№ 07 (133) 2024 ПЕРСОНАЛЬНЫЕ ДАННЫЕ

«Мы на пороге изменений»

02.09.2024 ИНТЕРВЬЮ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Усиление регулирования в области защиты персональных данных и рост зрелости российских компаний привели к быстрому развитию privacy-культуры на российском рынке. В крупных технологических компаниях появились сотрудники и даже целые команды, отвечающие за защиту данных. Мы побеседовали с руководителем практики правовой поддержки защиты данных компании «Авито» Мариной Юфой. Она выступила инициатором мероприятия Avito Privacy Day, собравшего регулятора и представителей «Яндекса», «Озона», «Сбера», «Самоката»

и многих других компаний.

— Как у вас возник интерес к защите персональных данных?

— На выпускном экзамене юридического факультета МГУ вопрос про персональные данные стоил мне красного диплома. В те годы регулирование по персональным данным практически не работало и это была одна из формальных тем на последних курсах. И вот, спустя девять лет, я уже разъясняю другим, что такое персональные данные, и являюсь руководителем функции по их защите. Персональными данными я начала заниматься, почти случайно, работая в юридической фирме, которая одной из первых открыла практику защиты данных и кибербезопасности. Проработав шесть лет в консалтинге, я перешла в один из крупнейших банков, который ввел у себя должность специалиста по защите персональных данных клиентов и сотрудников компании — DPO (data privacy officer). Потом я стала региональным консультантом по privacy в международной платежной системе, а после ее ухода из России пришла в «Авито», где и работаю уже около двух лет.

— Какими навыками должен обладать DPO?

— DPO — это аналог того, кто в Законе о персональных данных называется ответственным за организацию обработки данных. Мы также часто называем себя прайвисистами (образование от слов «приватность» и privacy). Поскольку в Законе о персональных данных речь идет больше о правовых и организационных требованиях к защите персональных данных, на роль DPO чаще всего назначают людей с юридическим бэкграундом. Вообще, развивать профессию DPO начали именно юристы.

DPO работает вместе с лицом, ответственным за техническую защиту информации — CISO (Chief Information Security Officer). Согласно Закону в обязанности DPO входят три ключевые функции: объяснять сотрудникам требования законодательства; гарантировать соответствие закону всего, что происходит в компании с персональными данными; работать с обращениями граждан, чьи персональные данные она обрабатывает. В целом же объем

работы DPO гораздо шире: тут и разработка методологии, и, главное, выстраивание процессов и контроля по обеспечению правильной работы с данными.

— Как, на ваш взгляд, развивается юридическое регулирование приватности в России, какие вызовы стоят перед юристами в этой области?

— Мы очень быстро прошли путь от почти полного отсутствия внимания к этому вопросу в течение долгих лет (закон был принят в 2006 г.) до ситуации, когда невнимание со стороны бизнеса к защите персональных данных стало чревато серьезным репутационным риском, несмотря на то, что штрафы остаются небольшими. Сейчас мы на пороге изменений: юридическая ответственность будет синхронизирована с тем репутационным ущербом, который наносит утечка данных. Судебная практика в этом направлении активно развивается, так как повышается осведомленность граждан о своих правах.

Что касается юридических вызовов, то ключевой тезис, который обсуждается экспертным сообществом с регулятором, мы между собой называем «не согласием единым». Комплаенс по персональным данным у многих ассоциируется с наличием у компании огромного числа согласий их клиентов, пользователей и т. д. Мы сейчас уходим от концепции бумажного комплаенса. Во-первых, согласие на обработку — это не формальное правовое основание, которое подходит к любой ситуации. Есть много судебных решений по спорам, в рамках которых компания отказывалась предоставлять услуги без получения согласия на обработку персональных данных и была наказана за это, ведь для работы с данными имеются и другие основания, такие как исполнение договора, требования закона, законный интерес и пр. Во-вторых, помимо правовых оснований, нужно задумываться о других требованиях — определиться с тем, когда данные должны быть уничтожены, убедиться, что компания собираем только те данные, которые действительно нужны (так называемый принцип минимизации). Важно также максимально прозрачно донести до пользователя, как компания работает с данными и как пользователя может на этой повлиять, какие права у него есть.

