На вопросы редакции отвечает
управляющий партнер
ООО «Комплай» (*Comply*)
Артем Юрьевич ДМИТРИЕВ

РЫНОК В ОЖИДАНИИ МЯГКОГО ПРАВА ДЛЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Эксперт в области регулирования персональных данных и технологий, имеет более 18 лет опыта оказания юридических услуг для компаний *Fortune*-500. Отмечен российскими и международными юридическими рейтингами, среди них *Best Lawyers*, Право 300, «Коммерсантъ», «Российская газета»; лауреат премий *Russian Privacy Awards* от *Regional Privacy Professionals Association* (*RPPA*); в 2023 году — обладатель премии «Цифровой юрист года» от *Moscow Digital School* (*MDS*). Эксперт рабочих групп Роскомнадзора и Центра компетенции Главного радиочастотного центра (ГРЧЦ). Приглашенный лектор профильных университетов и институтов повышения квалификации — *RPPA*, образовательной платформы *MDS*; назван лучшим преподавателем НИУ «Высшая школа экономики» 2024 года.

— Регулирование в сфере защиты персональных данных относительно молодое, но бурно развивающееся. Кажется, нет сейчас организации, государственного органа или учреждения, куда бы мы ни передавали свои персональные данные. Есть ли хоть кто-то сейчас, кто их не собирает или не обрабатывает?

— Нет. В любом случае вопросы обработки и защиты персональных данных в тех или иных преломлениях касаются всех. Ведь даже в *B2B*-бизнесе, где нет клиентов — физических лиц, у вас есть работники и даже бывшие работники. А если нет работников, то вы в любом случае касаетесь персональных данных контрагентов или их представителей. Да и клиенты *B2B*-бизнеса могут предъявлять свои договорные требования к обработке персональных данных.

— Какие ключевые изменения в регулировании персональных данных за последние два-три года Вы бы отметили?

— Изменений в этой области регулирования всегда было много, но в последние три года особенно. При этом появляется больше ограничительных норм, требований к бизнесу и новых видов ответственности. Это подтверждает возрастающую ценность данных, но становится ли от этого надежнее их защита? Сложный вопрос. Мы два года назад участвовали в подготовке стратегии рынка больших данных в России и считали количество регуляторных инициатив. На тот момент их было около 50, и каждый год это число увеличивается. Но при этом уровень защиты интересов субъектов персональных данных вряд ли растет. Все больше данных утекает, и не только из коммерческих источников, но и из государственных или окологосударственных, хотя государство вряд ли в этом признается. Интересы бизнеса не обеспечиваются, несмотря на развитие законодательства. И интересы государства, видимо, тоже недостаточно защищены, раз законодательство меняется так стремительно.

Ключевые изменения — это, конечно же, значительное увеличение ответственности: повышение размера административных штрафов и введение уголовной ответственности.

Другой тренд — это так называемая национализация данных, стремление государства направлять все потоки работы с данными через свои ресурсы («Госуслуги», «национальное озеро данных», или «ГосДата. хаб») и в пределах территории России.

Кроме этого, растет количество комплаенс-требований к бизнесу. В частности, это касается новых требований по уведомлению Роскомнадзора об обработке данных. Необходимо больше сведений включать в реестр операторов персональных данных. Также нужно уведомлять Роскомнадзор о трансграничной передаче. Более жесткие требования вводятся для управления согласием на обработку персональных данных, к внутренним документам организации, например, для обезличивания данных.

Согласно духу времени эволюционирует контрольный механизм Роскомнадзора. Сравнительно недавно этот орган стал активно применять дистанционный контроль, который осуществляется без взаимодействия с бизнесом. Инспектор может, сидя в кабинете, проверить сайт без предупреждения компании. Кроме этого, мораторий на внеплановые проверки закончился, а Роскомнадзор регулярно уточняет свой рискориентированный подход к проверкам, вводя новые показатели риска.

При этом никакого смягчения регулирования не наблюдается. Гайки только закручиваются, работать становится все сложнее. Предлагается большое количество законодательных инициатив, в том числе и от Минцифры, чтобы осовременить подходы к регулированию в этой области, но все они теряются в ходе межведомственных согласований. Например, уже несколько лет не получается согласовать введение экспериментального режима доверенных посредников, хотя, на мой взгляд, это достаточно безобидная концепция с точки зрения рисков и полезная как для бизнеса, так и для государства.

