УДК 340
DOI 10.32999/ksu2307-8049/2022-1-7

ВПЛИВ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ПРОВЕДЕННЯ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ З ГРОМАДЯНАМИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Спіцина Г.О., д. ю. н., професор,
завідувач кафедри права гуманітарно-правового факультету
Національний аерокосмічний університет імені М.Є. Жуковського «Харківський авіаційний інститут»
orcid.org/0000-0001-9131-0642

Турська В.М.,
здобувач вищої освіти першого року навчання, спеціальність 081 – Право,
третій освітньо-науковий рівень доктор PhD кафедри права
гуманітарно-правового факультету
Національний аерокосмічний університет імені М.Є. Жуковського «Харківський авіаційний інститут»
orcid.org/0000-0003-4911-7093

У статті розглянуто необхідні зміни в захисті персональних даних під час ведення господарської діяльності суб'єктами України з громадянами Європейського Союзу. Зроблено висновок про необхідність імплементації категорійного апарату Загального Регламенту захисту персональних даних у чинне законодавство України.

Ключові слова: *захист персональних даних, персональні дані, інформація, господарська діяльність.*

Spitsyna H.O., Turska V.M. THE IMPACT OF THE GENERAL REGULATION ON PERSONAL DATA PROTECTION ON CONDUCTING BUSINESS ACTIVITIES WITH CITIZENS OF THE EUROPEAN UNION

The paper considers the necessary changes in the protection of personal data in the conduct of economic activity by the subjects of Ukraine with the citizens of the European Union. The innovations of the Regulation and the expediency of their application in national legislation are investigated. The presence of a direct impact on the implementation of economic activity due to the existence of liability for violation of personal data protection standards has been traced. The absence of a mechanism for imposing liability on the state of Ukraine was revealed, but there is a possibility of limiting the collection of personal information on its territory. It is concluded that it is necessary to implement the categorical apparatus of the General Data Protection Regulation in the current legislation of Ukraine.

Key words: *personal data protection, personal data, information, economic activity.*

Мета статті полягає в тому, щоб на підставі системного аналізу правової регламентації висвітлити досвід змін в господарської діяльності з громадянами Євросоюзу після введення в дію Загального Регламенту захисту персональних даних.

Методи структурного аналізу і синтезу використовувалися для поділу отриманої інформації на окремі структурні одиниці та системного поєднання різних сторін інформації в єдину структуровану систему викладення інформації щодо особливостей, які започатковані Загальним регламентом захисту персональних даних.

Актуальність теми полягає в тому, що сьогодні жодна людина не уявляє свого життя без соціальних мереж чи месенджерів, купівлі товарів через Глобальну Мережу, заповнення анкет на отримання дисконтних чи банківських карток та інших документів, де необхідно вносити свої персональні дані. Зокрема, персональні дані збираються у фізичних осіб й при провадженні господарської діяльності, наприклад при купівлі товарів через Мережу, чи здійсненні фінансового моніторингу при вчиненні значних правочинів, укладанні договорів. Тобто вбачається досить стрімке розповсюдження персональних даних у всіх сферах людського існування, а тому постає логічне питання щодо захисту цих даних.

Виклад основного матеріалу.

«25» травня 2018 року набрав чинності Загальний регламент захисту персональних даних (англ. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679) (далі – Регламент, GDPR, Регламент GDPR). Саме особливістю цього Регламенту виступає уніфікація регулювання відносин щодо захисту персональних даних фізичних осіб, а також експорт персональних даних за межі Європейського союзу та Європейської економічної зони [1].

На національному рівні ключові документи у сфері захисту персональних даних – це Конституція України, Закон України «Про захист персональних даних» документи у сфері захисту персональних даних, ухвалені Уповноваженим Верховної Ради України з прав людини. Вагоме значення має також низка інших законів, як, наприклад, Закон України «Про доступ до публічної інформації» та Закон України «Про інформацію» [2].

Тож задля того, щоб простежити саме вплив Регламенту, необхідно зосередити увагу на саме визначенні поняття «персональних даних». Відповідно до Закону України «Про захист персональних даних» надається визначення: «Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [4]. Тобто персональні дані – це будь-які дані про особу, за допомогою яких її можна ідентифікувати як таку. Натомість Регламент у статті 4 надає визначення персональних даних, а також конкретизує, що саме слід відносити до саме таких даних. Зокрема, це не тільки прізвище, ім'я, по батькові, ідентифікаційний номер чи он-лайн ідентифікатор, а також інші фактори, які можуть бути визначальними для фізичної особи у фізичній соціальній, фізіологічній, генетичній, розумовій, економічній, культурній сфері життя особи.

