За п’ять хвилин до набрання чинності GDPR

Регламент General Data Protection Regulation: нові правила гри у сфері персональних даних

Олег КЛИМЧУК,
радник Sayenko Kharenko

General Data Protection Regulation (GDPR) було прийнято 14.04.2016 р. і до 25.05.2018 р. всім було надано час для приведення процесів обробки персональних даних у відповідність із GDPR. З часу анонсування відповідність GDPR стала топ-темою не лише в ЄС. Однією з причин широкого резонансу стало те, що GDPR застосовується екстратериторіально. Іншими словами, якщо володілець персональних даних має присутність в ЄС (наприклад, афілійована юридична особа, при цьому не важливо, здійснюється обробка персональних даних у межах чи поза межами ЄС) або якщо пропонує товари чи послуги (навіть якщо безоплатно) суб’єктам персональних даних, які знаходяться в ЄС, або здійснює моніторинг їхньої діяльності (поведінки) в ЄС, то на такого володільця фактично поширюються вимоги GDPR. Іншою причиною резонансу стали значні штрафи, передбачені GDPR (наприклад, штраф у розмірі 4% від глобального обігу або до 20 млн євро, залежно від того, що є більшим).

В Україні це питання отримало достатній резонанс лише кілька місяців тому, коли одні компанії почали приводити у відповідність з GDPR процеси у своїх українських афілійованих структурах, другі зрозуміли, що GDPR – це не про штрафи, а про репутацію і перспективи роботи з європейськими партнерами, треті зробили висновок, що це питання лояльності та довіри європейських споживачів. Якщо перші, найімовірніше, встигнуть до 25 травня привести свою діяльність у відповідність з GDPR, оскільки їхні материнські структури протягом тривалого часу готувалися до цього, то всім іншим залишається «остання ніч перед захистом диплому». До набрання чинності Регламентом залишилося менше ніж місяць. На що звернути увагу і з чого почати, якщо рішення про необхідність відповідності GDPR прийнято «за 5 хвилин» до або вже після набуття чинності GDPR?

З практичної позиції, рекомендується розподілити пріоритети щодо відповідності GDPR на 3 групи: першочергові, процедурні та технічні.

Першочергові пріоритети

Насамперед, володілець персональних даних повинен провести інформаційний аудит. Аудит має включати перевірку того, які персональні дані збираються та обробляються, яким чином і якими засобами вони збираються та обробляються, а також ким (в межах організації та зовнішньо) і на підставі яких задокументованих процесів вони збираються та обробляються. Інформаційний аудит надасть розуміння обсягу персональних даних, що обробляються, процесів, пов’язаних з обробкою персональних даних, та дозволить структурувати дані. Без інформаційного аудиту буде майже неможливо визначити, на якій правовій підставі володілець обробляє персональні дані (вказані у ст. 6 GDPR), а також належним чином підготувати документи щодо обробки персональних даних та привести їх у відповідність із GDPR.

Документом, який потребує першочергової підготовки володільцем, є privacy notice. Privacy notice не має нормативних аналогів в українському законодавстві. Зазвичай під privacy notice розуміють або privacy policy, яку розміщують на онлайн ресурсах, або порядок обробки персональних даних, який затверджується на підприємстві. В термінології GDPR, privacy notice – це документ, який лаконічно описує всі аспекти обробки персональних даних та адресований безпосередньо суб’єктам персональних даних. Privacy policy – це внутрішній, більш детальний, документ, який описує процеси та порядок обробки персональних даних у межах компанії (наприклад, порядок поводження працівників володільця з персональними даними).

> ***Насамперед, володілець персональних даних повинен провести інформаційний аудит***

Вимоги до privacy notice передбачені у ст. 12-14 GDPR, вони є достатньо детальними. Насамперед, privacy notice має бути викладено в лаконічній та легкодоступній формі, без приховування аспектів обробки персональних даних, а також, що не менш важливо, простою (не юридичною) мовою (ч. 1 ст. 12 GDPR).

