№ 10 (136) 2024 ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Принят Закон об оборотных штрафах

05.12.2024 СТАТЬИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

30 ноября 2024 г. подписан Президентом и опубликован закон об ужесточении наказания за утечку персональных данных (ПД). В тот же день были опубликованы поправки в Уголовный кодекс РФ, предусматривающие ответственность за неправомерное использование ПД, доступ к которым получен незаконным путем. Многие склонны драматизировать возможные последствия от принятия второй группы поправок, опасаясь привлечения к уголовной ответственности добросовестных ответственных за обработку ПД (DPO). Артем Дмитриев пока не видит оснований для этого. В настоящей статье он анализирует поправки в Кодекс об административных нарушениях РФ и дает рекомендации по минимизации штрафных санкций за утечку ПД.

Лет семь назад один из европейских чиновников, комментируя вступающий в силу Общий регламент защиты персональных данных, отметил, что вводимые большие штрафы будут иметь отрезвляющий характер для бизнеса. И это действительно было так. Все говорили о GDPR, а многие что-то предпринимали для GDPR-комплаенса, боясь многомиллионных штрафов. Сегодня то же самое происходит у нас. Штрафы действительно отрезвляющие!

К слову, первые лица государства обещали принять этот закон еще два года назад, но чиновники и представители GR бизнеса не уступали. Кто из них победил, вы и сами знаете. И все же если бы не GR бизнеса, все было бы гораздо хуже.

Что там по утечкам, из того, что и так все знают?

Состав нарушения остался широким. Отвечать придется *за неправомерную передачу ПД (предоставление, распространение, доступ)*

. Получается, что передача данных на основании некорректного договора поручения тоже утечка? А неправомерная передача внутри организации все еще не будет признаваться утечкой, как Роскомнадзор декларировал прежде? Пока ответов на такие важные вопросы нет (табл. 1).

А что там еще?

Если утекают ПД менее 1000 субъектов или 10 000 ID, то по старинке будут применяться части 1(1) или 2(1) ст. 13.11 КоАП РФ.

Неважно, сколько утекло ПД, относимых к специальным категориям. И одной записи достаточно для 10-15 млн рублей штрафа.

DPO за новые составы нарушения не накажут, но по старым частям ст. 13.11 КоАП РФ наказание все еще возможно!

Отсечка для применения штрафов и их размеров определяется по количеству субъектов ПД или их ID, то есть уникальных обозначений. Что это такое? Будут ли считаться уникальными, например, скоринг и эмбеддинг? А внутренние идентификаторы в системе при условии, что они имеют смысл и идентифицирующий потенциал только для оператора? Одним словом, неразбериха.

И обидно, что теперь не будет работать 50-процентная скидка за раннюю оплату штрафа по ст. 13.11 КоАП РФ. Очень кстати было бы получить скидку в размере 250 млн рублей, но нет.

Когда грянет гром?

Изменения вступят в силу через шесть месяцев после принятия. Уверяют, что за прошлые утечки кары не будет, но есть пара нюансов.

• Как оправдаться, если злоумышленник публикует все новые дампы из прежней утечки?

Очевидно, что шанс оправдаться есть только в том случае, если вы ранее уведомляли Роскомнадзор об утечке и объем заявленных в уведомлении данных соотносится с вновь опубликованными дампами. В любом случае надо понимать, что доказывать это Роскомнадзору предстоит именно вам. В отсутствие доказательств обратного каждый новый дамп по умолчанию — новая утечка.

• Пока нет однозначной позиции по поводу того, является ли длящимся нарушением неуведомление Роскомнадзора об утечке. Если будет являться, то, несмотря на то что закон обратной силы не имеет, можно будет штрафовать на 3 млн рублей за прежние утечки, о которых вы «забыли» рассказать Роскомнадзору. В настоящее время есть как практика признания утечки длящимся нарушением, так и практика непризнания таковым, например, неуведомления о намерении осуществлять обработку ПД.

При этом, если компания привлекалась к ответственности за утечку по старым составам нарушения, то новая утечка, произошедшая уже после вступления в силу новых составов, не будет квалифицирована как повторная по ч. 15 или 18 ст. 13.11 КоАП РФ. Для повторности нужно быть привлеченным к ответственности по ч. 12–14, 16, 17.

Мягко стелет, да жестко спать!

Закон предусматривает смягчающие обстоятельства, но не так, как это декларировалось при доработке законопроекта. Если одновременно выполнить все указанные далее условия, то штраф может быть снижен до 0,1 от его минимального размера, но составит не менее 15 млн и не более 50 млн рублей (табл. 2).

И вот тут внимание! Смягчающие обстоятельства предусмотрены *только для штрафов по повторности*, то есть ч. 15 и 18 ст. 13.11 КоАП РФ. Для иных новых составов правонарушения остаются «общие» смягчающие обстоятельства Кодекса, как и прежде,

например:

— исключительные обстоятельства, связанные с характером нарушения и его последствиями, а также с финансовым положением юридического лица (ч. 3.2, 3.3 ст. 4.1 КоАП РФ);

— предотвращены вредные последствия такового, добровольно возмещен ущерб или устранен причиненный нарушением вред (ч. 3.4–1 ст. 4.1; п. 5, 6ч.1ст.4.2КоАПРФ);

— отсутствуют вред / угроза причинения вреда жизни и здоровью, а также имущественный ущерб (ч. 1 ст. 4.1.1 ич.2ст.3.4КоАПРФ);

— суд может признать смягчающими и иные обстоятельства, не указанные в законах (ч. 2 ст. 4.2 КоАП РФ).

