ВІДПОВІДАЛЬНІСТЬ І САНКЦІЇ ЗА ПОРУШЕННЯ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ (GDPR)

ШЕВЧУК Олександр Олександрович - кандидат юридичних наук, асистент кафедри міжнародного права Навчально-наукового інституту міжнародних відносин Київського національного університету імені Тараса Шевченка
ORCID: https://orcid.org/0009-0009-7697-2950
СКОПІНЦЕВ Віктор Юрійович - радник з юридичних питань, «GSC Game World» Ltd.
ORCID: https://orcid.org/0009-0005-7310-7209
УДК 341.171
DOI: https://doi.org/10.32782/ep.2024.3.24

У XXI столітті у зв'язку зі швидким розвитком інформаційних технологій, постійним зростання масштабів передачі та обробки особистої інформації, захист персональних даних та право на приватність набувають особливо важливого значення. Транскордонна передача й обробка даних внесли помітні переваги в повсякденне життя: пошукові системи полегшують доступ до значних обсягів інформації, послуги соціальних мереж дозволяють людям у всьому світі спілкуватися, висловлювати свої думки та мобілізувати підтримку із соціальних, екологічних та політичних питань, а компанії та споживачі отримують вигоду від ефективних методів маркетингу в таких секторах, як страхування, охорона здоров'я тощо. Проте, швидкий розвиток інформаційних технологій упродовж останніх двох десятиліть приніс із собою і нові виклики для захисту персональних даних. Так, кожна особа повинна мати у своєму розпорядженні механізми для захисту своєї приватної інформації. Для того щоб надати можливість особі контролювати її інформацію та захистити від зловживань, дуже важливо, щоб закони про захист даних на інституційному рівні регулювали діяльність приватних та державних компаній, що стосується безпеки захисту персональних даних при їх передачі та обробці.

Інтернет спростив доступ до інформації, відвідавши веб-сайт або придбавши товари та послуги на сайті, організації збирають величезну кількість даних про осіб. Компанії збирають інформацію про ім'я та адресу, щоб відстежувати поведінку веб-переглядача, місце розташування та іншу інформацію, яка дає можливість компаніям ідентифікувати особу. Такі дані потім використовуються компаніями в різноманітних цілях, від продажу та управління відносинами з клієнтами до маркетингу. Доступність збору даних означає, що тисячі компаній не тільки збирають особисті дані, але і зберігають їх у небезпечних місцях, обмінюючись ними з третіми сторонами або переміщаючи ці дані через кордони для підтримки їх бізнесу. Крім того, їхні бізнес-моделі покладаються на продаж доступу до цих даних рекламодавцям. Кожного разу, користуючись послугою, купуючи продукт онлайн, реєструється за електронною поштою, звертаючись до лікаря, сплачуючи податки особі доведеться передати особисту інформацію з метою її обробки. Єдиним способом, яким громадяни та споживачі можуть забезпечити довіру як до уряду, так і до бізнесу, є застосування надійних механізмів захисту персональних даних, а також належний інституційний рівень захисту, який допомагає забезпечити ефективний моніторинг з боку наглядових органів за дотримання правил безпеки персональних даних і гарантувати право на захист у разі порушення безпеки даних.

Ключові слова: Європейський Союз, захист персональних даних, порушення безпеки персональних даних, відповідальність, санкції, Директива 95/46/ЄС, Регламент (ЄС) 2016/679.

Постановка проблеми

Ключовою новелою Регламенту (ЄС) 2016/679 є можливість накладання на організацію грошового стягнення в розмірі до чотирьох відсотків її річного світового обороту (або до 20 000 000 євро, якщо ця сума є більшою), або до двох відсотків її річного світового обороту (або до 10 000 000 євро, якщо ця сума є більшою). При вирішенні питання про накладання грошового стягнення і його розмір наглядовий орган з захисту персональних даних має враховувати такі обставини, як характер, тяжкість і тривалість порушення і його наслідків, заходи, вжиті для забезпечення виконання вимог Регламенту (ЄС) 2016/679, та будь-які заходи, спрямовані на запобігання спричинення порушенням негативних наслідків або на пом'якшення їхнього впливу.