Вплив Регламенту на господарську діяльність слід розглядати в територіально-просторовому аспекті, оскільки існує певне обмеження територіального поширення дії Регламенту. У статті 3 Регламенту визначається, що дія поширюється на Європейський Союз, поза межами Європейського Союзу, у разі якщо: використовується право держави-члена Європейського Союзу чи опрацьовується інформація, яка належить громадянину Європейського Союзу.

Більш докладно розглянути вплив Регламенту на провадження господарської діяльності хотілось би на прикладі впливу на Україну цього документа. Саме найбільш в Україні «відчуватимуть» цей вплив IT-компанії, туристичні агентства, дизайнерські фірми, архітектурні компанії, агропромислові комплекси тощо.

У першу чергу GDPR стосується українських компаній, які мають постійні представництва в Європейському Союзі. Будь-яка передача персональних даних резидентів Європейського Союзу в головний офіс, який розташований в Україні, та наступна їх обробка повинна відповідати нормам Регламенту.

Вимоги GDPR розповсюджуються й на українські компанії, які не є резидентами Європейського Союзу, але займаються обробкою даних осіб, які знаходяться на території Європейського Союзу, якщо їхня діяльність пов'язана з пропозицією товарів та послуг відповідним суб'єктам або пов'язана з моніторингом діяльності суб'єктів даних, якщо така діяльність провадиться в Європейському Союзі.

Регламентом встановлюються ознаки, які підтверджують намір пропонувати товари чи послуги вищевказаним суб'єктам у Європейському Союзі. Такими ознаками є: 1) використання мови чи валюти, які зазвичай використовуються у державах-членів Європейського Союзу з можливістю замовляти товари чи послуги цією мовою; 2) згадка споживачів або користувачів, які знаходяться у Європейському Союзі.

З вищенаведеного випливає, що компанії, які територіально знаходяться в Україні, надають або пропонують послуги, реалізують товари через мережу Інтернет, та мова сайту є мовою держави-члена Європейського Союзу, або оплата за товари чи послуги передбачається в Євро, то обробка даних в таких компаніях підпадає під дію та повинна відповідати положенням Регламенту GDPR.

Положення Регламенту передбачають такий вид діяльності суб'єктів господарювання як моніторинг поведінки суб'єктів даних. Для цілей цього Регламенту – це збір інформації про фізичну особу з метою прогнозування особистих вподобань, особливостей поведінки, а також особистісних характеристик. Таким чином, моніторинг поведінки суб'єктів в мережі Інтернет зазвичай виконується шляхом відстеження файлів «cookie». У разі якщо відстежуються файли резидентів Європейського Союзу, а також передаються у подальшому аналітичним компаніям або рекламним компаніям, це повинно відповідати також вимогам Регламенту [5].

Якщо ще декілька років тому це була рідкість, то наразі вбачаємо, що повідомлення про відстеження файлів «cookie» та надання згоди на їх збирання наявне навіть на сайті Верховної Ради України. Майже усі компанії, які мають офіційну веб-сторінку у мережі Інтернет на англійській мові, мають відповідне повідомлення.

Нововведенням Регламенту є також поширення його дії на такі категорії осіб: 1) «контролери» – особи, які саме вирішують, як і коли збирати персональні дані; 2) «оператори» ж– особи, які відповідно до вказівок «контролерів» та на засадах аутсорсингу виконують функції з обробки та наступної передачі цих даних (оброблених) «контролеру».

«Контролером» та «оператором» може бути фізична, юридична особа, орган публічної влади, агентство чи інший орган. Виходячи з вищенаведеного, «контролер» володіє персональними даними та може розпоряджатися ними, «оператор» – той, хто може виконувати саме певні дії з даними за вказівкою «контролера».

На «контролера» Регламентом покладається обов'язок щодо вжиття необхідних технічних і організаційних заходів для гарантування та можливості доведення, опрацювання персональних даних здійснюється відповідно до Регламенту, а також проведення відповідних політик щодо захисту даних.

«Оператор» відповідно до Регламенту повинен також гарантувати, що опрацювання даних здійснюється відповідно до Регламенту, а також опрацювання повинно здійснюватися на підставі договору або іншого нормативно-правового акту відповідно до законодавства Європейського Союзу або держави-члена, який пов'язує «оператора» та «контролера» зобов'язальними відносинами та встановлює: які данні дані оброблюватимуться, тривалість оброблення та зберігання даних, категорії суб'єкта даних, специфіку і цілі опрацювання, а також права та обов'язки кожної зі сторін.

