Життя після GDPR: вплив на українські компанії

Дар'я СТАДНИК,
юрист Pavlenko Legal Group

PAVLENKO LEGAL GROUP
Law & Government Relations

Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), який частіше називають за абревіатурою GDPR (від General Data Protection Regulation), звернув на себе увагу українців у травні минулого року. Природа цього Регламенту відрізняється відсутністю необхідності приймати національні закони для застосування заходів із захисту персональних даних, що встановлені GDPR. Це означає, що норми Регламенту застосовуються безпосередньо як норми національного законодавства та є імперативними для всіх осіб у межах Євросоюзу та Європейської економічної зони. Окрім того, положення GDPR мають бути дотримані у разі переміщення персональних даних за межі ЄС (наприклад, до України).

Як саме працює GDPR?

Захист персональних даних не є новелою. Майже кожна держава має власний закон, що регулює такі питання (наприклад, Закон України «Про захист персональних даних»). GDPR був прийнятий з метою уніфікації підходів до збору, обробки, зберігання та використання персональних даних європейської спільноти. Персональними даними вважається будь-яка інформація фізичних осіб (ім'я та прізвище, адреса, геолокація, номер телефону, банківські відомості, фінансовий стан, особисті повідомлення (соціальні мережі, електронна пошта), медична інформація, інші особисті дані, фотографії, відомості про орієнтацію, політичні погляди тощо). Будь-які такі дані можуть збиратися, оброблятися, зберігатися та використовуватися третіми особами лише у разі дотримання умов, передбачених GDPR.

На практиці до процесу захисту персональних даних за GDPR залучені сторони:

- суб'єкт даних (користувач), тобто власне фізична особа, чиї персональні дані обробляються;
- контролер даних, тобто організація чи компанія, яка визначає цілі та засоби обробки персональних даних;
- процесор даних, тобто організація чи компанія, яка обробляє персональні дані від імені контролера, при чому контролер та процесор можуть бути представлені однією організацією чи компанією.

Кожна залучена сторона має певний набір правил та вимог, встановлених GDPR, що конкретно описує процедури, які повинні виконуватися у випадках системних збоїв, порушень зберігання даних тощо. Слід зазначити, що GDPR запроваджує систему суворих штрафів за порушення вимог. Спосіб накладення штрафів розглядається окремо в кожному конкретному випадку та залежить від рівня порушення та розміру збитку, заподіяного порушенням. Загалом, штрафи можуть становити до 10-20 млн євро або 2% та 4% від глобального річного обігу компанії за попередній фінансовий рік, залежно від тяжкості випадку.

Для того щоб уникнути порушення правил обробки персональних даних та не отримати штраф, необхідно дотримуватися таких правил:

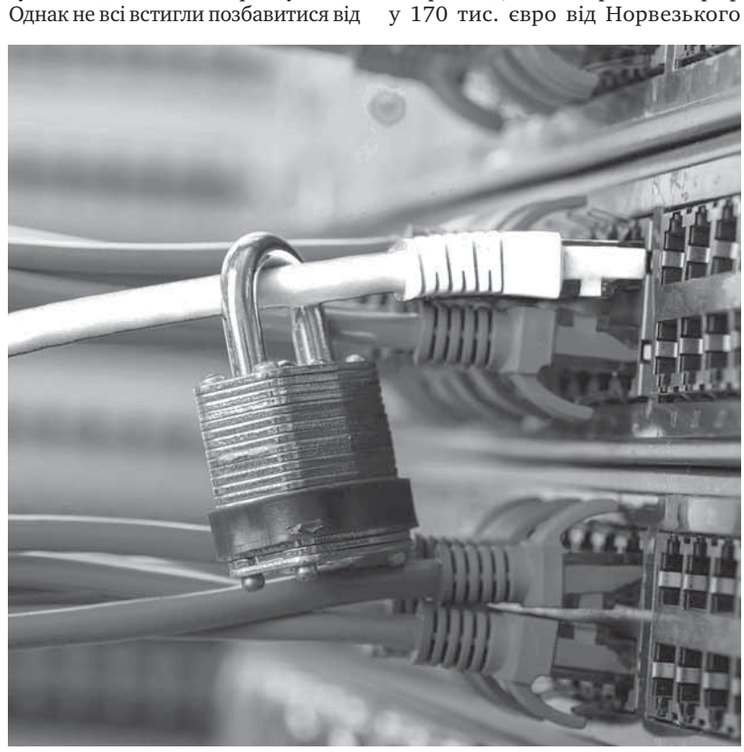
- здійснювати обробку персональних даних лише після отримання на це згоди відповідного суб'єкта даних, яка може бути скасована в будь-який час;
- мати змогу ретельно пояснити мету використання даних;
- надавати докази наявності згоди суб'єкта даних у матеріальному вигляді;
- здійснювати збір даних лише відповідно до наявної мети;
- встановлювати обмеження часу на зберігання даних на період, коли такі дані є необхідними;
- оновлювати дані (шляхом підтримання зв'язку із суб'єктами даних);
- дотримуватися принципу конфіденційності;
- зберігати історію обробки даних;
- забезпечувати надійне зберігання даних;
- інформувати відповідальну особу про порушення протягом 72 годин з моменту, коли про нього стало відомо;
- інформувати суб'єктів даних про порушення;
- впроваджувати технічні та організаційні заходи для забезпечення захисту прав суб'єктів даних;
- проводити регулярну оцінку ризику конфіденційності;
- призначити особу, відповідальну за питання захисту даних, для нагляду за діяльністю з обробки даних тощо.

