Юридичні науки

УДК 341(4-672 ЄС)+(477)

Рогальська Надія Володимирівна

студентка

Національного юридичного університету імені Ярослава Мудрого

Науковий керівник:

Петришин О.О.

кандидат юридичних наук,

асистент кафедри права Європейського Союзу

Національний юридичний університет імені Ярослава Мудрого

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ЄС ВІДПОВІДНО ДО GDPR

Анотація. *У статті розглянуто основні зміни у сфері захисту та обробки персональних даних у зв'язку із впровадженням Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 (GDPR). Досліджено основні вимоги, щодо здійснення обробки даних та санкції за їх недотримання. Проаналізовано випадки порушення вимог Регламенту та притягнення до відповідальності.*

Ключові слова: *GDPR, персональні дані, суб'єкт даних, контролер, процесор, «чутливі» дані.*

Summary. *The article considers main changes in sphere of personal`s data protection and processing in connection with implementation of Reglament (EU) 2016/679 of the European Parliament and of the Council (GDPR). The main requirements concerning data processing and sanction for non-compliance were researched. The cases of the requirement`s violation of the Regulation and prosecution were analyzed.*

Key words: *GDPR, personal data, data subject, controller, processor, «sensitive» data.*

25 травня 2018 року набрав чинності РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (GENERAL DATA PROTECTION REGULATION, GDPR) (надалі – Регламент, GDPR).

Це спричинило суттєві зміни в процесі обробки персональних даних та загального підходу до поводження з ними.

В основі ідеї впровадження Регламенту лежить необхідність забезпечення належного рівня захисту персональних даних з причин їх легкої доступності в цифровому середовищі, розповсюдженням консолідованих баз-даних через використання електронної комерції, інтернет – банкінгу, тощо.

Регламент спрямовано на сприяння формуванню простору свободи, безпеки і правосуддя, економічного союзу, соціально-економічному прогресові, зміцненню та конвергенції економік у межах внутрішнього ринку, підтриманню добробуту фізичних осіб [1].

Територія поширення дії Регламенту

GDRP впроваджує однакові «правила гри» при обробці персональних даних на території країн-членів ЄС. Документ прийнято саме у формі регламенту, що означає те, що всі країни-члени повинні ратифікувати його у незмінному вигляді. Окрім цього, він гарантує права на належну обробку та захист персональних даних поза межами Союзу для його громадян, закріпивши екстериторіальну дію.

Загальні правила обробки даних за GDPR

Описуючи механізм оброки персональних даних, Регламент вводить низку нових термінів, серед яких ключовими є: суб'єкт даних, контролер та оператор (процесор) персональних даних.

Перш за все, з'ясуємо зміст цих понять.

Суб'єктом даних є та фізична особа, чиї персональні дані підлягають обробці.

Контролер означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних; якщо цілі та засоби такого опрацювання визначаються законодавством Союзу чи держави-члена, контролер або спеціальні критерії його призначення може бути передбачено законодавством Союзу чи держави-члена. Іншими словами – контролер це суб'єкт якому передаються персональні дані для визначених цілей.

Оператором є суб'єкт, що здійснює опрацювання даних, за доручення контролера, в тому випадку, якщо його не здійснює він сам [1].

Правила щодо обробки та захисту персональних даних, встановлені Регламентом, передбачають низку вимог, насамперед до суб'єктів, що операційно її здійснюють – до контролера та процесора.

Яких же засобів необхідно вжити контролеру персональних даних для того, щоб вони відповідали вимогам Регламенту?

1. Слід провести аналіз даних, які надходять до контролера, зокрема слід визначити: обсяг інформації та джерела надходження даних.

Така необхідність обумовлена тим, що Регламентом заборонено збирати інформації більше, ніж це потрібно для досягнення мети такого збирання.

2. Здійснити низку організаційних заходів для забезпечення належного захисту.

Слід визначити, коло тих працівників контролера, хто має доступ до даних. Таким особам потрібно довести до відома умови поводження з даними, і як правило, укласти з ними Угоду про нерозголошення даних (NDA).

3. Співробітник з питань захисту даних (Personal data officer).

Регламентом передбачено вичерпний перелік умов, за яких обов'язкового має бути призначено співробітника з питань захисту даних. Такими умовами є:

1) якщо контролер є органом держаної влади - публічний орган або установа, за винятком судів, що діють як судові інстанції;

2) якщо контролер в силу специфіки своєї діяльності здійснює регулярний, систематичний і широкомасштабний моніторинг суб'єктів даних;

3) якщо контролер здійснює обробку «чутливих» даних (інформація про стан здоров'я особи, судимість, тощо).

Співробітник із захисту даних повинен інформувати та надавати рекомендації контролеру або оператору і працівникам, які здійснюють опрацювання, щодо їхніх обов'язків, на запит, надавати рекомендації щодо оцінювання впливу на захист даних і здійснювати моніторинг його проведення, тощо.

Такий співробітник може як бути обраний із числа працівників контролера, так і залучений на умовах цивільно-правового договору.

