Comply.Pulse

ТОП PRIVACY-УЯЗВИМОСТЕЙ ДЛЯ БИЗНЕСА

В этом выпуске мы поделимся мнением о подходе к privacy-комплаенсу в новом контексте, а именно, расскажем о наиболее критичных, на наш взгляд, privacy-уязвимостях, которые влекут немедленные или материальные последствия для бизнеса.

Многое изменилось и, как ожидалось, privacy не будет на повестке. Как оказалось, в последнее время потребность в privacy-комплаенсе значительно возросла. Причиной тому стал комплекс факторов, включая следующие:

- Локализация ПО и ИТ, изменение цепочек поставок;
- Цифровизация рутинных процессов;
- Атаки privacy-экстремистов;
- Утечки и грядущие оборотные штрафы;
- Реформа Закона «О персональных данных».

Кроме того, у менеджмента большинства компаний фокус сместился на непрерывность бизнеса и сокращение расходов. А значит и privacy-комплаенс должен стать более ~~экономным~~ эффективным.

Что с уязвимостями?

Ограничимся несколькими вопросами для проверки. Отрицательный ответ на любой из этих вопросов означает актуальность риска.

Коллеги, системы и процессы готовы ответить на запрос клиента за 10 дней?

Сегодня, когда так активны privacy-экстремисты, крайне важно настроить DSR-процедуры. Между тем, согласно нашему опросу 70% компаний никогда не проверяли, насколько корректно они способны отработать запросы клиентов. Обычно в компаниях есть локальные акты, регламенты и прочие бумажные артефакты. Уже неплохо! Но нет работающего процесса и его контролей.

О чем важно не забыть при выстраивании работающего процесса?

1. Знать все каналы, по которым вы можете получить запрос.

• В случае с телефоном, важно понимать, по каким именно номерам телефона возможен звонок. И что ответят клиенту, кого предупредят о новом запросе. Также важно продумать процесс, ведь звонок может получить или колл-центр, или, например, ресепшн.

• Если у вас есть выделенная почта для вопросов о privacy, например, privacy@company.ru. Здорово! Но это вовсе не значит, что запрос будет направлен туда, а не на info@company.ru и т.д.

2. Клиенты могут направить целый ряд запросов. Для каждого из них – разные сроки и требования к исполнению. На некоторые ответить придется немедленно или за 7-10 дней.

3. Важно понимать, а можно ли (или нужно ли), прежде чем ответить клиенту на запрос, что-то запросить у него. Это частая ошибка. В большинстве случаев встречные запросы клиенту будут ошибкой, которая повлечет жалобу в Роскомнадзор, запрос последнего и нежелательное внимание. В последнее время Роскомнадзор уделяет пристальное внимание этим процедурам. Наконец, запросы субъекта – попросту самый доступный инструмент для privacy-экстремиста.

Итак, получить, не потерять, донести до DPO, понять, что и как отвечать – 10 дней. А еще за 10 дней надо успеть либо собрать данные, которые вы обрабатываете о клиенте, либо отозвать его согласие, отметить это в ИТ-системах, сопроводить бумагами или…что там будет написано в запросе. За 10 рабочих дней. Хотя прежде в крупных компаниях с трудом хватало даже месяца.

С учетом этого целесообразно заранее разработать черновики ответов, в том числе уведомления о продлении срока на ответ на запрос на дополнительные 5 дней.

У вас есть план действий, если произойдет утечка данных, не так ли?

Хочется верить, что данные никогда не утекут. Но рано или поздно, в том или ином объеме это может произойти с любой компанией. Поэтому необходимо иметь четкий план действий на этот случай. Особенно сейчас, когда утечек много, а общество и регуляторы проявляют к этой теме повышенное внимание.

И раньше было важно молниеносно реагировать на утечки. Мы представляли в этом году несколько известных компаний при общении с Роскомнадзором по результатам не менее известных утечек. Наш опыт показывает, что регулятор может счесть компанию виновной независимо от реальных обстоятельств. Поэтому только выверенные и проактивные действия после утечки смогут противостоять презумпции вашей виновности.

А с недавних пор градус вопроса значительно повысился, ведь в Закон «О персональных данных» добавили обязанность уведомить Роскомнадзор в случае утечки в течение 24 часов.

