**Замечания и предложения РСПП**

**к проекту федерального закона № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»**

**(в части усиления ответственности за нарушение порядка обработки персональных данных)**

Проект федерального закона № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (в части усиления ответственности за нарушение порядка обработки персональных данных) (далее - законопроект) предусматривает введение составов административных правонарушений, связанных с утечкой персональных данных, и санкций для юридических лиц за утечку персональных данных, в том числе, штраф в размере до 3% от годовой выручки юридического лица (оборотный штраф), и устанавливает ответственность за неуведомление/несвоевременное уведомление уполномоченного органа об утечке персональных данных, повлекшей нарушение прав субъектов персональных данных.

По законопроекту имеются следующие замечания и предложения.

1. Нормы российского законодательства предусматривают возможность наступления ответственности только в случае совершения конкретных и определенных деяний. В соответствии со статьей 2.1 Кодекса Российской Федерации об административных правонарушениях 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 РФ 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.

В настоящее время ни одна из существующих инфраструктур информационной безопасности не способна обеспечить полную защищенность и неуязвимость хранимых данных. Таким образом, вложение компанией значительных средств в обеспечение информационной безопасности не снимает риск наступления ответственности в виде, в том числе, оборотного штрафа, размер которого может потенциально остановить хозяйственную деятельность и привести к банкротству.

Положениями проектируемых частей 12-14, 16 статьи 13.11 КоАП РФ предусматривается установление безусловной ответственности оператора, которая будет наступать также в случаях, когда неправомерная передача (предоставление, распространение, доступ) указанной информации произошла в результате неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование со стороны третьих лиц, не являющихся должностными лицами или работниками оператора.

При этом привлечение к ответственности не связано с принятием либо непринятием оператором организационных, правовых и технических мер по защите информации, предусмотренных законодательством о персональных данных.

Предствляется необходимым при введении новых составов административных правонарушений проектируемых частей 12-14, 16 статьи 13.11 КоАП РФ исключить безвиновную ответственность оператора персональных данных, при которых она могла бы наступить вне зависимости от принятых им организационных, правовых и технических мер защиты информации в результате неправомерных действий третьих лиц.

В этой связи в законопроекте предлагается изложить состав правонарушения таким образом, чтобы ответственность наступала только 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.

2. Законопроект предусматривает, что за повторное нарушение юридическому лицу устанавливается штраф в размере от 0,1% до 3% выручки за год, предшествующий году, в котором было выявлено нарушение, но не менее 15 млн руб. и не более 500 млн руб. (оборотный штраф), но не позволяет определить при каких обстоятельствах применяется тот или иной размер оборотного штрафа. Такое расширение дискреции уполномоченного органа, особенно при отсутствии сложившейся правоприменительной практики по данному вопросу, может привести к необоснованным взысканиям с российских компаний.

Полагаем, что размер штрафа за повторное нарушение за утечку персональных данных в обязательном порядке должен учитывать не только количественный показатель, но и состав утекших персональных данных. Законопроект не учитывает тот факт, что организации владеют различными по своему составу персональными данными, которые внутри одной категории могут существенно отличаться, что, в свою очередь, ведет к различным рискам при их утечке.

Базу оборотного штрафа предлагается 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.

В этой связи предлагается дополнить законопроект положением, что размер налагаемого штрафа за повторное правонарушение должен определяться на основании регламентированного расчета, учитывающего объемы утекших данных, их состав, чувствительность с точки зрения причинения возможного вреда субъекту персональных данных, непосредственную связь с осуществлением компанией предпринимательской деятельности и получением дохода.

3. Предлагаемые законопроектом оборотные штрафы создают риск информационных атак на компанию с целью воздействия на ее хозяйственную деятельность.

Подобная схема может быть применена в целях недобросовестной конкурентной борьбы, попытках дестабилизации отечественной экономики со стороны недружественных стран.

В этой связи предлагается дополнить законопроект термином «умышленная информационная атака» и в случае умышленной информационной атаки возложить ответственность не на оператора персональных данных, а на злоумышленника при условии, что оператор персональных данных исполнил необходимые предписанные законодательством меры по защите своих информационных систем.

