Российский союз промышленников и предпринимателей

ПРЕДЛОЖЕНИЯ
по вопросу об установлении ответственности за утечки персональных данных

Минцифры России разрабатывает проект федерального закона о внесении изменений в Кодекс Российской Федерации об административных правонарушениях (далее – КоАП), предусматривающих введение отдельных составов административных правонарушений, связанных с утечкой персональных данных. Инициатива предполагает существенные санкции для бизнеса за нарушение конфиденциальности персональных данных, в том числе в случае принятия всех предусмотренных законодательством технических, организационных и правовых мер защиты информации. Максимальный размер штрафа, который обсуждается, составляет 3% от годовой выручки юридического лица (оборотный штраф).

Предлагаемый подход не позволит эффективно бороться с утечками персональных данных и одновременно создаст высокие риски для добросовестных участников рынка.

Российский союз промышленников и предпринимателей, **поддерживая усилия, направленные на повышение защищённости персональных данных граждан Российской Федерации**, считает необходимым при установлении ответственности за утечки персональных данных придерживаться следующих принципов.

1. **Вводимое регулирование не должно носить исключительно репрессивный характер, но должно стимулировать принятие мер по повышению защищенности персональных данных и соответствующих информационных систем.**

2. При регулировании необходимо обеспечить комплексный подход, предусматривающий **дифференцированную персональную** ответственность **на всех стадиях, способствующих утечке персональных данных**, для лиц, которые:

- не принимают достаточных мер для предотвращения утечек персональных данных;
- похищают персональные данные;
- незаконно используют похищенные персональные данные.

3. При регулировании необходимо **предусмотреть сопоставимую (равную) степень ответственности за необеспечение защищённости персональных данных в коммерческих, некоммерческих и государственных информационных системах**, для чего предусмотреть соответствующие состав правонарушения и ответственность.

4. Действующие нормы российского законодательства предусматривают возможность наступления ответственности только в случае совершения конкретных и определенных деяний.

При введении нового состава правонарушения необходимо **исключить безвиновную ответственность оператора персональных данных**, при которой такая ответственность могла бы наступить вне зависимости от принятия им всех технических, организационных и правовых мер защиты информации, в том числе в результате целенаправленных неправомерных действий третьих лиц. Иное будет противоречить положениям Общей части КоАП.

В соответствии со статьей 2.1 КоАП административным правонарушением признается не только противоправное, но и виновное действие (бездействие) физических или юридических лиц. Соответственно, наличие вины – необходимое условие привлечения к административной ответственности. При этом частью 2 статьи 2.1 КоАП установлено, что юридическое лицо признается виновным, если будет установлено, что у него имелась возможность для соблюдения правил и норм, но данным лицом не были приняты все зависящие от него меры по их соблюдению.

Указанная позиция подтверждается судебной практикой. Так, согласно пункту 16.1 Постановления Пленума Высшего Арбитражного Суда РФ от 2 июня 2004 г. № 10 «О некоторых вопросах, возникших в судебной практике при рассмотрении дел об административных правонарушениях» «когда в соответствующих статьях Особенной части КоАП возможность привлечения к административной ответственности за административное правонарушение ставится в зависимость от формы вины, в отношении юридических лиц требуется лишь установление того, что у соответствующего лица имелась возможность для соблюдения правил и норм, за нарушение которых предусмотрена административная ответственность, но им не были приняты все зависящие от него меры по их соблюдению».

С учётом изложенного, необходимо предусмотреть состав правонарушения таким образом, чтобы ответственность наступала исключительно в случае непринятия или принятия неадекватных выявленным угрозам безопасности, характеру обработки, объему и чувствительности обрабатываемых данных, тяжести последствий для субъекта персональных данных технических, организационных и правовых мер защиты информации операторов персональных данных, что повлекло утечку персональных данных.

5. **Регулирование, при определении степени ответственности за правонарушение, должно учитывать объемы утекших данных, их состав и чувствительность с точки зрения причинения возможного вреда субъекту персональных данных.**

6. При определении меры ответственности оператора персональных данных необходимо учитывать иные регуляторные требования к компаниям

(субъекты критической информационной инфраструктуры, кредитные организации, операторы связи и др.) и уже принимаемые ими меры по защите информации.