Щодо більш конкретних вимог, то privacy notice має містити інформацію про автоматизоване рішення (наприклад, профайлінг), а також про значущість та наслідки обробки у такий спосіб персональних даних для суб’єктів персональних даних. Окрім того, інформацію про те, що володілець персональних даних має намір передати персональні дані в країну, яка не входить до Європейського економічного простору (ЄЕП) або міжнародної організації. Стосовно країни, яка не входить до ЄЕП, володілець також має повідомити, чи прийнято щодо такої країни рішення про адекватність захисту персональних даних. Якщо країна є такою, що не забезпечує достатній захист персональних даних, у такому випадку privacy notice має містити інформацію про належні та достатні заходи щодо захисту персональних даних (ст. 46 GDPR), що вчинені володільцем, а також вказувати на засоби, за допомогою яких суб’єкт персональних даних може отримати документи, які обґрунтовують такі

заходи, або вказати, де такі документи є доступними.

До того ж ст. 35 GDPR встановлює вимогу щодо проведення оцінки впливу на захист персональних даних (Data protection impact assessment). Проведення оцінки впливу вимагається у тих випадках, коли вид обробки (наприклад, використання нових технологій обробки), природа, обсяг, контекст і ціль обробки, найімовірніше, може спричинити високі ризики для прав та свобод фізичних осіб. Оцінка впливу має проводитися до початку обробки персональних даних, а також повинна бути задокументована. Вимоги до оцінки передбачені у ч. 7 ст. 35 GDPR. Для володільців та всіх зацікавлених доступні рекомендації щодо проведення оцінки (Guidelines on Data Protection Impact Assessment).

Не менш важливим є забезпечення достатнього інформування (awareness) працівників про те, що в ЄС набирає чинності нове законодавство щодо захисту персональних даних, що воно може мати вплив на подальшу роботу з іноземними клієнтами, їхніми афілійованими компаніями в Україні; якщо вони отримують запити від клієнтів щодо персональних даних (наприклад, щодо підписання додаткових угод, наявності сертифікату ISO 27001), то вони повинні відповідально поставитися до таких запитів; кожен працівник, який безпосередньо працює з клієнтами, має розуміти важливість забезпечення відповідності GDPR для останніх.

Процедурні пріоритети

Передусім, до процедурних пріоритетів варто віднести внутрішню перевірку на предмет відповідності та приведення у відповідність внутрішнього порядку обробки персональних даних (privacy policy). Важливо, щоб порядок обробки розроблявся на виконання privacy notice – зобов'язання щодо обробки персональних даних, про яке володілець заявляє публічно (насамперед, суб'єктам персональних даних, але також перевіряючим органам, контрагентам, іншим зацікавленим особам).

Окрім того, важливо перевірити та забезпечити, щоб внутрішні політики, процедури й процеси володільця персональних даних гарантували можливість ефективної фактичної реалізації суб'єктами персональних даних своїх прав, які передбачені у ст. 15-21 GDPR (право на доступ до персональних даних, право на видалення та знищення персональних даних, право обмежити обробку персональних даних, право на переміщення персональних даних (right of portability), право на претензію).

Володілець також повинен визначити внутрішні процеси та процедури, за якими у разі потреби відбуватиметься перевірка необхідності проведення додаткової оцінки впливу на захист персональних даних (наприклад, у разі появи нових продуктів, додатків, сервісів, пов'язаних з персональними даними та їх обробкою).

Технічні пріоритети

Ст. 24 GDPR вимагає, щоб володілець персональних даних здійснив належні організаційні та технічні заходи щодо захисту персональних даних, аби забезпечити та бути спроможним продемонструвати, що обробка персональних даних відповідає GDPR. Належність організаційних і технічних заходів має визначатися виходячи з природи, обсягу, контексту та цілей обробки, рівня небезпеки для прав і свобод фізичних осіб.