— Нужна ли компаниям отдельная функция по защите персональных данных?

— Не думаю, что такая функция нужна абсолютно всем компаниям. Она требуется там, где персональные данные — это актив, или там, где имеется огромный штат сотрудников. Критериями являются количество этих данных, их значимость для бизнеса и сама деятельность компании именно с точки зрения прав субъектов и вреда, который может быть причинен в случае неправильного обращения с персональными данными. У небольшой компании, обрабатывающей какие-то чувствительные данные, такая функция, безусловно, должна быть. Но в HR-проектах рисков не меньше, чем в пользовательских.

— Как сейчас выглядит privacy-функция в «Авито»? Как распределяется функционал между вами и другими службами?

— Если говорить о тех, кто занимается защитой данных, то у нас есть кросс-функциональная команда, которую мы называем Avito Privacy Office. В нее входят юристы (практика защиты данных), информационная безопасность и технические специалисты, а также процессные методологи и пиарщики. Лидерами этой команды являются юристы.

У нас есть privacy-программа — основополагающий документ, согласованный топ-менеджерами. В нем зафиксирован наш уровень privacy-зрелости и указано, какого уровня мы хотим достичь. Когда компания вообще не ду- мает о персональных данных, делая то, о чем ее просят контрагент или регулятор, — это уровень ad hoc. Зрелый уровень соответствует выстроенным процессам, максимально задоку- ментированным, работающим и всем известным, и есть определенные процедуры оценки эффективности этих процессов, своевременно меняющиеся и адаптируемые. Мы стремимся именно к такому уровню.

У нас сфера персональных данных разбита на определенные блоки. Есть административная часть (все, что касается кросс-функциональной команды, privacy -программы, планирования, приоритетов) и сущностные вопросы, такие как аудиты процессов по работе с персональными данными; прозрачность работы, обеспечение прав субъектов

персональных данных (пользователей); комплаенс всей группы компаний; автоматизация процессов, связанных с персональными данными; взаимодействие с регулятором (задачи по налаживанию процессов подачи уведомлений и сведений госорганам в соответствии с законом). Отдельный блок у нас посвящен вопросам хранения и уничтожения данных, техническим мерам их защиты. Всеми нами любимый отдельный блок — развитие privacy-культуры, в его рамках мы организовали наш Avito Privacy Day.

Помимо privacy-офиса у нас есть privacy- амбассадоры — люди из бизнес-подразделений, помогающие реализовывать наши проекты, находить правильные контакты в бизнес-командах, уточнять информацию по бизнес-процессам. Это активные коллеги, которые не только помогают по нашему запросу, но и под- сказывают, какие процессы нужно исправить или улучшить.

Для разграничения ответственности команд в privacy-офисе у нас есть матрица ответственности («живой документ»). Мы договорились, что в «Авито» только юристы решают, что такое персональные данные. При наличии каких-либо сомнений ориентироваться нужно строго на методологию юристов. Внедрение технических мер по защите данных — ответственность блока информационной безопасности, но юристы помогают, если нужно. С одной стороны, юристы и безопасники — это автономные команды, но с другой — у нас общее направление работы. Мы знаем, кто за что отвечает, с кем необходимо консультироваться по тому или иному вопросу и кто принимает окончательное решение.

— Сколько юристов занимается только защитой персональных данных?

— Команда по персональным данным состоит из семи юристов, которые входят в состав юридической дирекции (у нас их более 70). Есть правовые партнеры, отвечающие за определенные направления бизнеса, являющиеся лицом и точкой входа всей юридической команды для своих бизнес-заказчиков, и центры экспертизы. Наша команда — центр экспертизы. Если есть, например, правовой партнер по вопросам сервиса продажи и аренды

недвижимости, то он решает все юридические вопросы, в том числе по персональным данным. Мы снабжаем его методологией, шаблонами и решениями и, конечно, вовлекаемся в решение нестандартных вопросов.

— Это много или мало с учетом объема задач?