Дополнительно следует принимать во внимание, что импортозамещение, которое чаще всего производится без необходимого длительного тестирования устанавливаемого программного обеспечения и оборудования существенно повышает неконтролируемые для операторов персональных данных риски.

7. Предлагается рассмотреть следующий подход к установлению ответственности операторов персональных данных:

1) Минцифры России и Роскомнадзор с участием экспертов рынка разрабатывают детальные меры по защите персональных данных с учётом особенностей данных и риск-ориентированного подхода (характер обработки, чувствительность обрабатываемых персональных данных, оценки потенциального вреда субъекту персональных данных), которые являются рекомендательными.

Указанные меры должны быть основаны на анализе лучших решений и технологий в области информационной безопасности в России. Если оператор персональных данных их в полном объёме выполняет, но утечка персональных данных происходит, то оборотный штраф не может применяться (в том числе за повторную утечку).

2) Если оператор персональных данных принимает решение о самостоятельном определении принимаемых мер по защите персональных данных с учётом требований законодательства Российской Федерации, но у такого оператора происходит утечка персональных данных, тогда возможен оборотный штраф в случае повторного правонарушения.

8. Базу оборотного штрафа необходимо исчислять с учётом текущей практики введения оборотных штрафов по иным правонарушениям. **Если нарушение требований безопасности персональных данных повлекло утечку в процессе обработки данных, которая непосредственно связана с осуществлением предпринимательской деятельности и получением дохода, оборотный штраф может исчисляться исходя из этого дохода с учётом территории, на которой выявлено нарушение.** Во всех остальных случаях, в том числе, когда информационная система, в которой обрабатывались персональные данные, не используется для предпринимательской деятельности или нет дохода от ее использования, штраф должен быть фиксированным.

9. Предлагается **разработать подходы к добровольному внесудебному возмещению вреда субъектам персональных данных** в случае утечки их данных, однако требования к такому возмещению должны формироваться не на законодательном уровне, а в рамках саморегулирования. Такого рода компенсации должны носить добровольный характер в соответствии с принимаемыми компаниями правилами с учётом рекомендаций регуляторов.

10. Предлагается проработать **возможность введения регулярного добровольного аудита внедрения обязательных и дополнительных мер защиты персональных данных оператором персональных данных аккредитованными организациями** (или механизма добровольной сертификации), который бы исключал ответственность за утечки оператора при наличии положительного заключения такой аккредитованной организации.

11. Предлагается предусмотреть **исключение возможности привлечения к ответственности операторов в ситуации, когда субъекты персональных данных сами разместили персональные данные для неограниченного круг лиц, либо действия (бездействия) субъектов персональных данных привели к разглашению, изменению или удалению их персональных данных, например, нарушили режим обеспечения сохранности паролей и логинов для доступа к персональным данным на ресурсах операторов (многократное использование одного и того же логина и пароля, сообщение их третьим лицам).**

Это обусловлено спецификой функционирования пользовательских сервисов (социальные сети, маркетплейсы, сайты знакомств, стриминговые и блогерские сервисы), в рамках которых пользователи самостоятельно размещают личную информацию (в том числе персональные данные), чтобы другие пользователи могли связаться с ними (в целях знакомства, обсуждения размещенного развлекательного контента, согласования условий сделки и ее заключения, и т.д.). В связи с тем, что указанные данные размещаются самими пользователями и в их интересах публично, для неограниченного круга лиц, такие сведения могут быть использованы третьими лицами.

12. При регулировании предлагается учитывать практику зарубежных стран.

Так, законодательство Европейского Союза, США, Великобритании, Бразилии, Индии и Южной Кореи предусматривает следующий подход в отношении утечек персональных данных. Штрафы не взыскиваются за сам факт нарушения конфиденциальности персональных данных (то есть несанкционированную передачу данных). В указанных странах штрафы взыскиваются за нарушение обязанности принять адекватные выявленным угрозам, характеру обработки, чувствительности обрабатываемых данных, тяжести последствий для субъекта персональных данных технические и организационные меры по обеспечению безопасности персональных данных, если это привело к утечке персональных данных.