Comply.Pulse
#5| Октябрь 2022

ПЛОХО ДЛЯ НАС, ОТЛИЧНО ДЛЯ ВАС 😄

Правительство утвердило продление моратория на проведение плановых проверок бизнеса на 2023 год. Да, и проверок Роскомнадзора. Что это значит для бизнеса, и можно ли пока забыть про privacy-комплаенс?
Читайте в новом выпуске Comply.Pulse.

К кому в 2023 году Роскомнадзор сможет заглянуть с проверкой?

Мораторий на плановые проверки не распространяется на компании с высоким уровнем риска. Такие компании могут быть включены в план проверок на следующий год.

У кого высокий уровень риска?

Практически наверняка НЕ у вас! Если есть сомнения, читайте этот раздел.

Высокий уровень риска складывается из двух переменных: (i) тяжести и (ii) вероятности. Высокому уровню риска соответствует (i) группа тяжести А или Б + (ii) 1-я группа вероятности (скучные детали см. в Постановлении Правительства № 1046). Хотя почти каждая компания попадает в требуемую группу тяжести, но в 1-ю группу вероятности «угодить» не так просто. И вот почему:

i. Такие группы **тяжести** применимы, если вы осуществляете трансграничную передачу данных (ПД) в «неадекватные» страны (например, США), обрабатываете биометрию и специальные категории ПД или храните данные на зарубежных серверах, обрабатываете данные более 20 тысяч человек или, например, используете зарубежные сервисы и ПО для сбора данных. Во избежание сомнений, достаточно любого из приведенных критериев.

ii. А к 1-й группе **вероятности** относятся только те компании, которые повторно нарушают законодательство о ПД по отдельным составам КоАП РФ. Например, обрабатывают данные без согласия, когда оно необходимо, или нарушают сроки ответа на запрос субъекта ПД. Критерий повторности означает наличие уже вынесенного предписания или предупреждения Роскомнадзора за последние 2 года, либо привлечение к ответственности по аналогичному составу за 3 предшествующих года.

Если эти критерии неприменимы, то можно ли забыть о privacy на год?

Отнюдь! Ведь мораторий не распространяется на проведение других контрольно-надзорных мероприятий, а именно:

i. дистанционное наблюдение и

ii. внеплановый контроль.

Кроме этого, несмотря на мораторий могут проводиться (и даже прямо сейчас проводятся) внеплановые проверки Роскомнадзора по требованию прокуратуры или по поручению Правительства.

Мы прежде и представить себе не могли, что чиновники будут задействовать эти крайние меры. Но, как показывает практика, очень даже будут! За последние месяцы нам известно минимум о пяти таких внеплановых проверках. А это очень много.

Как выглядят сохранившиеся в 2023 году формы контроля?

- При дистанционном наблюдении Роскомнадзор (в т.ч. с помощью автоматизированных скриптов) анализирует сайты и мобильные приложения. Наблюдение бывает плановым (на основании плана наблюдений, в котором могут оказаться ваши сайты или приложения) или внеплановым, поводом для которого может стать жалоба клиента или работника, заявление privacy-экстремиста или новость в СМИ / на Интернет-портале о произошедшей утечке данных. Да в общем-то что угодно!

- По результатам дистанционного наблюдения Роскомнадзор может направить компании предписание об устранении выявленных нарушений, а также вынести предостережение или назначить внеплановую проверку (документарную или выездную). Игнорирование предписаний или предостережений также может привести к ответственности за неисполнение требований органа власти или назначению внеплановой проверки.

- Если жалоба или обращение субъекта поступит прокурору, он может потребовать от Роскомнадзора провести инспекционный визит или внеплановую выездную проверку, о которой компания узнает лишь за 24 часа. А такая проверка рискует материализоваться в предписания и административные протоколы...

- Более того, буквально в конце прошлой и на этой неделе уже сразу несколько компаний получили уведомления о проведении внеплановых документарных проверок, потому что ранее была информация об утечках ПД в таких компаниях.

Как предотвратить риски для бизнеса?

Таким образом, несмотря на мораторий, у Роскомнадзора есть возможности по назначению проверок компаний и реализации иных форм контроля. Более того, «заработать» два предупреждения на самом деле проще, чем кажется. Например, просроченные ответы на запрос субъекту (напоминаем, что срок был обновлен – на ответ есть всего 10 рабочих дней) или необновление или неполное обновление информации в реестре операторов Роскомнадзора. Готовы спорить – это применимо к большинству компаний!

Внеплановый контроль могут «триггерить» такие события:

внеплановый контроль и наблюдение	обращения третьих лиц, СМИ, Интернет	требование прокурора, поручение Президента и Правительства	истечение срока для устранения нарушений	сведения об угрозе (неотложные меры)
дистанционное наблюдение	✓	✗	✗	✗
внеплановая документарная проверка	✗	✓	✓	✓
внеплановая выездная проверка	✗	✓	✓	✓
внеплановый инспекционный визит	✗	✓	✓	✓

Для митигации рисков необходимо поддерживать front-end гигиену и безопасность IT-систем.

Чтобы исключить такие события, необходимо обратить внимание на их ключевые триггеры — жалобы субъектов и privacy-экстремистов, а также сведения об утечках или иных нарушениях в СМИ. Соответственно, критично важно соблюдать front-end гигиену всех возможных точек контактов, до которых может дотянуться субъект или Роскомнадзор, а также обеспечивать кибербез IT-систем.

P.S. Подробнее о топ-privacy уязвимостях для бизнеса читайте в предыдущем выпуске Comply.Pulse #4.

#BetterCallComply

Артем Дмитриев
Управляющий партнер
Privacy, Tech & IP

artem.dmitriev@comply.ru
+7 (961) 806-2776