4. Законопроектом устанавливается ответственность за неуведомление/несвоевременное уведомление уполномоченного органа об утечке персональных данных, повлекшей нарушение прав субъектов персональных данных. При этом не установлены объективные критерии, в соответствии с которыми будет решаться вопрос о наличии или отсутствии последствий в виду нарушения прав субъектов персональных данных. Кроме того, данная норма может быть интерпретирована неоднозначно и имеет определенные коррупционные риски, поскольку наложение штрафных санкций зависит от возможности юридического лица доказать факт обнаружения утечки персональных данных (при невыполнении обязанности), а также от конкретной даты обнаружения такой утечки (при несвоевременном выполнении обязанности).

В связи с этим предлагается дополнить законопроект положениями, конкретизирующими случаи наступления такой ответственности, учитывающими при определении суммы штрафов степень и размер вреда, наносимого субъекту персональных данных, количество дней просрочки направления уведомления об утечке персональных данных.

5. Предлагается дополнить законопроект положением, предусматривающим исключение возможности привлечения к ответственности операторов персональных данных 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).

Указанное 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.).

6. Положениями проектируемых частей 12-14 статьи 13.11 Кодекса РФ об административных правонарушениях предусматривается установление административной ответственности, в том числе за действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей идентификаторы.

Предлагаемое законопроектом понятие «идентификатор» полностью дублирует аналогичный термин, определяемый пп. 6 ст. 2 Федерального закона от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации». Введенное законодательно в оборот понятие «идентификатор» используется в целях идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных с использованием государственной информационной системы «ЕСИА», а также при ее взаимодействии в целях осуществления аутентификации с использованием биометрических персональных данных физических лиц с информационными системами аккредитованных государственных органов, Банка России. Различие в сферах применения законодательно установленных понятий «идентификатор» и «персональные данные» не создает правовых коллизий и не порождает негативных последствий. Идентификаторы в законодательстве об идентификации и аутентификации либо являются атрибутом государственной информационной системы, либо изначально присваиваются ею. Использование в КоАП РФ для целей, связанных с защитой персональных данных, понятия «идентификатор», введенного ранее исключительно для целей законодательного регулирования правоотношений, связанных с идентификацией и аутентификации, одновременно содержательно совпадающего с понятием «персональные данные», установленным в ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», создаст правовую коллизию, которая с высокой степенью вероятности негативно отразится на формировании практики применения проектируемых и действующих норм КоАП РФ, дальнейшем применении связанных норм законодательства о персональных данных и иных смежных отраслей законодательства. Так, например, сохранение понятия «идентификатор» в проектируемых нормах КоАП РФ влечет риск того, что под собственно идентификатором будет пониматься исключительно государственный идентификатор – мнемоника системы в ЕСИА или идентификатор пользователя в ЕСИА. Эта информация может присутствовать в утечках из ГИС или систем, обеспечивающих взаимодействие с ЕСИА

Одновременно следует обратить внимание на то, что проектируемая статья 2721 УК РФ (проект федерального закона № 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации») не предусматривает уголовной ответственности за незаконное использование и (или) передачу (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации, содержащей идентификаторы, полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование.

С учетом изложенного предлагается в проектируемом пункте 12 ст. 13.11 КоАП РФ слова «и (или) от десяти тысяч до ста тысяч уникальных обозначений сведений о физических лицах, необходимых для определения таких лиц (далее - идентификаторы),» исключить, в проектируемых пунктах 13-14 той же статьи КоАП РФ соответственно слова «и (или) от ста тысяч до одного миллиона идентификаторов,» и слова «и (или) более одного миллиона идентификаторов,» исключить.

7. Положения проектируемой части 16 статьи 13.11 КоАП РФ предусматривают установление ответственности оператора за утечку специальной категории персональных данных без ее дифференцирования в зависимости от масштаба (устанавливается одинаковая ответственность за утечку данных 1 субъекта или 100 тысяч и более субъектов персональных данных), что противоречит принципам соразмерности и справедливости административного наказания.