При розробці проєкту Регламенту (ЄС) 2016/679 рівень штрафів за порушення безпеки персональних даних став предметом палких дискусій. У той час, як Європейська Комісія пропонувала штрафи в розмірі до 1 мільйона євро або 2% річного світового обороту компанії, Європейський Парламент вимагав збільшення штрафів до 100 мільйонів або 5% річного світового обороту компанії. З огляду на те, що компромісним рішенням стало встановлення максимального рівня штрафу в розмірі 20 мільйонів євро або 4%.

Аналіз останніх досліджень і публікацій

Теоретичною основою для цієї статті є наукові розробки вітчизняних та зарубіжних учених. Зпоміж робіт вітчизняних науковців, які досліджували особливості правового регулювання захисту персональних даних у Європейському Союзі слід виділити праці таких учених: Л. Олексюк, Ю. Деркаченко, В. Брижко, В. Пилипчук, О. Баранов, К. Мельник, В. Венгер, І. Городиський та М. Бем.

Серед зарубіжних учених, які акцентують свою увагу на питаннях захисту персональних даних слід, згадати таких дослідників, як: С. Уорен, Л. Брендіс, Т. Хікман, Д. Габель, А. Маєрс, Д. Футтер, Р. Хеймес та інші.

Проте, існуючий науковий доробок свідчить про необхідність продовження вивчення, комплексного аналізу і дослідження відповідальності та санкцій за порушення безпеки персональних даних відповідно до Регламенту (ЄС) 2016/679.

Метою цієї статті є аналіз механізмів притягнення до відповідальності і накладання санкцій за порушення безпеки персональних даних відповідно до Регламенту (ЄС) 2016/679.

Методологічна основа дослідження базується переважно на загальнонаукових і спеціально-юридичних методах, підходах, принципах дослідження. Зокрема, використано діалектичний, феноменологічний, аксіологічний, порівняльно-правовий, формально-логічний, формально-юридичний, модельний, прогностичний та інші методи.

У результаті сформовано низку наукових положень

Положення Регламенту (ЄС) 2016/679 з накладання санкцій за порушення безпеки персональних даних замінюють фрагментарну систему заходів примусу, передбачену Директивою 95/46/ЄС, одночасно запроваджуючи механізми невідворотності й послідовності призначення покарання, відсутні в Директиві 95/46/ЄС. Суттєві штрафи за порушення не лише стимулюють невідворотність покарання, вони є помітною особливістю Регламенту (ЄС) 2016/679, яка змусить національні й транснаціональні компанії інвестувати більше ресурсів у системи і механізми безпеки для забезпечення виконання вимог Регламенту (ЄС) 2016/679.

Виклад основного матеріалу

Нові розміри штрафів є, мабуть, однією з найважливіших новел Регламенту (ЄС) 2016/679, яка може змусити організації докорінно переглянути свої погляди на питання відповідності вимогам законодавства ЄС із захисту персональних даних та відчути ризик понести реальну відповідальність за порушення положень Регламенту (ЄС) 2016/679.

Регламент (ЄС) 2016/679 надає наглядовому органу повноваження з визначення розміру штрафних санкцій, які мають бути «ефективними, пропорційними й стримувальними». Регламент (ЄС) 2016/679 формулює також обтяжувальні й пом'якшувальні обставини, які наглядовий орган має враховувати, визначаючи розмір штрафу. Наприклад, умисні порушення є тяжчими за допущені з халатності. Пом'якшувальними обставинами є дотримання кодексу поведінки або стандартів механізму сертифікації і впровадження належних технічних і організаційних заходів захисту персональних даних. У випадку порушення вимог контролер та процесор вправі зменшити розмір штрафу, пом'якшивши «шкідливий характер, тяжкість і тривалість порушення» шляхом оперативного інформування про нього та співпраці з наглядовим органом.

