающихся отношений в ИТ-сфере.

КОНТАКТЫ

АЛЕКСАНДРА
ВАСЮХНОВА

Руководитель Группы
Технологий и Инвестиций

vasukhnova@vegaslex.ru

Подробную информацию о продуктах и услугах VEGAS LEX можете узнать на www.vegaslex.ru.

VEGAS LEX

VEGAS LEX – одна из ведущих российских юридических фирм, предоставляющая широкий спектр правовых услуг. Основанная в 1995 году, Фирма объединяет более 100 юристов, офисы в Москве, Волгограде, Краснодаре и ряд региональных партнеров.

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ:

- Взаимоотношения с государственными органами. Нормотворчество
- Вопросы конкуренции. Антимонопольное регулирование
- Отраслевое право. Топливно-энергетический комплекс
- Техническое регулирование
- Разрешение споров и досудебное урегулирование конфликтов. Медиация
- Проекты с иностранным элементом. Международный арбитраж. Международные сделки. Локализация
- ГЧП и инфраструктурные проекты
- Недвижимость. Земля. Строительство
- Корпоративные вопросы и M&A. Юридическая экспертиза
- Инвестиции. Проектное финансирование
- Инновационные проекты
- Комплаенс. Антикоррупционный комплайенс и противодействие корпоративному мошенничеству
- Международное налогообложение
- Налоговый консалтинг
- Ценные бумаги, листинг, секьюритизация
- Интеллектуальная собственность
- Отраслевое право. Экологическое право

ОТРАСЛИ ЭКОНОМИКИ:

- Авиация
- ЖКХ
- Информационные технологии
- Инфраструктура и ГЧП
- Машиностроение
- Металлургия
- Нанотехнологии
- Недвижимость
- Недропользование
- Пищевая промышленность
- Страхование
- Строительство
- Телекоммуникации
- Транспорт
- ТЭК
- Тяжелая и легкая промышленность
- Фармацевтика
- Финансы
- Химия и нефтехимия

ПРИЗНАНИЯ И НАГРАДЫ:

- European Legal Experts 2013
- Best Lawyers 2012
- International Financial Law Review 2014
  - Реструктуризация и банкротство
  - Слияния и поглощения
  - Проектное финансирование
- Chambers Europe 2013
  - Государственно-частное партнерство
  - Антимонопольные вопросы
  - Разрешение споров
- The Legal 500 Europe, Middle East&Africa 2013
  - Государственно-частное партнерство
  - Разрешение споров
  - Недвижимость
  - Корпоративная практика, M&A
  - Налоги
  - Энергетика и природные ресурсы
- Право.Ru-300 2013
  - Антимонопольное право
  - Коммерческая недвижимость/ строительство
  - Природные ресурсы/ энергетика
  - Корпоративное право/M&A
  - Налоговое право
  - Арбитраж
  - Интеллектуальная собственность
  - Международный арбитраж
- PLC which lawyer? 2012
  - Антимонопольное право
  - Страхование

НАШИ КЛИЕНТЫ:

Внешэкономбанк, РусГидро, РОСНАНО, СИТРОНИКС, Газпром нефть, Газпром добыча Астрахань, Мосэнергосбыт, МРСК Центра, МРСК Волги, Белон, ФосАгро АГ, РОСНО, Ильюшин Финанс Ко, Русские фонды, РЕСО-Гарантия, Сан ИнБев, МТС, R-Quadrat, HOCHTIEF, MAN, British Airways, Rockwool, MTD Products

СОТРУДНИЧЕСТВО:

Министерство экономического развития РФ, Министерство транспорта РФ, Министерство регионального развития РФ, Федеральная антимонопольная служба РФ, Федеральная служба по тарифам РФ, Федеральная служба по финансовым рынкам РФ, комитеты Государственной Думы и Совета Федерации, ГК Внешэкономбанк, федеральные агентства (Росморречфлот, Росжелдор, Росавтодор, Госстрой), комитеты по собственности и защите конкуренции, ГЧП и инвестициям РСПП, Комиссия по защите прав инвесторов при НФА, Агентство Стратегических инициатив и т.д.

МОСКВА
Тел.: +7 (495) 933 08 00
Факс: +7 (495) 933 08 02
vegaslex@vegaslex.ru

ВОЛГОГРАД
Тел.: +7 (8442) 266 312/313/314/315
Факс: +7 (8442) 26 63 16
volgograd@vegaslex.ru

КРАСНОДАР
Тел.: +7 (861) 274 74 08
Факс: +7 (861) 274 74 09
krasnodar@vegaslex.ru