Технологии по работе с данными активно развиваются, но не их нормативное определение. Хотя с 1 сентября заработало "национальное озеро данных", это прежде всего государственный инструмент, частные аналоги пока невозможны.

Есть инициативы, которые вызывают опасение. Например, идея оставить право работать с персональными данными только большим компаниям, соответствующим определенным требованиям. Остальные должны будут делегировать им обработку. Эта инициатива влечет антиконкурентные риски и риски информационной безопасности, а также не учитывает реалии, в которых каждое юридическое лицо в России является оператором персональных данных, и сложно логистически представить, как можно реализовать эту идею.

У нас формируется какой-то свой подход к регулированию этих отношений, но логика его и целевой образ пока не очевидны.

— В чем, как Вам кажется, выражается этот наш особый подход?

— Раньше можно было сказать, что законодательство у нас в целом схоже с европейским, поскольку в его

основу были заложены Конвенция 108[1] и Директива ЕС 1995 года[2]. Но за последние годы оно существенно поменялось и использует нечто среднее между европейским и китайским подходами. Европейский подход — в первую очередь субъектно-центричный, когда во главу угла ставятся интересы субъекта персональных данных. Китайский в большей степени преследует публичные интересы, перенимая многие формальные аспекты из Европы. При этом американский ориентируется прежде всего на интересы бизнеса, но его также нельзя назвать вседозволяющим.

— Если все так или иначе вовлечены в обработку персональных данных и Роскомнадзор может удаленно вести контроль и проверять любого, то зачем нужен Реестр операторов персональных данных?

— На данный момент однозначного ответа на этот вопрос нет. Скорее всего, Роскомнадзор видит какую-то логику в существовании этого реестра. Это определенный открытый перечень контактов лиц, ответственных за обработку данных в компании, с которыми контролирующий орган может связаться. Это также дает дополнительный инструмент контроля посредством дистанционного наблюдения, т.е. возможность проверить, соблюдает ли компания те условия обработки данных, о которых заявила. Но эти доводы все же несколько наигранны. Во многих зарубежных юрисдикциях такого реликта, как наш реестр, уже давно нет. В Европе, где ранее были такие процедуры, теперь в контролирующий орган нужно сообщить лишь контактные данные лица, ответственного в компании за обработку персональных данных. Есть только отдельные национальные исключения для конкретных обработок данных, например в медицине. В иных юрисдикциях, например в США и Израиле, уведомлению подлежат отдельные базы / виды деятельности по обработке данных, в частности уведомлять должны брокеры данных.

Возможно, если сейчас примут очередной пакет изменений и введут новые правила о получении согласий на обработку персональных данных, то информация из реестра операторов может быть использована для проверки соответствия заявленных и реальных объемов обработки данных. Правда, остается большой вопрос о соотношении затрат на его ведение и пользы от него как для бизнеса, так и для государства.

Наверное, в установлении обязанности заявляться в этот реестр можно найти какой-то воспитательный элемент, когда бизнес таким образом принуждают разобраться с процессами сбора и обработки данных, более осознанно и ответственно подходить к этому процессу. Но все так же остается вопрос соотношения трудозатрат и эффективности такого стимула воздействия на бизнес.

— Насколько известно, в европейских юрисдикциях меры ответственности, применяемые к бизнесу в сфере защиты персональных данных, зависят от его размера. Есть ли у нас какая-то дифференциация ответственности?

— У нас есть определенные ограничения ответственности для индивидуальных предпринимателей, но в целом общая концепция КоАП РФ по интересующим нас «драматичным» статьям, в которых предусмотрены оборотные штрафы, различий в зависимости от размера бизнеса не предполагает, только в части расчета выручки компании. Дифференциация предусмотрена по объему обрабатываемых данных, если мы говорим про утечку. И если смотреть статьи с фиксированными штрафами в размере нескольких миллионов, то они применяются в равной степени ко всем.

— Возможно ли отдельно взятой компании выполнить все требования Закона о защите персональных данных[3]?

— В целом возможно. Основная сложность, на мой взгляд, заключается в том, что требования законодательства довольно часто меняются, а подходы контролирующих органов иногда отходят от сути закона, и бизнесу все труднее каждый раз перестраивать процессы для соблюдения меняющихся требований,

[1] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981).

[2] Директива Европейского парламента и Совета Европейского союза 95/46/ЕС от 24.10.1995 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных.

[3] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон о защите персональных данных).

особенно в случаях, когда бизнес-модель построена именно на работе с данными.