4. Гарантування технічної безпеки схоронності даних.

Забезпечння належного рівня захисту серверів зберігання даних, способів доступу до даних, впровадження належної системи верифікації при здійсненні доступу, тощо.

Як ми зазначали раніше, безпосередню обробку даних може здійснювати не лише сам контролер, але і оператор даних. Така ситуація може виникнути, наприклад, якщо контролер для надання послуг суб'єкту даних контролер залучає інших осіб, які при наданні послуг використовують дані суб'єкта і таким чином стають операторами.

Обов'язковою вимогою, що ставиться до оператора є забезпечення не нижчого рівня захисту персональних даних, ніж обумовлений та гарантується контролером по відношенню до відповідного суб'єкта.

Таким чином, для здійснення обробки персональних даних без порушень вимог Регламенту суб'єктам здійснення такої обробки необхідно вжити багатьох організаційних заходів.

Однак, навіть дотримання всіх вищезазначених умов, не є визначальними для законності обробки даних суб'єкта, адже головною умовою є отримання згоди самого суб'єкта на таку обробку.

У цьому аспекті Регламент також передбачив низку новел, встановивши вимоги до такої згоди.

Відтак, згода суб'єкта даних повинна бути прямою та активною (не підтвердження згоди, а саме її надання) у кожному конкретному випадку.

Надання згоди здійснюється у формі погодження з повідомленням про обробку персональних даних (Privacy Notice). Таке повідомлення необхідно надавати у письмовій формі або іншими засобами, в тому числі, за необхідності, електронними засобами. У разі надання запиту суб'єктом даних, інформацію може бути надано усно, за умови, що особу суб'єкта даних доведено іншими засобами.

Саме повідомлення має бути максимально простим у формулюваннях, доступним та зрозумілим.

Водночас попри те, що в загальній системі захисту даних передбачається, що обробка персональних даних залежить від згоди суб'єкта персональних даних, згода не може використовуватися в тій же мірі, що і правова підстава для обробки даних у діяльності судових органів влади. Відповідно до принципу законності, обробка таких даних повинні здійснюватися на підставі правового акту і відповідно до законних підстав, викладених у цьому акті. Така обробка повинна здійснюватися виключно у зв'язку з виконанням конкретних завдань, передбачених законом [3, с. 4].

Санкції за порушення Регламенту

Дотримання Регламенту забезпечується можливістю накладення штрафів у значних розмірах на порушників його вимог. Водночас

Регламентом встановлено, що в кожному конкретному випадку накладення санкцій повинно бути дієвим, пропорційним і стримувальним. Наведені також і критерії, що впливатимуть на вирішення питання про накладення штрафу та визначення його розміру, зокрема, до таких віднесено - специфіку, ступінь тяжкості і тривалість порушення, обсяг чи ціль відповідного опрацювання, а також кількість суб'єктів даних, які зазнали впливу, навмисний або недбалий характер порушення, будь-які дії, вжиті контролером або оператором для зниження рівня шкоди, заподіяної суб'єктами даних, категорії персональних даних, на які вплинуло порушення, тощо.

Розміри штрафів можуть стягуватися або у чітко встановленому розмірі, наприклад, за порушення контролером і оператором, обов'язків визначених Регламентом можу бути накладено штраф у розмірі до 20 000 000 євро, або у відсотковому відношенні від доходу - якщо це підприємство - до 4% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою [1].

Як свідчить аналіз, впровадження нового порядку захисту персональних даних потребує кардинальних змін ментальності, законодавчого регулювання та ділової практики не лише у країнах – членах ЄС, а й в інших державах, що є партнерами країн – членів Євросоюзу та у більшості з яких рівень захисту персональних даних не завжди відповідає правовим стандартам ЄС [2, с. 44].

Надалі розглянемо застосування Регламенту та перші наслідки порушення порядку поводження з персональними даними.

Австрія

Вже у вересні 2018 року регулятор у Австрії - Data Protection Authority – наклав штраф на підприємство за порушення вимог Регламенту. Суть порушення полягала в тому, що на фасаді приміщення була розташована відеокамера, яка окрім, входу до приміщення підприємства, охоплювала

також і значну частину тротуару. Камера не була належним чином позначена, а тому було порушено принцип прозорості збору даних. Не здійснювалась фіксація обробки даних та їх видалення. Порушення не мало б місця, якби перехожі знали про наявність відеокамери. Натоміть на порушника накладено штраф у розмірі 5,280,00 євро [4].

Португалія

Одним із перших порушників правил GDPR і стала Клініка в Португалії - Centro Hospitalar Barreiro Montijo. Контролюючий орган Португалії Comissão Nacional de Protecção de Dados встановив одразу три порушення Регламенту з боку лікувального закладу.