Поэтому теперь надо будет выявить инцидент и определить, например, имейл, направленный не тому клиенту, является утечкой или нет, и были ли при этом нарушены права другого клиента. Кто готовит такое уведомление, и кто его подписывает, кто указан в качестве контактного лица, что стало причиной утечки, как правильно принести извинения клиентам. Еще и с ГосСОПКой надо будет успеть провзаимодействовать.

Нет, это еще не все. Далее у вас будет еще 48 часов, чтобы провести расследование и сообщить о его результатах Роскомнадзору.

Обо всем этом лучше подумать заранее, ведь потом времени не будет. А проактивные и выверенные действия имеют ключевое значение и в спорах с регуляторами (особенно с учетом скорых оборотных штрафов), так и в последующих коллективных исках.

Вы проверяли privacy-by-design в ИТ-системах?

Конечно, вы и так знали, что при выборе и внедрении бизнес-систем (CRM, HRM, BPM и КЭДО) крайне важно проверить privacy-механизмы этих систем (т.е. «проектируемую приватность»). Но было ли это сделано? Спокойна ли privacy-совесть вашего DPO? Рано или поздно озадачиться этими вопросами неизбежно придется.

Например, CRM обязана уметь дедуплицировать клиентские карточки. И делать это правильно, то есть не оставляя дубликаты, но и не объединяя попутно разных клиентов. В противном случае будет непонятно, у какого клиента отозвать согласие, а какому можно направлять рекламу. Система должна контролировать действительность согласий и иных оснований для обработки и понимать связи между ними. Представим, что клиент в привязке к имейл и телефону дал одно согласие, а другое для – имейл и адреса регистрации. Когда истечет первое согласие, оставите ли вы его телефон или удалите все данные или не удалите никакие данные? Ваша CRM может счесть такие вопросы риторическими. Кстати, если эти вопросы закрываются ручными трудом, то клиентская база, скорее всего, уже напоминает минное поле. Это далеко не полный privacy-минимум для CRM.

Кстати, это же будет актуально и для кадрового электронного документооборота (КЭДО). В КЭДО содержится большой массив персональных данных (ПД) работников и отсутствует алгоритм контроля сроков и удаления протухших данных. Инспектор Роскомнадзора знает об этом, поэтому он обязательно заглянет в КЭДО при проверке.

А давно ли проверяли точки контактов со своими клиентами?

Как правило, в компаниях есть много лендингов или рекламных кампаний с обработкой ПД, о которых юристам или DPO случайно забыли рассказать. Лучше проверить. А еще лучше настроить процесс так, чтобы без вовлечения юристов/DPO их вовсе не появлялось.

С учетом недавних изменений Закона «О персональных данных» не лишним будет проверить согласия, размещенные на сайте и в приложениях, наличие политики об обработке ПД на каждой страничке, где есть сбор ПД, клиентские договоры – а не спряталось ли в них «случайно» согласие? Это очевидно и скучно. Но это отличный повод поэксплуатировать выявленные privacy-уязвимости вашему конкуренту или privacy-экстремисту или даже инспектору Роскомнадзора в рамках удаленного мониторинга. А так и до коллективных исков недалеко.

Рекомендации

Таким образом, именно сейчас крайне важно убедиться, что ваш «front-end» комплаенс на 5+. Все, до чего могут дотянуться внешние пользователи, конкуренты или инспектор Роскомнадзора, должно быть максимально выверенным, и именно в публичном периметре больше всего рисков. Если недостатки во внутренних процессах или документах возможно выявить только в ходе выездной проверки, количество которых год от года сокращается, здесь же – все на виду.

Комплаенс внешнего периметра компании позволяет исключить порядка 90% рисков в сфере privacy. Чтобы его проверить и обеспечить мы проводим privacy-пентест, т.е. тестируем внешний контур компании на предмет уязвимостей по всем возможным каналам коммуникации и векторам атаки. Результат – внешний контур безопасен! #BetterCallComply

Эти и многие другие вопросы в сфере privacy мы обсудили на деловом завтраке по privacy-уязвимостям, который провели совместно в Legal Insight. Материалы мероприятия доступны по ссылке.

Команда Comply.

Артем Дмитриев
Privacy, Tech & IP

artem.dmitriev@comply.ru
+7 (961) 806-2776
t.me/artydmitriev