Например, когда-то согласие на обработку данных для бизнеса было не столь актуально. Потом практика контролирующего органа стала иной, причем изменения инициировал сам Роскомнадзор, и согласие теперь необходимо получать практически на всё. Появился даже такой термин, как «культ согласий», по аналогии с карго-культом. Теперь вдруг оказалось, что инструмент согласий бизнес использует неправильно и собирает их слишком много. Опять надо менять подходы. Уже есть даже и законопроект, потенциально ограничивающий сбор согласий.

Значит ли это, что на практике компаниям невозможно обеспечить соблюдение Закона о защите персональных данных, так как сложно успеть за изменениями и, более того, не всегда понятно, как их применять? И да и нет. Действительно, регулирование очень волатильное, исполнять его по силам тем компаниям, которые не формально следуют букве закона, а пытаются реально обеспечить защиту персональных данных и организуют соответствующий комплаенс. Вот нашим клиентам, например, не потребовалось ничего принципиально переделывать в своих процессах и документах, несмотря на значительные изменения закона, начиная с 2022 года и не приходится сейчас.

Например, требование об отдельности сбора согласий появилось только сейчас, однако мы всегда и так собирали их отдельно от иных документов или договоров, поскольку это следует из общих принципов и понимания того, как функционируют основания обработки данных. Или требования к договорам поручения — в 2022 году законодатель их изменил, конкретизировав содержание поручения, но мы и так всегда предусматривали эти положения и обязанности в наших поручениях для клиентов.

Конечно, к нашему сожалению, есть все же эксцессы, когда изменения выходят за рамки логики. Но проблема в том, что при таких изменениях придется поменять не просто формы бумажек, а сложные бизнес-процессы, за которыми стоят *IT*-системы, причем не только фронтенд- (видимая внешняя пользовательская часть сайта или приложения), но и бэкенд-системы (внутренняя логика построения программ). Такие доработки программ в крупных компаниях могут стоить десятки миллионов рублей. В худшем случае программы, которые не могут быть переработаны под новые требования, придется в целом заменять новыми версиями. Да, можно сказать, что при разработке программного обеспечения бизнес должен учитывать риски изменений регуляторных требований, но некоторые изменения выходят за рамки даже самых смелых предположений.

— Что это за эксцессы, например?

— Речь идет о планируемых изменениях в части использования согласий. Идея в том, что согласие не может требоваться оператором, кроме случаев, определенных законом[4].

Такая концепция в принципе не выглядит полностью неожиданной, скорее это можно рассматривать как уточнение и детализацию уже существующего требования о добровольности согласия и недопустимости его навязывания. В то же время многие трактуют законопроект радикально как запрет на сбор согласий, если они не требуются законом. В такой трактовке практическая реализация этой нормы потребует пересмотра бизнес-процессов, а также внесет дополнительные издержки не только для компаний, но и для государства (например, при перестройке тех же «Госуслуг»).

Проблема скорее в том, что до сих пор отсутствуют стабильные и понятные подходы в правоприменительной практике: разъяснения разрозненные, единообразие решений не сформировано, своего рода белой книги от регулятора нет, правовые основания на практике не равноценны между собой. Поэтому есть риск, что новое регулирование создаст неопределенность. Все будет зависеть от того, как оно будет применяться на практике: это может оказаться просто детализацией давно существующего принципа, но может и повлечь за собой значительные издержки без очевидного позитивного эффекта.

---

[4] В настоящий момент обсуждается законопроект (https://regulation.gov.ru/projects/159652) о внесении изменений в отдельные законодательные акты РФ («Антифрод-2»), которым предлагается дополнить ст. 18 Закона о персональных данных запретом на сбор согласий в случаях, не предусмотренных федеральным законом.

— Нужно ли, на ваш взгляд, что-то менять в подходах Роскомнадзора к проведению контроля за операторами данных?

— Сейчас Роскомнадзор в основном ограничивается формальным контролем, не исследуя глубоко бизнес-процессы и системы компаний. Понятно, что у него ограничены ресурсы и финансирование, и по-другому, наверное, быть не может. Но надо отметить, что между контролирующим органом и бизнесом становится больше полезного взаимодействия на различных площадках.

Вот сейчас, пока мы с вами разговариваем, идет День открытых дверей в Роскомнадзоре, где его представители отвечают на вопросы бизнеса. Есть, например, и центр компетенций при Роскомнадзоре, включающий экспертное сообщество и представителей бизнеса, а есть отраслевые стандарты, например стандарт Ассоциации больших данных, поддерживаемый регулятором. Диалог есть, не хватает только, чтобы достигнутые договоренности и решения оперативно оформлялись в виде разъясняющих документов и стандартов. Кажется, что Роскомнадзору можно брать еще больше ответственности и инициативы при транслировании рынку подходов и позиций. В любом случае в этом уже наметился позитивный тренд.

Вероятно, в следующем году могут появиться такие результаты. Например, в 2026 году Роскомнадзор планирует работу над определением стандартных наборов данных, требуемых операторам для конкретных целей, — такие наборы можно будет положить в основу и разъяснений по стандартным сценариям применимости законного интереса, и презумпции минимизации данных, и других благостных для бизнеса концепций, но только при условии, что государство таким образом не ограничит сбор данных, выходящих за пределы установленных наборов. В таком формате эту работу можно только поддержать.

— Допустим, компания выполнила все формальные требования закона: заявилась в реестр операторов, разработала политики, назначила ответственных за обработку персональных данных и т.п. Насколько реально технически бизнесу сейчас защитить персональные данные?

— В принципе, конечно же, защитить можно. При этом большинство известных утечек произошло под влиянием человеческого фактора. Хочется думать, что ответственность компании не должна зависеть только от того, насколько каждый ее работник действительно придерживается тех обязательств, которые компания на него накладывает.

Аксиома в том, что защитить данные на 100% нельзя, но компания должна сделать все возможное, чтобы их защитить, в том числе учить своего работника тому, что делать можно, а чего нельзя, проводить технические тесты защищенности, осуществлять периодические проверки и адаптировать меры по защите данных, в конце концов, минимизировать сбор и хранение данных. И если компания предпринимала все возможные меры, то это должно учитываться в качестве смягчающих или исключающих вину оснований в момент привлечения ее к ответственности за утечки и другие нарушения в области оборота персональных данных. Сейчас же это не берется в расчет вне зависимости от того, какие меры предпринимались компанией для защиты данных: она будет нести ответственность в соответствии с установленными санкциями. Такой подход не особо мотивирует бизнес усиливать меры по защите данных и больше инвестировать в информационную безопасность. Ведь все равно человеческий фактор полностью нельзя исключить.

Хочется надеяться, что этот недочет в подходе к ответственности бизнеса в сфере оборота персональных данных будет устранен, в том числе благодаря тому, что сейчас споры, относящиеся к персональным данным, переданы в ведение арбитражных судов, а не судов общей юрисдикции. Если процессы в компании правильно настроены, данные были достаточно защищены с точки зрения процедур и технических мер защиты, то в таких случаях компания нести ответственность не должна.

— С конца 2024 года введена еще и уголовная ответственность за незаконные действия с персональными данными. За что могут теперь привлечь к ответственности по УК?

— Нужно отметить, что статья 272.1 УК РФ скорее бланкетная и потому влечет риски расширительного толкования. На практике это означает, что теперь есть

риски уголовной ответственности для работников компаний за вполне рутинные бизнес-процессы, в которых есть какие-то изъяны. Например, компания получила согласие на использование персональных данных, срок его действия истек, но компания в силу каких-то случайных или технических ошибок не прекратила их обработку. Таким образом, использование этих данных стало незаконным и подпадает под уголовный состав. Очевидно, что, когда законодатель вводил эту норму, он преследовал другую цель, но вышло то, что вышло.

Менять норму нужно, добавив как минимум указание на заведомость незаконного доступа. Так, деяние должно включать в себя два элемента: незаконный сбор данных и незаконное использование. На практике незаконность получения персональных данных имеет очень широкую интерпретацию — практически любой порок при сборе данных приводит к незаконному сбору.

Понятие незаконного использования для целей уголовного преследования тоже необходимо существенно ограничить. Это не ситуации, когда на сайте компании нет политики по обработке персональных данных или она не включена в реестр операторов персональных данных, а только те случаи, когда у компании нет правового основания для их обработки. Эта статья — дамоклов меч, и при существующей редакции бизнес находится под постоянным риском привлечения к уголовной ответственности.

— Может ли компания застраховаться от риска утечек и привлечения к ответственности за них?

— Дискуссия о возможности введения такого страхования идет. Всероссийский совет страховщиков (ВСС) сейчас активно трудится над выработкой общих подходов к рынку киберстрахования и, например, уже рекомендовал признать недобросовестной практикой обещание клиентам по договорам оплатить штрафы за счет страховой выплаты. Страховые компании готовы предлагать так называемое киберстрахование, в том числе страхование риска начисления оборотных штрафов. Закон формально не позволяет страховать ответственность за его нарушение, так как это противоречит логике самого института страхования от рисков, наступление которых не зависит от страхователя. Наличие такой страховки у компании могло бы стать основанием, смягчающим ответственность, так как в этом случае компания сможет, например, компенсировать ущерб пострадавшим.