Перш за все, вказано на порушення статті 5 (1) (c) Регламенту , а саме, «Персональні дані необхідно: вважати достатніми і відповідними та обмежити їх мірою необхідності в них з огляду на цілі опрацювання («мінімізація даних»), дозволяючи надмірному числу персоналу Клініки мати доступ до персональних даних пацієнтів. Внаслідок цього, відповідно до статті 83(5)(a) Клініку оштрафували на 150 000,00 євро.

Другим стало порушення цілісності та конфіденційності даних внаслідок незастосування технічних та організаційних заходів для запобігання незаконному доступу до даних пацієнтів (стаття 5 (1)(f)), внаслідок чого сума штрафу склала ще 150 000,00 євро.

Підставою для накладення третього штрафу регулятором стало порушення статті 32(1)(b) – «…контролер і оператор повинні вжити необхідних технічних і організаційних заходів для забезпечення рівня безпеки відповідно до ризику, в тому числі, між іншим, у належних випадках здатність забезпечувати безперервну конфіденційність, цілісність, наявність та стійкість систем та послуг опрацювання».

Суть порушення цієї вимоги полягала у тому, що система зберігання та обробки даних, яка використовувалась Клініко не забезпечувала належного рівня захисту, внаслідок чого із 985 користувачів, що були зареєстровані як

лікарі, лікарями були лише 296 осіб, однак всі користувачі мали доступ до даних пацієнтів [5].

Загальна сума штрафу за порушення вимог Регламенту склала 400 000,00 євро, що є співрозмірним враховуючи характер інформації, щодо якої було здійснено порушення.

Франція

Французький регулятор - National Data Protection Commission (далі – Комісія) у січні 2019 року притягнув до відповідальності за порушення GDPR-вимог корпорацію Google.

До Комісії надійшли групові скарги від організацій None Of Your Business та La Quadrature du Net щодо порушень при обробці персональних даних. В обох скаргах зазначалося про те, що Google не має належних правових підстав здійснювати обробку персональних даних користувачів пошуковика, зокрема для здійснення персоналізованої реклами.

На початку розслідування факту порушень виникла проблема із визначенням основного місця розташування компанії. Це пов'язано з тим, що повинен бути один «головний учасник переговорів» з боку компанії, оскільки політика поводження з даними визначається центральним офісом. Попри те, що головний офіс Google на території Європи розташований в Ірландії, цілком очевидним є те, що керівництво загальною політикою здійснюється не ним. Для можливості розгляду скарг Комісія імплементувала новий Європейський Рамковий документ, розтлумачений усіма європейськими органами в керівних принципах Європейської ради з захисту даних.

Розслідування Комісією здійснювалося он-лайн, шляхом аналізу навігації та документів користувача, до яких він отримує доступ при створення Google- акаунту. Було виявлено два аспекти порушення GDPR.

1) Порушення зобов'язання щодо прозорості та поінформованості - інформація що призначена для користувачів не є легкодоступною – така важлива інформація як: мета обробки даних, період зберігання даних,

категорії даних, що використовуються для персоналізації оголошень розміщена в декількох документах, доступ до яких потребує дій з 5-6 кроків. Більш того, деяка інформаціє не є достатньо чіткою та зрозумілою для користувачів.

2) Відсутність правової підстави для персоналізації реклами – Google вважає, що отримує згоду на таку обробку даних, однак Комісія наводить дві причини її відсутності, зокрема:

а) користувачі не достатньої мірою поінформовані;

б) згода не має характеру ані конкретної, ані однозначної.

Внаслідок цього, Google було оштрафовано на 50 млн. євро [6].

Висновок. Отже, сфера захисту персональних даних та її правове регулювання в Європейському Союзі зазнала значних змін після впровадження Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних – GDPR.

Завдяки екстериторіальній дії Регламенту, суттєвих змін зазнають і процедури обробки даних поза межами ЄС.

При здійсненні обробки персональних даних слід дотримуватися принципів пропорційності кількості даних до мети їх збирання, часу зберігання а також кількості осіб, що мають доступ до таких даних.

Важливим є забезпечення схоронності окремих категорій даних, зокрема, так званих «чутливих» даних про особу. Одним із ключових механізмів є забезпечення суб'єкта даних повною та доступною інформацією про операції із його даними та отримання беззастережної згоди від останнього.

Література

1. РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з

опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) // Офіційний вісник Європейського Союзу. Офіційний переклад. URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf

2. Пилипчук В. Г. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України/В. Г. Пилипчук, В. М. Брижко // Вісник Національної академії правових наук України. - Харків:Право, 2017. N 2017. №3 (90). – С. 36-50.
3. Magdalena K˛edzior GDPR and beyond—a year of changes in the data protection landscape of the European Union. Europäische Rechtsakademie (ERA) 2019 URL: https://link.springer.com/article/10.1007%2Fs12027-019-00549-x
4. First Austrian Fine: CCTV Coverage – Summary. URL: https://edpb.europa.eu/news/national-news/2018/first-austrian-fine-cctv-coverage-summary_en
5. Ana Monteiro First GDPR fine in Portugal issued against hospital for three violations. The International Association of Privacy Professionals. URL: https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/
6. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. URL: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc