Comply.Pulse |#3| июль 2022 г.

Полтора месяца на комплаенс с новым 152-ФЗ – время пошло!

Совет Федерации одобрил законопроект об изменениях в Закон "О персональных данных" (152-ФЗ). Кратко о наиболее очевидных нововведениях обновленного 152-ФЗ с нашими комментариями:

- До 10 рабочих дней сокращены **сроки реагирования** оператора на запросы субъектов и регуляторов. Прежде отвечать можно было месяц.

  “ Чтобы уложиться в столь сжатые сроки, придется проверить и «прокачать» процедуру реагирования на обращения субъектов (DSR). Отсутствие в компании отработанных DSR-процедур является сегодня одной из ключевых privacy-уязвимостей – наиболее очевидный вектор атаки на компанию для privacy-экстремистов или конкурента.

- Больше требований к содержанию локальных актов компании, в частности, к **реестру процессов** (RoPA). Так, **для каждой цели** обработки ПД необходимо указать в т.ч. категории ПД и субъектов, способы и сроки их обработки, порядок уничтожения таких ПД.

  “ Хотя раньше такого требования не было, а в ходе проверок Роскомнадзор требовал только упрощенную версию такого реестра, ведение RoPAявлялось хорошей практикой. Если такого документа нет, то стоит начать его готовить уже сегодня, так как сбор информации о процессах, как правило, задача крайне трудоемкая.

- Аналогичные требования теперь применимы и к **уведомлению Роскомнадзора** об обработке ПД. Для каждой цели обработки нужно будет указать категории ПД и субъектов, правовое основание, перечень действий и способы обработки.

  “ Прежде можно было подавать эту информацию единым списком без дробления на цели. Теперь будет сложнее подготовить правильное уведомление, нагрузка возрастет. К тому же абсолютно всем операторам потребуется обновить ранее поданные сведения.

- Необходимо уведомлять Роскомнадзор в случае **утечки ПД**. За 24 часа необходимо сообщить об инциденте, за 72 – о результатах внутреннего расследования.

  “ Это новый для России процесс, который необходимо внедрить в компании. Особенно актуально с учетом существующей «презумпции виновности» оператора за любую утечку ПД. Для проверки поможет bugBounty@Comply– об этом сервисе скоро расскажем в нашем дайджесте.

- Новые требования к **содержанию договора поручения** на обработку ПД. Потребуется включить перечень ПД, обязанности защиты ПД и прав субъектов, подтверждение privacy-комплаенса обработчиком, его обязанности по уведомлению оператора и содействия оператору.

  “ Это и так было хорошей практикой. Но рекомендуем проверить ваши договоры

и, если необходимо, заключить дополнительные соглашения, чтобы дополнить договоры выпадающими условиями.

- Появились дополнительные требования **к согласию** на обработку ПД. Оно должно быть предметным и однозначным. Кроме этого, в договоре, на основании которого обрабатываются ПД, нельзя ограничить права и свободы субъекта, а сам договор нельзя заключить на основе бездействия субъекта.

  “ Непонятно, что означают эти новые требования – разве раньше было не так? Остается ждать развития правоприменительной практики и, конечно, надеяться, что не вы станете ее участником…

- Если предоставление субъектом ПД или согласия на их обработку обязательно в силу федерального закона, то оператор обязан **разъяснить субъекту последствия отказа**.

  “ Это новая обязанность, поэтому надо предусмотреть такое информирование в соответствующих формах. Но что делать при отказе – остается не понятным как и прежде. Можно ли не заключать договор или ограничить субъекта в возможностях? Остается следить за развитием практики , в частности – на базе дела Аэрофлот vs. Роскомнадзор.

- Экстерриториальная применимость требований 152-ФЗ к **иностранным компаниям**, которые самостоятельно обрабатывают ПД российских граждан на основании согласий или договоров. Кроме этого, иностранные обработчики теперь напрямую отвечают перед субъектами ПД.

  “ Вопрос в том, какие именно требования 152-ФЗ будут распространяться на зарубежные компании. Будут ли применимы специфические требования к обеспечению безопасности ПД? За какие нарушения будет отвечать иностранный обработчик – только за свои как обработчика или за «операторские» тоже? Критерии экстерриториальной применимости сформулированы… Хотя, проще сказать, что они не сформулированы.

- Операторам необходимо обеспечить **взаимодействие с ГосСОПКА**. Порядок взаимодействия должен быть определен регуляторами.

  “ Самое загадочное и, на наш взгляд, сложное с т.з. исполнения требование для бизнеса, особенно – малого и среднего. Подключение к ГосСОПКе – весьма нетривиальная задача даже для госкомпаний, поэтому абсолютно не ясно, как его выполнить, например, какому-нибудь региональному интернет-магазину.

Указанные требования вступят в силу **с 1 сентября 2022 года**. Таким образом, остается **всего 1,5 месяца** на проверку и доработку клиентских и локальных документов, а также адаптацию процессов. Как всегда важнее всего убедиться к этому моменту в front-end комплаенсе, о котором недавно рассказывали газете Коммерсантъ.

Ряд требований вступит в силу **с 1 марта 2023 года**.

- Наиболее драматичным является **предварительное уведомление**Роскомнадзора о **трансграничной передаче ПД**.

  “ Для этого оператор обязан предварительно оценить privacy-framework для такой передачи, в частности – юрисдикцию получателя ПД на предмет защиты прав субъектов. Роскомнадзор может запросить подтверждение того, что такая оценка выполнена. Будет действовать уведомительный порядок для передачи ПД в

адекватные юрисдикции, и разрешительный – для неадекватных (например, США, Индия, Китай и т.д.).

Важно, что механизмы и размер ответственности остались без изменений. То есть большинство требований не сопряжено с немедленной ответственностью бизнеса, и, например, штрафы возможны только по результатам неисполнения предписания Роскомнадзора. Это конечно же не отменяет риски для бизнеса из дефектов легитимности собираемых баз клиентских данных, риски из повышенного внимания регуляторов и privacy-экстремистов и т.д.

Вместе с тем Минцифры готовит законопроект о введении **оборотных штрафов**за утечку ПД, в отношении которого появилась инициатива снижения размера штрафов и даже исключения штрафов за первую утечку.

Исполнение новых требований предполагает издание ряда актов регуляторами, без которых новый 152-ФЗ вряд ли исполним. Будем следить за развитием событий и держать вас в курсе.

Как Вы считаете, какое влияние на бизнес окажут эти поправки?

Пройти опрос

Предлагаем **оценить законопроект** в нашем анонимном опросе по ссылке слева. Результаты опроса вместе обсудим на семинаре RPPA 25 июля.

Команда Comply.

Артем Дмитриев

Руководитель IP, Tech & Privacy
artem.dmitriev@comply.ru
+7 (961) 806-2776
t.me/artydmitriev

Сергей Сайганов

Руководитель Technology & Product
sergei.saiganov@comply.ru
+7 (916) 968-1554
t.me/saiganov