То есть для большей части утечек практика будет складываться ровно так, как она складывается сейчас. Поэтому далее разберем, что же сегодня помогает счастливчикам избегать штрафов за утечку ПД, ведь именно эта стратегия сохранится после вступления в силу изменений.

Как быть? Быть privacy-совестливым. Как им стать?

Если утечка все же имела место, то далее у уважаемого DPO только два пути: сокращать размер штрафа либо пытаться полностью избежать такового. И то, и другое возможно, правда, первый путь сегодня не столь актуален, ведь сейчас коридор, в рамках которого суд назначает штраф за утечку ПД, составляет условные 40 тыс. рублей, но после изменений счет пойдет на миллионы.

Изменится ли стратегия по защите от штрафов после утечки?

Мы проанализировали судебную практику за прошлый год и вот, что получили. На данный

момент она неоднородна, суды же склонны признавать компании виновными в утечке ПД, не вдаваясь в подробности случившегося. И все же некоторым компаниям удавалось достучаться до судов.

Сначала назовем аргументы, на которые не следует уповать, поскольку они скорее всего не сработают или даже сработают против вас:

— хакерская атака чаще всего не воспринимается судами как обстоятельство, исключающее ответственность, хотя есть и обратная практика, но для того, чтобы этот аргумент работал, нужно соблюсти ряд иных условий (об этом далее);

— следует осторожнее упоминать меры, принимавшиеся в рамках реагирования на утечку ПД. Например, если после утечки вы внедрили двухфакторную аутентификацию и апеллировали к этому, суд может обратить такой аргумент против вас: если внедрили сейчас, значит, могли внедрить и раньше, следовательно, не приняли своевременно мер по защите ПД;

— поданное в Роскомнадзор уведомление об утечке чаще всего судами не признается смягчающим обстоятельством: это же и так ваша обязанность.

Какими аргументами оправдаться?

А вот что поможет, так это две группы доказательств, которые необходимо собрать:

— доказательства рутинных privacy-процедур по предотвращению утечек;

— доказательства надлежащего реагирования на утечку для минимизации ее последствий (табл. 3).

Важно, что это те дополнительные доказательства, которые Роскомнадзор у вас сам не

запросит в рамках утечки. Это то, что вам самостоятельно нужно предоставить ему для минимизации рисков и ущерба для компании — ваша extra mile, чтобы избежать штрафов. Отчеты по расследованию, уведомления, базовые локальные акты, согласия или договоры, реестр процессов у вас запросит инспектор сам.

По каждому из указанных комплаенс-доменов необходимо зафиксированными на бумаге доказательствами подтвердить исполнение компанией требования на практике. Буквально несколько примеров.

Проведение тренингов, посвященных защите ПД. При этом проводимый тренинг должен обновляться в соответствии с законодательными изменениями, а факты его проведения следует фиксировать в специальных журналах или логах, готовых к демонстрации Роскомнадзору.

Другой пример. Вы не только заключаете соответствующее требованиям закона поручение на обработку, если привлекаете обработчиков, но и проверяете каждого из них на предмет обеспечения должного уровня защиты ПД при обработке и в качестве доказательства проведения такой проверки можете представить, например, заполненные контрагентом чек-листы.

Если компания стала жертвой кибератаки, одним из убедительных доводов в пользу отсутствия ее вины в утечке будет уголовное дело, по которому она выступит потерпевшей стороной. Но опять-таки одной лишь записи в книге учета сообщений о преступлениях (КУСП) недостаточно — требуется возбуждение дела.

И последний пример. Компания ссылается на то, что никакого ущерба субъектам ПД утечкой не нанесено. Это нужно подкрепить доказательствами. Например, имела место коммуникация с субъектами по поводу произошедшего инцидента, усилен контроль за получением запросов субъектов, все запросы зафиксированы в журнале обращений и, наконец, что со стороны субъекта не поступало требований о возмещении убытков или

компенсации.

Таким образом, в случае утечки необходимо доказать, что комплаенс процедуры и контроли работают в каждодневной практике компании, а не просто зафиксированы на уровне регламентов и внутренних положений. Чем убедительнее вы будете, тем больше у вас шансов избежать штрафа или кратно его сократить. Напомним, что хотя нам удавалось добиваться положительных судебных решений, используя указанные выше аргументы, единой практики пока не сложилось.

В этом контексте также важным нововведением стала новая редакция ст. 23.1 КоАП РФ. Теперь нарушения, предусмотренные ст. 13.11 КоАП и совершенные юридическими лицами, их работниками и ИП, будут рассматриваться в арбитражных судах. Передача такого рода дел от мировых судей арбитражным, несомненно, повысит качество и однородность практики, а также приведет к более тщательному изучению всех обстоятельств случившейся утечки.

А напоследок...

Нельзя не сказать и о договорной обвязке с контрагентами, которые получают ПД от вас или которые ваша компания получает от них.

Как известно, ответственность за действия обработчика несет оператор ПД, поэтому уже сегодня каждый сознательный контрагент стремится получить от вас поручение и сделать его максимально широким. А это значит, что необходимо усилить контроль за бизнесом и за заключаемыми им договорами, чтобы в конце дня не оказалось, что ваша компания несет ответственность за все и вся.

А в межоператорских договорах необходимо четко разграничивать ответственность вашей компании за инциденты с ПД и ответственность контрагента.

Наш совет: не дожидаясь жаркого лета 2025 года, проводите внутренний аудит и налаживайте защиту ПД! Наш чек-лист вам в помощь.

Общий регуляторный ландшафт уже очерчен, но еще предстоит длительное обсуждение внесенных корректировок. Так, уже обсуждается более дифференцированная шкала в зависимости от типа бизнеса или специфики оператора.

Артем Дмитриев управляющий партнер Comply

СТАТЬИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