Предлагается изменить данный подход и применить принцип дифференциации ответственности аналогично нормам, устанавливаемым в проектируемых частях 12-14 статьи 13.11 КоАП РФ.

8. Законопроект не предполагает учет смягчающих обстоятельств. Наряду с отягчающими обстоятельствами предлагается ввести смягчающие обстоятельства, в частности назначение штрафа в минимальном размере, если компания - оператор приняла дополнительные требования к защите данных в рамках прохождения добровольной сертификации/аудита, проводила обезличивание персональных данных, в результате чего объективно минимизирован вред гражданам в результате утечки, а также предприняла меры, необходимые и достаточные для устранения последствий утечки или причин, способствовавших утечке. Такой механизм практикуется в ряде стран и стимулирует ответственное и проактивное отношение к вопросам информационной безопасности, а также развивает рынок соответствующих услуг и сервисов.

9. Согласно части 3 статьи 6 Федерального закона «О персональных данных» оператор вправе поручить обработку персональных данные третьему лицу – обработчику персональных данных при условии включения в поручение на обработку требований, предусмотренных ч.3 статьи 6 Федерального закона «О персональных данных» (в частности, такие обязанности обработчика, как соблюдение конфиденциальности персональных данных, обеспечение безопасности персональных данных при их обработке, уведомление оператора о фактах неправомерной или случайной передачи данных).

Отношения оператора и обработчика регулируются гражданским законодательством: то есть обязательство обработчика соблюдать требования поручения оператора обеспечиваются только гражданско-правовой ответственностью, установленной в договоре с оператором. При этом в ч.3 статьи 6 Федерального закона «О персональных данных» указано, что обработчик обязан соблюдать принципы и правила обработки персональных данных, а также соблюдать конфиденциальность персональных данных. При этом КоАП РФ не устанавливает ответственность обработчика.

Утечка и незаконная передача персональных данных могут произойти на стороне обработчика, при этом оператор может в принципе не быть об этом не извещен обработчиком. Таким образом, оператор, не совершавший правонарушения, будет привлечен к административной ответственности, при этом обработчик понесет только гражданско-правовую ответственность (без учета необходимости доказывания оператором наличия оснований для взыскания с обработчика возмещения, а также сложностью с исполнением судебного решения). В связи с чем у обработчика будет меньше стимула соблюдать законодательство о персональных данных.

В этой связи предлагаем в законопроекте предусмотреть, что ответственность за утечку и незаконную передачу персональных данных несет обработчик персональных данных, если правонарушение совершено обработчиком.

В частях 10 – 14 статьи 13.11 КоАП РФ в редакции законопроекта слова «оператором» предлагаем заменить на слова «оператором или лицом, обрабатывающими персональные данные на основании поручения оператора».

10. Установленный законопроектом срок вступления в силу предлагаемых изменений не позволит операторам персональных данных сформировать ответственную политику компании по отношению к сохранности персональных данных. Для качественного улучшения ситуации потребуется дать компаниям возможность подготовиться к новым требованиям, повысить уровень информационной безопасности и принять все необходимые меры для защиты от утечек.

В России зарегистрировано более 6 млн субъектов малого и среднего предпринимательства, государственных и муниципальных организаций, крупных компаний. При этом организаций, которые обеспечивают кибербезопасность существенно меньше. При вступлении закона в силу большое число организаций будет вынуждено единовременно обратиться к ограниченному количеству компаний в сфере кибербезопасности, которые не справятся с повышенным спросом в столь ограниченный срок.

В этой связи предлагается в законопроекте предусмотреть более длительный переходный период перед вступлением новых штрафов в силу – не ранее 1 января 2026 года.

Предусмотренный законопроектом репрессивный подход без комплексного решения вопросов обеспечения информационной безопасности, без принятия эффективных мер против «хакеров» и иных злоумышленников, без подробной регламентации требований по защите информации, не только не будет способствовать достижению заявленной в пояснительной записке цели законопроекта - стимулировать операторов персональных данных инвестировать в развитие инфраструктуры информационной безопасности, но создаст предпосылки, что компании начнут передавать функцию обработки персональных данных отдельным компаниям с минимальной выручкой.