При вирішенні питання про накладання грошового стягнення і його розмір наглядовий орган із захисту персональних даних має враховувати такі обставини, як характер, тяжкість і тривалість порушення і його наслідків, заходи, вжиті для забезпечення виконання вимог Регламенту (ЄС) 2016/679 та будь-які заходи, спрямовані на запобігання спричинення порушенням негативних наслідків або на пом'якшення їхнього впливу.

Регламент (ЄС) 2016/679 встановлює два рівні максимальних штрафних санкцій в залежності від наявності в контролера і процесора історії порушень і характеру самого порушення. Верхньою межею розміру штрафу є чотири відсотки річного світового обороту компанії або 20 мільйонів євро. Нижньою межею розміру штрафу є два відсотки річного світового обороту компанії або 10 мільйонів євро.

Штрафні санкції верхньої межі накладаються за більш суттєві порушення контролера і процесора, як-от порушення прав суб'єктів даних.

Зокрема, штрафні санкції верхньої межі накладаються за порушення наступних положень Регламенту (ЄС) 2016/679 [1]:

(a) основні принципи обробки, у тому числі умови надання згоди, відповідно до статей 5, 6, 7 і 9;

(b) права суб'єктів даних відповідно до статей 12-22;

(c) акти передавання персональних даних до одержувача в третій країні чи до міжнародної організації відповідно до статей 44-49;

(d) будь-які обов'язки відповідно до закону держави-члена, ухваленого згідно з главою IX;

(e) невідповідність постанові або тимчасовому чи остаточному обмеженню на опрацювання чи призупинення потоків даних наглядового органу відповідно до статті 58(2) або ненадання доступу як порушення статті 58(1).

Штрафні санкції нижньої межі накладаються за порушення наступних положень Регламенту (ЄС) 2016/679 [1]:

(a) обов'язки контролера і оператора відповідно до статей 8, 11, 25-39, і 42, і 43;

(b) обов'язки органу з сертифікації відповідно до статей 42 і 43;

(c) обов'язки органу з моніторингу відповідно до статті 41(4).

Тім Хікман [2] зазначає, що нові максимальні штрафи у розмірі 20 мільйонів євро або чотири відсотки річного світового обороту компанії, мабуть, найважливіша зміна, закріплена в Регламенті (ЄС) 2016/679, та, ймовірно, призведе до того, що компанії почнуть розглядають питання своєї відповідності законодавству ЄС щодо захисту персональних даних принципово іншим чином.

Анніка Спонзелее [3] стверджує, що нові штрафи можуть нанести значні фінансові збитки компанії, і навіть призвести до закриття бізнесу. Тому важливо, щоб компанії повністю були готові виконати всі зобов'язання, встановлені Регламентом (ЄС) 2016/679.

Анна Маєрс підкреслює [4], що штрафні санкції сприятимуть підвищенню відповідальності контролера і процесора дотримуватись положень Регламенту (ЄС) 2016/679, завдяки чому компанії інвестуватимуть більше коштів у системи безпеки персональних даних та розробку алгоритмів пошуку, виявлення та мінімізації витоку інформації.

Коли ж ми говоримо про відповідальність та санкції, важливо звернути увагу на практичні випадки порушення безпеки

персональних даних після вступу в силу Регламенту (ЄС) 2016/679.

Як приклад пропонуємо розглянути випадок стосовно Інтернет платформи з продажу квитків Ticketmaster. Так, 23 червня 2018 року було оголошено, що Ticketmaster [5] зазнав пролому в системі безпеки, який, як повідомляється, містив особисту та платіжну інформацію (імена, адреси, номери телефонів, платіжні дані та дані реєстрації) 40 000 користувачів у Сполученому Королівстві.

Ticketmaster [6] стверджував, що порушення, ймовірно, вплинуло лише на клієнтів Британії, які придбали або намагалися придбати квитки з 1 лютого по 23 червня 2018 року.