— Для таких масштабов это вполне пропорциональный размер команды, хотя с учетом ужесточения ответственности проектов мы имеем потенциал для дальнейшего расширения.

В нашей команде почти каждый юрист сопровождает юридических бизнес-партнеров, то есть коллег, которые отвечают за правовую поддержку конкретных сервисов/направлений бизнеса. Юрист по данным должен разбираться в механике сервиса, чтобы помогать внедрять требования по работе с данными.

Большой пласт работы у нас связан с отработкой запросов и обращений. При наличии разных служб поддержки всегда есть эскалация на юриста, решающего наиболее сложные вопросы. Этим у нас занимается отдельный человек. Такова реалия любой большой компании — люди действительно стали чаще задавать вопросы по передаваемым ими сведениям.

Отдельный человек у нас занимается персональными данными сотрудников. Таков мой экспертный посыл: нельзя воспитать культуру уважения к пользовательским данным, если не соблюдать права сотрудников как субъектов персональных данных. Поэтому у нас очень много HR-проектов и выделен сотрудник на это.

Также отдельные сотрудники у нас занимаются группой компаний, поскольку это тоже актуально. Есть чисто наши DPO-проекты по внедрению реестра процессов организации обработки данных, выстраиванию какого-то процесса. Например, у нас есть процесс согласования выгрузок персональных данных. Если кто-то говорит, что ему нужны данные, мы никогда не выгрузим их ему просто так, не спросив предварительно, зачем они ему

потребовались, кому эти данные будут передаваться и для чего, есть ли договор.

— Сколько времени у вас ушло на выстраивание такой системы?

— При поддержке руководства на то, чтобы наладить все распределения матрицы ответственности и сделать так, чтобы Avito Privacy Office заработал как единая команда, нам понадобился приблизительно год.

— Должен ли юрист, который хочет заниматься персональными данными, разбираться в бизнес-процессах компании?

— Он должен в той или иной степени уметь разговаривать с людьми, задействованными в этих процессах, на одном языке. Главный вызов нашей работы состоит в том, что мы имеем дело с реально происходящими процессами. Важно понимать, что не бывает процессов по обработке персональных данных. Никто не работает с данными ради обработки данных. Всегда есть цель — запустить новый функционал в продукте, принять какого-то на работу, провести маркетинговое исследование, запустить рассылку и т. д. Это цели обработки данных. И чтобы правильно внедрить требования, нужно хорошо понимать цель, процесс, которые выстраивается для ее достижения и знать применимое к данному вопросу законодательство (трудовое, гражданское и т. д.). В противном случае все советы по персональным данным могут быть сведены к банальному взятию согласия, и это скорее всего поломает процесс. Поэтому мне кажется, что специалисты по данным всегда изучают что-то новое.

Второй момент. DPO в ходе работы сам тоже выстраивает процессы. Например, у нас есть процесс процесс оценки контрагентов на предмет их privacy-зрелости. Команда задает определенные вопросы, чтобы понять, насколько достойно происходит обращение с нашими персональными данными при их обработке.

— Как это проверить?

— Есть разные методики. Сейчас на российском рынке все чаще просят заполнить анкеты и предоставить основные документы. Наличие у контрагента отдельного функционала/должности DPO, как у нас, — очень хороший показатель зрелости этой компании. Мы проверяем их локальные нормативные акты, формулировки, описание процессов, регламенты реагирования на инциденты с данными. Нас интересует не копирование закона, а реальные процессные схемы.

— Что для вас первично при выстраивании процессов работы с данными: проблемы бизнеса, комплаенса или потребности пользователей?

— Мне кажется, что здесь нет особого конфликта. Основа нашего успеха — это доверие пользователей, поэтому мы ориентируемся на их ожидания.

Мы провели опрос по поводу того, как люди относятся к ценности своих персональных данных и какую работу с ними считают правильной. Понятно, что все ценят свои паспортные данные, все идентификаторы, которые выдаются государством, данные банковских карт, номера телефонов, адрес электронной почты. С одной стороны, люди говорят, что это всегда и везде запрашивают, но с другой — не хотят столкнуться например со спамом.