— Есть ли требования закона, которые потеряли смысл в связи с развитием технологий и использования искусственного интеллекта?

— Да. Например, болезненная тема — бесчисленные письменные согласия работников из-за формулировок Трудового кодекса. И новая норма, которую планируют ввести в рамках второго антифрод-пакета, эту проблему не решает, так как сбор таких согласий предусмотрен законом. Вообще письменные согласия по строгой форме сами по себе устарели, и, очевидно, их надо как-то реформировать — возможно, путем упрощения требований к их содержанию или формату получения, а может быть, и расширять такие основания обработки данных работников, как законный интерес или трудовой договор и локальные нормативные акты компании. Но пока практика меняется крайне осторожно. Хотя Роскомнадзор постепенно «оттаивает» к основаниям, альтернативным согласию, и уже обещает в грядущем году выпуск разъяснений по сценариям применения законного интереса. Сейчас такая работа активно ведется экспертами, с нетерпением ждем ее результатов!

Нужен взаимовыгодный подход. Можно, например, предложить бизнесу вместо использования согласий на обработку персональных данных собирать и обрабатывать их на основании законного интереса, но ввести запреты на конкретные случаи использования данных и требование предлагать субъекту данных возможность возражать против такой обработки (*opt-out*). Либо предписать внедрить обязательный функционал на сайте, в личном кабинете пользователя, через который можно было бы запретить отдельные цели обработки данных субъекта. Также можно было бы установить требование для компаний уведомлять Роскомнадзор о коммерческом использовании персональных данных или иных специфических действиях по обработке, имеющих высокие риски. Для этого как раз пригодился бы существующий реестр операторов.

Еще одно неактуальное требование, которое было введено в 2006 году с принятием Закона о защите персональных данных, — ограничение на объедине-

ние баз данных с разными целями обработки. Оно и тогда не работало, и сейчас не работает.

Болезненной остается ситуация с обезличиванием персональных данных. В России принят жесткий подход, согласно которому обезличенные данные остаются персональными во всех ситуациях, законодатель и Роскомнадзор не признают понятие анонимизации данных. К обезличиванию предъявляются довольно строгие требования, которые, однако, не позволяют бизнесу эффективно использовать полученные данные. Исключения для обработки обезличенных данных, которые формально прописаны в законе, проблему не решают: разработка и обучение моделей искусственного интеллекта с трудом укладываются в рамки аналитики или статистики, а само обезличивание в некоторых случаях все так же нуждается в самостоятельном основании.

За рубежом, например, подход к обезличиванию более лоялен. Так, в ЕС есть традиционное разделение анонимизированных данных, не подпадающих под регулирование персональных данных, и псевдонимизированных, которые остаются персональными. Но и псевдонимизированные данные в некоторых ситуациях можно рассматривать как анонимные в зависимости от того, кому они доступны. Это так называемый относительный подход к персональным данным, недавно поддержанный Судом справедливости ЕС. Это позволяет потенциально легализовать многие ситуации получения обезличенных данных, например, в результате автоматизированного процесса извлечения данных со страниц веб-ресурсов (скрейпинга) или совместного использования данных партнерами.

Или иной пример: в Южной Корее обезличенные данные прямо допускаются к использованию для научных и аналитических целей, включая разработку и обучение ИИ-моделей, при условии соблюдения технических и организационных гарантий. Кроме того, корейский законодатель рассматривает возможность ввести новое исключение: разрешать использование персональных данных для обучения ИИ и без их обезличивания, если цель обучения совместима с исходной целью их сбора и при условии разрешения регулятора.

При этом, к сожалению, законодательство не учитывает некоторые технологии, которые позволяют развивать новые продукты, делать взаимодействие человека, бизнеса и государства удобнее, в частности технологии дифференциальной приватности[5] и повышения конфиденциальности (*PETs*) — механизмы, которые позволяют минимизировать риски при обработке данных, в том числе их обмене между разными компаниями, например гомоморфное шифрование[6], федеративные вычисления и т.д. В России, где регулирование, особенно в части средств защиты информации, крайне формализованное и специфичное, пока нет понимания, как эти технологии «приземлить» в существующие нормы и возможно ли их использование без однозначного «зеленого света» от надзора. Хотя уже было несколько инициатив по институализации таких технологий.