Показові кейси

Більшість європейських компаній серйозно поставилися до впровадження правил GDPR та одразу ж почали вносити зміни в організацію своєї діяльності з обробки персональних даних. На багатьох підприємствах з'явилися посади контролерів обробки персональних даних у межах компанії, почалося масове отримання дозволів від суб'єктів даних на їх обробку тощо. Однак не всі встигли позбавитися від наявних порушень до моменту перевірок та їх виявлення, внаслідок чого ми маємо багато прикладів притягнення європейських компаній до відповідальності та накладення великих штрафів.

Наразі найбільш показовим є кейс щодо порушення правил обробки персональних даних компанією Google, яка отримала штраф на суму 50 млн євро. Користувачі системи Android, які налаштували свої телефони, не надавали при цьому чіткої згоди на обробку їхніх персональних даних для наступної персоналізації реклами. Регулятором (Національною комісією з інформатизації та свободи Франції) також було встановлено, що Google не надає споживачам чіткої та доступної інформації про те, як саме збираються та зберігаються їхні персональні дані. Зазначалося, що незважаючи на заходи, впроваджені компанією Google, виявлені порушення позбавляють користувачів важливих гарантій стосовно операцій з обробки даних, які можуть оприлюднити важливі аспекти їхнього приватного життя, оскільки вони базуються на величезній кількості даних, широкому спектрі послуг та майже необмежених можливих комбінаціях.

Також можна навести приклад з Муніципалітетом міста Берген (Норвегія), який отримав штраф у 170 тис. євро від Норвезького



агентства із захисту даних. Увагу привернула доповідь одного з учнів державної школи, що адмініструється Муніципалітетом, який знайшов файл з обліковими даними 35 тис. студентів та співробітників у публічному сховищі.

У березні вперше був накладений штраф за порушення GDPR польським регулятором. За неповідомлення більше ніж 6 млн осіб про обробку їхніх персональних даних на 220 тис. євро була оштрафована компанія Bisnode, що займається цифровим маркетингом. Причиною стало небажання компанії витрачати значні кошти на поштову розсилку повідомлень про обробку персональних даних, внаслідок чого було прийняте рішення повідомите лише тих осіб, чиї електронні адреси відомі компанії.

За невидалення телефонних номерів користувачів компанію Taxa 4x35 (Данія), що надає послуги таксі, було оштрафовано приблизно на 150 тис. євро. Загалом, сьогодні можна нарахувати більше ніж 200 тис. випадків притягнення до відповідальності за порушення GDPR, а сума накладених штрафів вже перевищує 56 млн євро.

Наразі під загрозою перебуває компанія Facebook, яка може отримати штраф за порушення GDPR на суму близько 2 млрд євро. Комісія з захисту даних була повідомлена Facebook про те, що сотні мільйонів паролів користувачів, які користуються Facebook, Facebook Lite та Instagram, зберігаються Facebook у форматі відкритого тексту на внутрішніх серверах. Наразі проводяться розслідування Facebook та його дочірніх компаній з метою встановлення обставин справи.

Вплив на українські компанії

Слід звернути увагу, що до українських компаній GDPR застосовується в тому випадку, якщо вони здійснюють збір, обробку, зберігання чи використання персональних даних суб'єкта з Євросоюзу. Наприклад, якщо українська компанія має власний інтернет-магазин, для здійснення покупки в якому необхідно пройти реєстрацію на веб-сайті, а також заповнити відомості про доставку та оплату, чи має вона дотримуватися GDPR, якщо хоча б одним покупцем буде громадянин ЄС?

За умови, що сайт викладено не лише українською, але й англійською/німецькою/французькою та іншими мовами; та/або оплату на веб-сайті можна проводити не лише у гривнях, але й у доларах/євро/фунтах тощо; та/або домен сайту зареєстровано на території ЄС; та/або інтернет-магазин пропонує доставку товару на територію ЄС тощо, існує велика ймовірність того, що українська компанія, яка є власником такого сайту, повинна буде дотримуватися GDPR та нести відповідальність за його порушення.

Однак якщо зареєстрована в Україні компанія, яка здійснює свою діяльність через український веб-сайт, доставляє товар лише на території України та приймає оплату лише у гривнях, здійснить продаж свого товару громадянину ЄС (навіть із залученням його персональних даних), GDPR до неї не застосовуватиметься.