Ст. 32 GDPR передбачає, що володілець, враховуючи вказані вище чинники, серед іншого, може здійснити такі технічні заходи:

- псевдонімізацію (визначення дається в GDPR) та шифрування персональних даних;
- безперервну конфіденційність, цілісність, доступність та стабільність систем обробки персональних даних.
- технічну здатність вчасно відновити доступність та доступ до персональних даних у разі виникнення інцидентів технічного або фізичного характеру;
- процес регулярного тестування й оцінки ефективності технічних та організаційних заходів для забезпечення безпеки обробки персональних даних.

Технічні заходи мають бути синхронізовані з privacy policy, а також у простій, доступній та лаконічній формі бути донесені до відома суб'єктів персональних даних у privacy notice.

Чи бути бізнесу з ЄС після 25 травня?

З хороших новин, якщо ви не GAFA-компанія (Google, Apple, Facebook, Amazon) і ваш бізнес корпоративно не присутній в ЄС, найімовірніше, 26 травня, тобто у перший день після набрання чинності GDPR, для українського володільця персональних даних нічого не зміниться. Очевидно, що володільці персональних даних з України матимуть додатковий час, для того щоб забезпечити відповідність GDPR. Однак навряд чи варто відкладати відповідність GDPR до першого втраченого контракту з європейським партнером через невідповідність бізнес-процесів вимогам GDPR чи наступного квартального звіту відділу продажів, який засвідчить падіння онлайн-продажів споживачам з ЄС (з тієї ж причини). Для тих, хто пропонує свої товари та послуги на ринку ЄС (або навіть їхнім афілійованим особам в Україні) та має справу з персональними даними осіб, що знаходяться в ЄС, бізнес-важливим є вчинення заходів із забезпечення «малої» євроінтеграції (в цьому випадку – забезпечення відповідності вимогам GDPR).

Аргумент. Позиція. Ідея

В Раді буде розглянуто новий законопроект щодо електронних доказів

17.04.2018 р. в Раді був зареєстрований Проект Закону про внесення змін до ст. 100 Цивільного процесуального кодексу України (щодо засвідчення копій електронних доказів) (реєстр. №8281). Згідно з текстом пояснювальної записки, законопроектом пропонується внести зміни до ст. 100 Цивільного процесуального кодексу, а саме замінити слова «посвідчених в порядку, передбачених законом» на «посвідченим в нотаріальному порядку».

Максим МИКИТАСЬ,
народний депутат,
ініціатор законопроекту

«Ваші докази суд може проігнорувати. Знаєте в якому випадку? Якщо це паперові копії електронних доказів. Адже ніхто не визначив, як вони повинні завірятися. Цивільний кодекс не дає відповіді на це питання. Згідно з ним завіряти підписом, як письмові докази, не можна, тому що копії електронних доказів кодекс такими не вважає. Однак у переліку випадків, в яких вимагається нотаріальне посвідчення, про копії електронних доказів ні слова.

Як же їх тоді завіряти? Виходить, що це питання сьогодні залишено виключно на розсуд судді. Таким чином, у висновку не просто виникає плутанина. Ваші докази можуть взагалі ігноруватися і не долучатися до справи. А суддя, навіть якщо зробить це навмисно, не понесе жодної відповідальності, адже немає прямої норми. Чи можна говорити в таких умовах про якусь справедливість процесу та змагальність сторін?

На мою думку, не можна. Тому я вніс у Раду законопроект, який залатає цю малопомітну, але дуже серйозну дірку в законодавстві. Рішення дуже просте – чітко встановити, що копії електронних доказів завіряються нотаріусом. Вже одним цим кроком ми помітно звузимо поле для здійснення помилки або навмисної маніпуляції з боку судді. А докази, які часто здатні переломити перебіг судового процесу, більше не будуть ігноруватися через те, що комусь невигідно приєднати їх до справи».