Насправді, Ticketmaster [6] був попереджений про потенційну атаку набагато раніше. Fintech фірма Monzo виявила шахрайську активність за кількома картами клієнтів у квітні, які було використано для платежів в Ticketmaster, поділившись своїми висновками з ними 12 квітня 2018 року. Проте, Ticketmaster заявив, що не знайшов жодних доказів порушення системи безпеки за результатами проведення внутрішнього розслідування.

Відповідно до Регламенту 2016/679 компанії повинні інформувати клієнтів про порушення захисту персональних даних без зайвої затримки. Вони також повинні повідомити наглядовий орган протягом 72 годин. Невиконання цього може призвести до штрафу в розмірі до 10 мільйонів євро або 2% річного обороту компанії відповідно до положень Регламенту (ЄС) 2016/679.

У своєму листі до клієнтів Ticketmaster зазначив, що він на протязі 72 годин співпрацював з наглядовим органом для розслідування кібератаки.

Отже, можна зробити висновок, що, зважаючи на обстави цієї справи, зазначимо, що існує ряд можливих порушень, включаючи несанкціонований доступ, невиконання адекватних технічних заходів для захисту даних, відсутність достатньої внутрішньої політики та внутрішньої організації для забезпечення достатніх механізмів безпеки даних.

Наведемо ще приклад порушення системи безпеки персональних даних компанією після вступу в силу Регламенту (ЄС) 2016/679. Власне, менш ніж через місяць після набуття чинності Регламенту (ЄС) 2016/679, компанія Dixons Carphone [7] - багатонаціонапьна компанія, що займається роздрібним та сервісним обслуговуванням електротехніки та телекомунікацій, заявила, що вона зазнала серйозної атаки на дані клієнтів. Компанія Dixons Carphone [8] визнала величезний витік інформації, що включає 5,9 мільйонів платіжних карток та 1,2 мільйона записів персональних даних.

Порівняно з останнім штрафом, який компанія отримала за порушенням захисту даних у розмірі 400 тисяч фунтів стерлінгів внаслідок кібератаки у 2015 року, коли постраждали понад три мільйони клієнтів, штраф у розмірі до 4 % річних загальнорічного обороту компанії або на суму до 20 000 мільйонів євро виглядає значно суворішим, що тільки посилює позиції Регламенту (ЄС) 2016/679.

Прес-секретар голови наглядового органу з питань захисту персональних даних Великобританії [9] зазначив, що компанія «Dixons Carphone підтвердила, що інцидент вплинув на особисті дані 10 мільйонів записів, що значно перевищує початкові дані.

Він заявив: «Наше розслідування інциденту триває, і нам буде потрібно час для оцінки цієї нової інформації. Тим часом ми очікуємо, що компанія якнайшвидше попередить усіх тих, хто зазнає впливу від порушення у Великобританії, і вживатиме всіх необхідних заходів для зменшення потенційної шкоди споживачам».

Таким чином, зроблений аналіз надає підстави стверджувати, що порушення системи безпеки персональних даних у компанії Dixons Carphone відбувається вже не вперше за декілька років, що слугує підтвердженням факту неналежної організаційної структури і механізмів захисту на випадки проникнення і зламу системи захисту.

Важливо також і те, що служба запобігання шахрайству у Великобританії (CIFAS) [10] повідомила про збільшення останнім часом більш ніж на 50% кількості випадків, коли шахраї незаконно викрали рахунки фізичних осіб та використовували їх для власної вигоди. CIFAS зазначив, що приклади

шахрайства щодо захоплення об'єктів можуть бути, коли злочинці викрадають інформацію про особисті дані через хакерство комп'ютера, перехоплюючи дані з електронної пошти або через Інтернет.

«Шахрайське використання ідентифікаційних даних є найбільшою та найголовнішою загрозою шахрайства», - сказано в повідомленні CIFAS».