Українське законодавство не можна назвати бідним на норми, що регулюють питання обробки персональних даних. Зокрема, Законом України «Про захист персональних даних» передбачаються основні принципи, які закріплені в GDPR. Однак чимало норм Регламенту не знаходять свого відображення в українських законах. З метою наближення до європейських норм та правил доцільним є запровадження в Україні серйозного ставлення до персональних даних українських громадян та іноземців.

Кожній українській компанії, незалежно від перспектив розповсюдження на неї умов GDPR, необхідно провести аудит та систематизувати наявні дані, належним чином вести їх облік, отримувати згоду на їх обробку від суб'єктів таких даних, зберігати конфіденційність. Не тільки кадрові працівники мають бути обізнані з правилами поводження з особистою інформацією, але й весь персонал кожного підприємства. Це дозволить уникнути будь-яких непорозумінь та неприємних ситуацій, а також штрафів.

* * *

Отже, проаналізувавши європейський досвід, який склався за рік активного використання правил GDPR, можна зробити висновок, що громадяни ЄС отримали значно більший захист від неправомірної обробки їхніх персональних даних. З моменту набрання чинності Регламентом він набув більш чіткого значення та став зрозумілішим. Завдяки практиці, що склалася, випущеним до Регламенту пояснювальним документам, сфера застосування, межі відповідальності та правила GDPR стали більш реальними та окресленими. Поглянувши на приклади, які виникали в минулому році, можна здійснити аналіз ситуації та приблизно зрозуміти, що необхідно бізнесу сьогодні, щоб уникнути відповідальності за GDPR завтра.

Українським компаніям також необхідно переглянути свою діяльність на предмет наявності умов, через які вони мають дотримуватися GDPR, незважаючи на адресу своєї реєстрації. Окрім того, незалежно від європейського законодавства й практики, Україна має свої закони, а її громадяни — права та гарантії, які мають охоронятися і захищатися. Таким чином, жодній українській компанії не завадить провести аудит на предмет процедури збору, використання та зберігання персональних даних, а також у разі потреби — переглянути власні правила. ЮГ

Про що говорили на INTA 2019

Продовження. Початок на стор. 11

Тетяна ХАРЕБАВА,
адвокат, керівник юридичного департаменту SPORT LABS GROUP

Це була моя третя щорічна зустріч INTA, яку відвідало 11 000+ учасників з понад 100 країн світу. Попри вражаючі масштаби конференції, цього року я піймала себе на думці, що на «інту» прилітаю вже як додому: чимало знайомих облич та вже рідних серцю «інтівських» фішок, починаючи від локацій у величезних, схожих на аеропорти, конвеншн-центрах до веселих стрічок-наліпок «Ask me about Saul», «IP superhero» на фірмовому бейджі, який нізащо не можна знімати з себе чи губити, однак зручно використовувати як сумочку для візитівок.

Хочу відзначити цьогорічні тенденції INTA. По-перше, ще більше нетворкінгу, особливо інтерактивного. Для цього у фірмовому додатку INTA було навіть додано модуль з грою, бали в якій можна було отримати, відсканувавши QR-коди на бейджах інших учасників, відвідавши booth-стенди у виставковому залі, вказавши розгорнуту інформацію про себе тощо (переміг один з патентних повірених з Індії). Схожі ігрові знайомства були влаштовані на тематичних ресепшнах. Наприклад, на вечірці для інхаузів нам видали стар-мер, куди потрібно було вклеювати «зірочки», дізнавшись більше про компанії колег.

По-друге, дослідження судової практики в різних країнах (case study). Цього разу була організована панель під назвою Міжнародний IP-суд, куди увійшли IP-судді з ключових світових юрисдикцій (США, Канада, Китай, Німеччина, Японія, Бразилія тощо). Багато уваги судді-учасники панелі приділили поняттю bad faith (недобросовісність) власника ТМ при розгляді справ про скасування реєстрації торговельної марки.

По-третє, технології та IP. Чимало цікавих сесій було присвячено сфері ІСТ. Це не дивно, адже дуже активними учасниками INTA є великі технологічні компанії: Amazon, Facebook, Google, Microsoft та ін., представники яких ділилися своїм досвідом. Серед топіків, які збирали зацікавлену авдиторію, можна виділити: 4D-принтинг та IP-аспекти, вплив GDPR на розкриття даних власників доменів-порушників, технології для ефективного IP-портфоліо, штучний інтелект, який захищає від контрафакту онлайн, тощо.

Щорічна зустріч INTA — це подія must-have to visit для кожного IP-спеціаліста, для якого IP-практика — це не лише робота, але й задоволення від можливості отримувати нові знання, обмінюватися досвідом та здобувати нових друзів-однодумців з усього світу.

Продовження на стор. 19