— Вы говорили, что стоило бы ввести экспериментальный режим доверенных посредников. Кто к ним будет относиться?

— Доверенные посредники могут быть разные, главное, что это центр не сбора данных, а обработки, из которого без фактического доступа к данным можно получить результаты аналитики, чтобы сделать модель машинного обучения, проверить бизнес-теорию, адаптировать какие-то услуги или продукт. Таким образом, интересы субъектов персональных данных не страдают, владелец данных может на этом дополнительно заработать, а другие участники рынка — получать выгоду для разработки нового продукта, сервиса и т.п.

Сейчас таким доверенным посредником фактически становится государство, создавая «национальное озеро данных». Проблема только в том, что оно создается не для развития рынка, данные будут использоваться по определенному неизвестному алгоритму, бизнес сможет их применять только после того, как они немного отлежатся. Неизвестно, в каком виде будут эти данные в ГИС и в каком виде к ним получит доступ бизнес. В любом случае это произойдет после того, как данные «протухнут».

---

[5] Дифференциальная приватность — совокупность методов, которые обеспечивают максимально точные запросы в статистическую базу данных при одновременной минимизации возможности идентификации отдельных записей в ней. — *Прим. ред.*

[6] Гомоморфное шифрование — метод криптографии, позволяющий проводить вычисления над зашифрованными данными без предварительного их расшифрования. — *Прим. ред.*

— Тогда персональные данные должны быть предметом купли-продажи? Сейчас это возможно?

— Между компаниями данные могут продаваться и покупаться. Естественно, для этого должны быть получены те самые согласия граждан или иные правовые основания. Но формулируются эти сделки не как договор купли-продажи данных, а как услуги или предоставление доступа к базе данных. Может ли сам субъект персональных данных продать их? Российское право в настоящее время исключает такую возможность, а контролирующие органы не допускают ее. То есть если предложить субъекту персональных данных: давай ты нам данные, а мы тебе скидку, или давай я тебе скидку, а ты нам согласие на рекламу, — то у нас это считается недобросовестной практикой, ненадлежащим согласием. Делать так нельзя, по мнению контролирующих органов, кстати, даже не столько Роскомнадзора, сколько ФАС.

В американской модели во многих случаях продавать персональные данные можно по умолчанию, если субъект персональных данных это не запретил. В Европе тоже осторожно, но допускается встречное предоставление за данные. В Китае и США есть даже биржи данных. Почему у нас такой особый подход к этому вопросу, непонятно. Опять же — свой путь.

— Как Вы оцениваете рынок специалистов по защите данных? Достаточно ли юристов, работающих в этой сфере?

— На мой взгляд, сейчас чрезмерное внимание к сфере персональных данных ведет к тому, что в эту отрасль приходят много молодых юристов, а вот специалистов с достойным опытом не хватает. Уровень экспертности растет потому, что есть большое количество различных программ обучения, курсов, много информации в открытом доступе. Сообщество экспертов здесь довольно активное. Например, есть Ассоциация профессионалов по персональным данным (ПРОПД) и Общественное учреждение «Сообщество профессионалов в области приватности» (*Regional Privacy Professionals Association*, *RPPA*), которые активно поддерживают экспертов.

Мы в *Comply* также активно стараемся формировать практику, например постоянно публикуем тематические авторские материалы и разъяснения в СМИ и нашем телеграм-канале, запустили сервис «Комплайтека» — уникальную в своем роде базу знаний, содержащую разъяснения надзорных органов, которая позволяет юристам находить комментарии по разным вопросам нашей тематики в одном месте и не тратить время на поиски информации на разных ресурсах.

— То есть рынок практиков наполнен, на Ваш взгляд?

— Он наполнен, но не хватает подготовленных людей. Надо учитывать, что не всем компаниям, особенно малому бизнесу, нужны на полную ставку собственные сотрудники по защите персональных данных.

Поэтому сейчас спросом пользуются услуги *DPO-as-a-Service* — когда роль ответственного за эту сферу выполняет сторонняя организация на согласованных уровнях (*SLA*) и параметрах обслуживания. Для многих компаний, не имеющих нужных ресурсов, это крайне полезный сервис, позволяющий на постоянной основе получать от внешних экспертов все необходимое для соблюдения законодательства и развивать внутренние компетенции в сфере защиты данных без расходов на содержание собственной команды специалистов по защите персональных данных.