Кейт Беддінгтон-Браун [10], керівник відділу комунікацій CIFAS, зазначила, що організаціям потрібно буде ще більше боротися з шахрайством. Збільшення випадків шахрайства служить попередженням і викликом організаціям, - сказала вона. Останнім часом організації активно інвестували кошти на оновлення своїх механізмів безпеки, щоб забезпечити додаткові кроки для створення надійної системи захисту даних. Незважаючи на це, злочинність у цій сфері продовжувала зростати, що свідчить про те, що найближчим часом потрібно зробити набагато більше».

Керівник CIFAS Пітер Херст [10] зазначив, що компанії можуть зменшити витрати, які вони зазнають внаслідок шахрайства, шляхом інвестування в належні системи та підходи щодо запобігання шахрайству.

Висновок

Таким чином, можна стверджувати, що положення Регламенту (ЄС) 2016/679 з накладання санкцій за порушення безпеки персональних даних замінюють фрагментарну систему заходів примусу, передбачену Директивою 95/46/ЄС, одночасно запроваджуючи механізми невідворотності й послідовності призначення покарання, відсутні в Директиві 95/46/ЄС. Суттєві штрафи за порушення не лише стимулюють невідворотність покарання, вони є помітною особливістю Регламенту (ЄС) 2016/679, яка змусить національні й транснаціональні компанії інвестувати більше ресурсів у системи і механізми безпеки для забезпечення виконання вимог Регламенту (ЄС) 2016/679.

Література

1. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) URL: http://eur-lex.europa.eu/eli/reg/2016/679/oj

2. Dr. Detlev Gabel, Tim Hickman Chapter 16 – Remedies and Sanctions. URL: https://www.whitecase.com/publications/article/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection

3. Annika Sponselee and Nicole Vreeman GDPR Top Ten: #7 - Data Protection Authority enforcement methods. URL: https://www2.deloitte.com/nl/nl/pages/risk/articles/gdpr-top-ten-7-data-protection-authority-enforcement-methods.html

4. Anna Myers Top 10 operational impacts of the GDPR: Part 10 – Consequences for GDPR Violations. URL: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-10-consequences-for-grpr-violations/

5. Ticketmaster Data Breach Could Equal GDPR Fines in Millions. URL: https://www.ticketnews.com/2018/07/ticketmaster-data-breach-could-equal-gdpr-fines-in-millions/

6. Ticketmaster breach: 'We've complied fully with GDPR'. URL: https://www.decisionmarketing.co.uk/news/ticketmaster-breach-weve-complied-fully-with-gdpr

7. Dixons Carbon data breach could cost company 400m in GDPR fines. URL: https://www.verdict.co.uk/dixons-carphone-data-breach-gdpr-fines/

8. Dixons Carphone pummelled as hackers strike again. URL: https://www.decisionmarketing.co.uk/news/dixons-carphone-pummelled-as-hackers-strike-again

9. ICO statement in response to Dixons Carphone breach announcement. URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/ico-statement-in-response-to-dixons-carphone-breach-announcement/

10. Personal data theft behind 65% of all fraud cases, says UK Fraud Prevention Service. URL: https://www.out-law.com/en/articles/2013/january/personal-data-theft-behind-65-of-all-fraud-cases-says-uk-fraud-prevention-service/

SUMMARY

An important change from the Data Protection Directive is that the GDPR harmonizes data protection enforcement in the EU. In particular, the GDPR determines the level of fines that can be imposed for data protection infringements in all EU Member States. GDPR introduces two levels of fines: (1) up to €10 million or 2% of the undertaking's global annual turnover, whichever is higher, for certain infringements; and (2) up to €20 million or 4% of the undertaking's global annual turnover, whichever is higher, for more severe infringements.

The amount of fine that will be imposed will depend on various criteria, including the severity and duration of the violation, the intentional character of the violation, any mitigation measures, the categories of personal data affected, the degree of cooperation with the Data Protection Authority and previous violations by the same controller or processor.

These fines add real "teeth" to data protection enforcement in the EU.

Keywords: European Union, personal data protection, data breach, liability, sanctions, Ticketmaster, Dixons Carphone, Directive 95/46/EC, Regulation (EU) 2016/679.