STONEBRIDGE LEGAL

УЖЕСТОЧЕНИЕ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3 декабря 2024

30 ноября 2024 года Президент РФ подписал законопроекты № 502113-8 (изменения в Уголовный кодекс РФ — ***УК РФ***)[1] и № 502104-8 (изменения в Кодекс об административных правонарушениях — ***КоАП***)[2], которые были опубликованы в тот же день. Указанные документы, помимо прочего, ужесточают ответственность бизнеса и менеджмента за нарушение правил обработки персональных данных.

При этом изменения в УК РФ вступят в силу уже 10 декабря 2024 года, а вот изменения в КоАП начнут действовать только с 30 мая 2025 года (после завершения переходного периода в 180 дней). Тем не менее, именно изменения в КоАП представляют особый интерес для бизнеса, поскольку существенно повышают штрафы за нарушения в области обработки персональных данных.

ИЗМЕНЕНИЯ В КОАП

Указанный законопроект вводит как новые составы правонарушений, так и меняет ответственность за уже существующие.

1. Новые штрафы

Кратно повышены штрафы за «общие» правонарушения в области обработки персональных данных (то есть, в случае обработки в не предусмотренных законодательством случаях либо при обработке, несовместимой с целями сбора персональных данных, — ч. 1 и 1.1 ст. 13.11 КоАП). Далее мы приводим сравнительный анализ этих изменений.

Ст. 13.11 КоАП	Субъекты	Действующий размер штрафа (руб.)	Новый размер штрафа (руб.)
ч. 1 (первичное нарушение)	Должностные лица	от 10 000 до 20 000	от 50 000 до 100 000
	Юридические лица	60 000 до 100 000	от 150 000 до 300 000
ч. 1.1 (повторное нарушение)	Должностные лица	от 20 000 до 50 000	от 100 000 до 200 000
	Юридические лица	от 100 000 до 300 000	от 300 000 до 500 000

2. Новые составы правонарушений

Законопроект вносит новые составы правонарушений, которые условно можно разделить на деяния:

a. в связи с неуведомлением Роскомнадзора;
b. связанные с неправомерной передачей (*предоставлением, распространением, доступом*) персональных данных (далее — «***утечка персональных данных***»); и
c. нарушающие порядок или правила обработки персональных данных.

[1] https://sozd.duma.gov.ru/bill/502113-8
[2] https://sozd.duma.gov.ru/bill/502104-8#bh_histras

Далее мы не указываем размер штрафов для представителей государственных или муниципальных органов либо некоммерческих организаций.

Нарушения за неуведомление Роскомнадзора

В ст. 13.11 КоАП в качестве частей 10 и 11 добавлены новые составы правонарушений, которые предусматривают наказания за неуведомление или несвоевременное уведомление Роскомнадзора:

- о намерении обрабатывать персональные данные; а также
- о случаях неправомерной или случайной утечки персональных данных, повлёкшей нарушение прав субъектов персональных данных.

За указанные нарушения для юридических лиц предусмотрены следующие штрафы:

- от 100 тыс. до 300 тыс. рублей; или
- от 1 млн до 3 млн рублей соответственно.

Нарушения, связанные с утечками персональных данных

Отдельного внимания заслуживают новые административные взыскания за утечку персональных данных и идентификаторов физических лиц. К последним могут относиться такие отдельно взятые данные, как номера, числовые, буквенные или иные уникальные обозначения сведений о физическом лице. Правонарушением будут считаться действия или бездействие оператора, повлёкшие неправомерную утечку персональных данных.

В зависимости от объёма и категорий неправомерно переданных сведений штрафы для юридических лиц могут достигать **20 млн рублей**. В случае повторных нарушений, связанных с утечкой данных, предусмотрены **оборотные штрафы в размере от 1% до 3% от годовой выручки** оператора персональных данных, но **не менее 20 млн** и **не более 500 млн рублей**.