Как показывают наши исследования, представители совсем молодого поколения считают, что какие-то данные требуют больше защиты, а какие-то не требуют ее вовсе. Но большинство говорит, что все виды персональных данных надо защищать.

Я не думаю, что ожидания пользователей расходятся с комплаенсом. Порой они даже строже. Как показывают наши исследования, пользователи хотят, чтобы любая компания хранила данные строго на своих собственных серверах.

При этом в индустрии аутсорсинг в этой области невероятно распространен и не запрещен

законом (конечно, при соблюдении определенных требований).

— Должны ли вы в числе прочего разбираться в технологической части этого процесса?

— Как правило, DPO не отвечает за информационную безопасность, но, если мы говорим о DPO с юридическим бэкграундом, то он должен уметь разговаривать с безопасниками на одном языке. Иногда мероприятия, которые проводит служба безопасности, влияют на персональные данные сотрудников. Легализация мониторинга сотрудников, решений, которые отслеживают направление информации за контур компании, чтобы не допустить утечки, — это задачи юристов.

— Что вы делаете для повышения осведомленности сотрудников «Авито» в области работы с персональными данными?

— Одна из ключевых обязанностей команды DPO — изменение культуры. В этом году мы совершили прорыв среди российских компаний — мы провели Avito Privacy Day. Данное мероприятие напоминало фестиваль: сотрудников ждали печеньки с предсказаниями: «Печенька очень просит тебя установить двухфакторку», «Не проявляй эмпатию к человеку, который просит код из твоего СМС», «Персональные данные пользователей в твоих руках, поэтому их нельзя опускать». В офисе на всех экранах демонстрировалось слайд-шоу из privacy-картин. Например, картину «Неравный брак» мы подписали следующим образом: «Согласие должно быть добровольным». К этому дню мы запустили отдельный сайт на нашем внутрикорпоративном портале, собрав в одном месте все материалы и политики компании. Мы также в краткой и увлекательной форме изложили историю развития приватности через призму ключевых судебных процессов и громких событий, когда нарушения приватности привели к трагическим последствиям.

Нам очень помогает менеджмент. Анонс празднования privacy-дня и важности требований по персональным данным подготовили наши управляющие партнеры. Также топ-

менеджеры снялись в специальном ролике, рассказывающем сотрудникам, как мы относимся к приватности.

Ключевой посыл обучения — персональные данные принадлежат не нам, а нашим пользователям. Сейчас у нас в распоряжении могут находиться персональные данные, которые были собраны совершенно законно. Но это не означает, что мы можем делать с ним все, что угодно, потому что по закону персональные данные принадлежат людям, к которым они относятся.

Также у нас есть Avito Live — это регулярные встречи, когда мы собираемся всей компанией и делимся новостями. В privacy-день Avito Live полностью был посвящен вопросам обращения с персональными данными. Главный итог мероприятия состоит в том, что люди сами стали приходить и просить проверить, все ли у них в порядке.

— Вы провели Avito Privacy Day не только для себя, но и для других участников рынка. Какова была ваша цель?

— Да, это было мероприятие не только для сотрудников, но и бизнес-завтрак с коллегами из других компаний. Мы хотели сказать своим сотрудникам, что мы не одни такие, вся индустрия думает об этом. Хотели получить возможность пообщаться с регуляторами, а также с нашими соратниками и сообществом. Нам важна кооперация с индустрией, в какие-то моменты хочется синхронизироваться с ее представителями.

Были интересные инсайты, обмен опытом. Мы поняли, что все идут в одном направлении в плане подготовки к грядущим законодательным изменениям. Выяснили, что у всех одни и те же болевые точки. Обменялись лайфхаками по способам взаимодействия с бизнесом. Ведь у команд DPO во всех компаниях одна цель — сделать так, чтобы коллеги из бизнеса приходили к нам на этапе идеи и чтобы юристы по данным были полноценной частью проектной команды.

Марина Юфа

руководитель практики правовой поддержки защиты данных компании «Авито»

ИНТЕРВЬЮ

ПЕРСОНАЛЬНЫЕ ДАННЫЕ