Тобто українські компанії можуть виступати як «контролером», так і «оператором». В більшості випадків українські компанії виступають «операторами», які не мають осередків

у Європейському Союзі, тому відповідно до статті 27 Регламенту «контролер» або «оператор» повинен призначити в письмовій формі представника в Європейському Союзі.

Єдиною вимогою для призначення представника є бути заснованим чи проживати або перебувати на території країни, персональні дані громадян якої оброблює компанія.

Новим для українських компаній є введення посади «співробітник з питань захисту даних», або Data Protection Officer. Це здійснюється в кожній компанії, яка збирає чи оброблює значний обсяг персональних даних резидентів Європейського Союзу, або якщо компанія збирає чи оброблює спеціальні категорії даних, а саме даних, що розкривають расову чи етнічну приналежність, політичні переконання, релігійні чи філософські вірування, чи членство в професійних спілках, і опрацювання генетичних даних, біометричних даних для цілей єдиної ідентифікації фізичної особи, даних стосовно стану здоров'я чи даних про статеве життя фізичної особи чи її сексуальної орієнтації. Такий перелік спеціальних категорій персональних даних надається в статті 9 параграфі 1 Регламенту. Такий працівник може бути залучений як на підставі трудового договору, так і на підставі договору про надання послуг. Якщо компанія складається з декількох філіалів чи структурних підрозділів, така компанія може мати одного співробітника із захисту персональних даних, за умови доступу до всіх підрозділів.

Головним завданням цього співробітника є здійснювати контроль, нагляд, а також сприяти реалізації всіх положень та норм Регламенту та інших положень про захист персональних даних Європейського Союзу чи держав-членів. Він також проводить навчання для працівників компанії, надає консультації з питань дотримання Регламенту, співпрацює з наглядовим органом, може виступати в ролі координатора з розподілення обов'язків серед співробітників та проведення відповідних перевірок.

Наступною обов'язковою умовою збирання та обробки даних є обов'язкове укладання договорів на обробку персональних даних – Data processing Agreement. Регламентом встановлюються обов'язкові умови, які повинні міститися у такій угоді: 1) предмет та тривалість обробки персональних даних; 2) характер та мета обробки персональних даних; 3) вид персональних даних та категорії суб'єкта даних; 4) зобов'язання та права «контролера» та «оператора».

Регламентом передбачається можливість надання усної згоди на обробку даних, але контролер повинен мати можливість довести наявність такої згоди. У разі письмового запиту чи спливаючого вікна на сторінці в мережі Інтернет така згода повинна чітко відрізнятися від інших питань, бути в доступній формі, з використанням чітких і простих формулювань. Суб'єкт повинен мати право відкликати таку згоду. Оскільки відповідно до статті 17 Регламенту існує право у кожного суб'єкта «право бути забутим». Кожен суб'єкт за своїм вільним і власним волевиявленням має право на стирання своїх персональних даних. Стирання персональних даних повинен здійснити контролер без затримки. Цікавим є те, що Регламент передбачає стирання персональних даних у разі, якщо немає більше потреби в їх зберіганні. З цього випливає, що «контролер» повинен чітко встановлювати строки обробки персональних даних, яких як і «контролер», так і «оператор» повинні дотримуватися.

У разі, якщо вчасно не знищуються персональні дані, це буде порушення прав особи на захист персональних даних.

Внаслідок можливості порушення прав особи Регламент передбачає розділ «Безпека персональних даних». Перш за все перед збиранням персональних даних «контролер» повинен оцінити всі ризики, які можуть виникнути під час збирання, обробки, збереження та передання таких даних третім особам або країнам. Тому не тільки «контролер» має обов'язок із забезпечення безпеки персональних даних, а й «оператор». Оскільки більшість даних зберігається на електронних носіях чи в мережі Інтернет, тому необхідно вжити саме заходів у сфері забезпечення захисту інформації, наприклад, шифрування, доступ на підставі спеціального ключа «токена», який існує тільки на фізичному носії у певної особи.

У разі порушення та втрати даних чи частини даних «контролер» або «оператор» повинні сповістити наглядовий орган країни протягом 72 годин з моменту виявлення такої втрати даних. У разі затримки повідомлення таке повідомлення повинно супроводжуватися супровідною інформацією про причини затримки.

