Как DPO помогает бизнесу управлять рисками в сфере защиты данных

07.11.2024 СТАТЬИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЮРИДИЧЕСКАЯ ФУНКЦИЯ В КОМПАНИИ

Новые вызовы, встающие перед юридическими департаментами, придают нашему конкурсу The DEPARTMENT дополнительный импульс, и мы объявляем об открытии в 2025 г. номинации «Эффективная правовая защита конфиденциальной информации», партнерами которой станут комплаенс-бутик Comply и Ассоциация Больших Данных. Эта номинация призвана отметить компании, которые не только успешно внедрили программы по защите данных и обеспечению конфиденциальности, но и используют инновационные подходы и технологии. К участию в данной номинации мы приглашаем департаменты, которые формируют лучшие практики и демонстрируют высокие результаты по минимизации рисков нарушения конфиденциальности. Подробное описание номинации смотрите на сайте конкурса, а в этом номере журнала мы попросили Артема Дмитриева, управляющего партнера Comply, рассказать, почему значение функции Data Protection Officer (DPO) для бизнеса неуклонно возрастает.

Информация стала одним из самых ценных ресурсов нашего времени, это подтверждают такие инициативы, как Национальный проект «Экономика данных» и Стратегия рынка больших данных. Вместе с ростом значимости информации существенно повысилась и комплаенс-нагрузка на бизнес, появились новые риски. Компании все чаще сталкиваются с растущим числом угроз, связанных с утечкой данных, с новыми требованиями регуляторов и увеличивающимся количеством жалоб со стороны пользователей. Прежде всего это касается обработки и защиты персональных данных, где центральную роль играет функция DPO. В

таких условиях роль DPO становится не только юридической, но и стратегической, требующей постоянной адаптации к изменениям и выработки эффективных решений для снижения рисков. В статье рассматриваются ключевые причины приобретения функцией DPO столь весомой значимости в современных компаниях и ее помощь бизнесу в управлении рисками в сфере защиты данных.

Митигация рисков из случившихся утечек — дело рук не столько службы ИБ, сколько DPO

Независимо от зрелости информационной защиты компании исключить риск утечки данных невозможно. Поэтому следует озаботиться не только тем, как эту утечку не допустить, но и тем, как минимизировать наносимый ею ущерб. Если предотвращение утечки — задача преимущественно для отдела ИБ, то управление последствиями утечки и минимизация рисков из такой утечки — ответственность прежде всего DPO функции. Анализ судебных дел за последние 12 месяцев показывает, что только одной из восьми компаний удается доказать свою невиновность в утечке и избежать штрафа (рис. 1).

В этом году мы сопровождали несколько дел, касающихся утечки данных, и в двух из них нам удалось избавить компании от штрафов. Сейчас штрафы за утечку данных сравнительно невелики (до 1,5 млн рублей), однако грядущие изменения в законодательстве повысят их до 15 млн рублей за первый случай утечки и до 3% от выручки за последующие случаи. Это делает подготовку к соблюдению норм критически важной, а значит, самое время убедиться, что при необходимости вы сможете доказать Роскомнадзору, а затем и суду, что своевременно и в полном объеме сделали все возможное для предотвращения случившейся утечки данных и минимизации ее последствий.

Для этого вам потребуется доказать наличие в компании рутинных privacy-процедур по предотвращению утечки и надлежащее реагирование на допущенную утечку. Внедрение и поддержание таких privacy-процедур — задача непростая и трудоемкая. И это задача именно DPO. На основе опыта сопровождения проверок по следам утечек мы подготовили чек-лист

privacy-процедур, который вы можете скачать по ссылке. Кроме этого, в контексте обсуждения крайне полезно ознакомиться и с требованиями отраслевого стандарта защиты данных. Стандарт основывается на скоринговой модели оценки зрелости процессов обеспечения безопасности данных в компании. Такую модель как раз обсуждали в треках разработки смягчающих обстоятельств при назначении грядущих оборотных штрафов.

Систематический контроль за большинством бизнес-доменомов компании

Уже скоро мы будем провожать не только 2024-й год, но и мораторий на внеплановые проверки Роскомнадзора. Минцифры регулярно расширяет перечень индикаторов риска, свидетельствующих о нарушении обязательных требований. Например, обнаружение Роскомнадзором трех расхождений между сведениями из реестра его операторов и данными, размещенными на сайте компании, может стать основанием для проведения внеплановой проверки. Более того, Минцифры предлагает дополнить такой перечень случаями трансграничноŭ передачи без предварительного уведомления Роскомнадзора.

Медленно, но уверенно набирает обороты и осуществляемый Роскомнадзором дистанционный мониторинг сайтов. Для этого инспекторы могут использовать автоматизированный сервис по выявлению допущенных на сайтах нарушений. Его ожидаемая пропускная способность — десятки тысяч сайтов в год.

Указанные факторы требуют от DPO-функции внедрения рискориентированного подхода, поскольку рисков слишком много и они постоянно меняются вместе с бизнес-процессами. Причем для приоритезации контроля необходимо оценивать материальность и вероятность каждого риска и, конечно же, риск-аппетит компании.

Стандартизация и автоматизация

Количество обращениŭ граждан в Роскомнадзор по поводу защиты их персональных данных растет с каждым годом: прирост составляет около 30% (рис. 2). Так, в 2023 г. в Роскомнадзор

было более 64 тыс. жалоб на неправомерную обработку данных (всего из 71+ тыс. жалоб в Роскомнадзор). Это свидетельствует не только о повышении осведомленности граждан в данной сфере, но и об их заинтересованности в соблюдении своих прав компаниями.

Такие вызовы заставляют DPO разрабатывать и внедрять play-book'и по ключевым процедурам и институт privacy-чемпионов на все подразделения компании, использовать RACI-матрицы, повышать осведомленность работников, рутировать все возможные запросы по заранее определенным каналам и принимать другие нетривиальные организационные меры.

Кроме того, очевидна необходимость внедрения инструментов обнаружения и удаления неструктурированных данных, автоматизации управления и учета согласий и клиентских данных, внедрения иных решений privacy tech. Это тоже задача DPO.

Адаптация стратегии по работе с данными

Регуляторный ландшафт в сфере регулирования данных стремительно меняется. В течение года обсуждались десятки законодательных инициатив. Некоторые из них скоропостижно стали законами, например обязательность передачи данных в государственное «озеро». Остальные еще активно обсуждается, например, отход от согласий, реинкарнация законного интереса, токсичность накопления данных, ограничение прав компаний накапливать персональные данные. Таким образом, DPO должен не только понимать актуальное регулирование, но и предупреждать бизнес о том, что будет с регулированием завтра. Игнорирование и непонимание регуляторных трендов может стать дорогостоящей ошибкой: утратой возможности работать с данными или необходимостью перестройки ИТ-инфраструктуры. Такие операционные риски зачастую оказываются кратно дороже штрафов, поэтому бизнесу нужна privacy-программа «на вырост», адаптированная к стратегии компании.

***

Приведенные примеры существенно меняют функцию DPO в компаниях, повышая ее значимость, увеличивая объем решаемых задач и закрываемых рисков. Ведь и сегодня DPO функция вовлечена в большинство бизнес-процессов компании, закрывает не только и не столько риски штрафов, сколько критичные операционные риски. А с учетом векторов изменения регуляторного ландшафта — дальше — значимость DPO функции будет только возрастать.

Артем Дмитриев управляющий партнер Comply

СТАТЬИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЮРИДИЧЕСКАЯ ФУНКЦИЯ В КОМПАНИИ