При этом штраф может быть назначен ниже минимального порога лишь при одновременном соблюдении следующих условий:

- юридическое лицо произвело значительные инвестиции для обеспечения информационной безопасности (не менее 0,1% годового совокупного размера суммы выручки либо размера собственных средств (капитала) кредитной организации за предыдущие 3 года);
- дополнительным требованием является наличие у самого оператора соответствующей лицензии в области шифрования (криптографии) или технической защиты конфиденциальной информации либо привлечение бизнесом лицензированной организации для обеспечения своей информационной безопасности;
- юридическое лицо документально подтверждает соблюдение за предыдущие 12 месяцев требований законодательства при обработке персональных данных в своих информационных системах; и

- отсутствуют такие отягчающие обстоятельства, как продолжение противоправного поведения и (или) повторные нарушения, предусмотренные частями 1 — 11 статьи 13.11 КоАП (включая новые нормы о неуведомлении Роскомнадзора об обработке персональных данных и/или их утечке) и/или статьями 13.6 и 13.12 КоАП (о нарушениях в области использования средств шифрования и правил защиты информации).

Размер пониженного административного взыскания также лимитирован и составляет 1/10 минимального размера административного штрафа, но не менее 15 млн и не более 50 млн рублей.

Правонарушения в области порядка или правил обработки персональных данных

Компании, нарушающие порядок или технологические правила обработки биометрических персональных данных для идентификации и аутентификации физических лиц, могут быть подвергнуты штрафам в размере до 2 млн рублей. Руководители таких компаний за те же нарушения могут быть оштрафованы на сумму до 1 млн рублей.

Помимо прочего, штраф до 500 тыс. рублей может быть наложен на юридическое лицо за отказ в заключении, исполнении, изменении или расторжении договора с потребителем, если это связано с отказом потребителя от идентификации или аутентификации с использованием его биометрических данных. За то же правонарушение на должностное лицо компании может быть наложен штраф до 100 тыс. рублей.

ИЗМЕНЕНИЯ В УК РФ

В УК РФ вводится новая статья 272.1, устанавливающая ответственность за незаконные действия с неправомерно полученной компьютерной информацией, содержащей персональные данные. Помимо общей нормы, предусмотрены специальные составы преступлений с соответствующими более строгими наказаниями за них, такие как:

- действия в отношении персональных данных несовершеннолетних, специальных категорий или биометрических персональных данных;
- деяния, совершённые из корыстной заинтересованности с причинением крупного ущерба группой лиц по предварительному сговору или с использованием служебного положения;
- деяния, связанные с трансграничной передачей персональных данных или трансграничным перемещением носителей информации, которые их содержат; и
- деяния, которые повлекли тяжкие последствия или совершены организованной группой.

Отдельно предусмотрено наказание за создание и (или) обеспечение работы ресурса, предназначенного для совершения незаконных операций с персональными данными, полученными незаконным путём.

Указанные преступления могут повлечь за собой наказания вплоть до 10 лет лишения свободы. Исключение составляют случаи, когда персональные данные обрабатываются физическими лицами для личных или семейных нужд.

НАШИ ПРЕДЛОЖЕНИЯ И РЕКОМЕНДАЦИИ

- Несмотря на длительный срок обсуждения законопроектов, их положения могут порождать неоднозначные трактовки у представителей власти и бизнеса. В частности, для применения штрафов ниже минимальных значений неоднозначны методы расчёта инвестиций (расходов) оператора: требуется брать средневзвешенный показатель годового совокупного размера суммы выручки за предыдущий трёхлетний период или же учитывать общий суммарный объём выручки за все 3 года. Также нет однозначной позиции по поводу того, какие именно документы должны подтверждать факт соблюдения законодательных требований.

- Мы рекомендуем заблаговременно начать подготовку к внутренней проверке (аудиту) по вопросам обеспечения информационной безопасности и надлежащей обработки персональных данных, поскольку такую проверку целесообразно проводить с учётом уже новых требований, которые вступят в силу по завершении 180-дневного переходного периода. Учитывая объём внесённых в законодательство изменений, по результатам аудита необходимо будет актуализировать действующие локальные нормативные акты, политики, инструкции и иные документы об обработке и защите персональных данных. В некоторых ситуациях может потребоваться корректировка технологических бизнес-процессов, а также способов и методов управления данными.

- В отдельных случаях для снижения риска привлечения к ответственности целесообразным может быть получение лицензий в сфере шифрования (криптографии) и технической защиты конфиденциальной информации.

STONEBRIDGE LEGAL

T: +7 495 785 30 00
E: marketing@stonebridgelegal.ru

119017, Россия, Москва
Кадашёвская наб, д. 14, к. 2