Сьогодні в Україні ще не було запроваджено такого органу. В державах –членах Європейського Союзу запроваджені такі органи у різних проявах: Комісія Парламенту та Омбудсмен із захисту даних підзвітний парламенту, Національна комісія з інформатики, яка обирається Парламентом, Комісар із захисту персональних даних, Інспекційна рада підзвітна Парламенту [6].

Тому в Україні при втраті даних немає до кого звертатися. Лише повідомляти постійного представника у Європейському Союзі та Європейського Омбудсмену або Європейського інспектору із захисту даних [7, с. 45].

Також обов'язковим є повідомленим суб'єкта даних про порушення захисту персональних даних. У разі, якщо при втраті даних існує великий ризик ідентифікації особи, що є порушення права на захист персональних даних, «контролер» зобов'язаний негайно повідомити суб'єкта даних. Якщо «контролер» вжив усі можливі заходи щодо унеможливлення порушення прав суб'єкта даних, «контролер» не зобов'язаний повідомляти таку особу. У разі порушення норми про належне повідомлення суб'єкта даних для суб'єктів даних передбачено відшкодування шкоди, завданої розголошенням, втратою персональних даних в повному обсязі.

Як вже зазначалося вище, українські компанії зазвичай виступають «оператором», тому до компаній теж можуть застосовуватися

санкції, передбачені Регламентом. Оскільки Україна не є державною – членом Європейського Союзу, немає механізму накладення штрафу на Україну. Проте наглядовий орган держави-учасниці може заборонити передачу та обробку даних на території України, що може призвести до втрати значної частини доходу компанії.

Отже, частина 2 статті 32 Конституції України зазначає, що не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [3]. Право на захист персональних даних передбачено статтею 8 Хартії фундаментальних прав Європейського Союзу і статтею 16 Договору про функціонування Європейського Союзу. Тому проблема захисту персональних даних протягом існування Європейського Союзу завжди існувала, а з роками лише посилювалась. Стрімкий розвиток мережевої торгівлі та «зникнення кордонів» у договірному праві підвело до регулювання захисту персональних даних в середині Європейського Союзу, а також за його межами, якщо це стосується безпосередньо громадян Європейського Союзу. Слід зазначити, що 23 червня 2022 року під час саміту лідерів країн ЄС Україна отримали статус кандидатів на членство у ЄС, а тому окрема увага зараз приділяється встановленню відповідності норм чинного законодавства України встановленим нормам законодавства Європейського Союзу. Важливим є не тільки захист, а й наявність відповідальності за порушення такого захисту або «втечу» таких даних, тобто зростає необхідність створення державного органу контроля за дотриманням законодавства щодо збереження персональних даних. Все вищеперелічене надає нам Загальний регламент захисту персональних даних. Він встановлює чіткий вплив на господарську діяльність шляхом застосування санкцій у вигляді штрафів, розмір яких достатньо великий для українських реалій.

Україна стоїть на шляху євроінтеграції та адаптації українського законодавства відповідно до норм та стандартів Європейського Союзу, особливо після підписання Угоди про асоціацію між Україною та Європейським Союзом, отримання статусу кандидата у члени та закріплення такого вектору розвитку в Конституції України. Тому положення Регламенту розповсюджується й на українські компанії, але лише у випадку, якщо така компанія є «контролером» або «оператором» таких даних.

Тобто усі компанії в Україні, які мають намір опрацювати персональні дані резидентів Європейського Союзу, повинні докладно вивчити положення Регламенту та впровадити та виконувати його положення на своїх сайтах, у договорах та угодах про спільну діяльність. Із чого випливає, що в майбутньому Закон України «Про захист персональних даних» потребує імплементації положень Регламенту та його понятійного апарату для гармонізації положень щодо захисту персональних даних.

ЛІТЕРАТУРА:

1. GDPR. Офіційний український переклад. URL: http://aphd.Ua/gdpr-ofitsiinyi-ukranskyi-pereklad-/.

2. Бем М.В., Городиський І.М. Захист персональних даних: Правове регулювання та практичні аспекти : науково-практичний посібник / Рада Європи, 2021. 160 с. URL: https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69.

3. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#n4263.

4. ЗУ «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#n11.

5. Тарасюк А.В. Вплив загального регулювання захисту даних на контролерів та процесорів персональних даних – резидентів України. *Інформація і право.* 1(24). С. 28–35. URL: http://ippi.org.ua/.

6. Посібник з європейського права у сфері захисту персональних даних. URL: https://www.echr.coe.int/Documents/Handbook_data_protection_UKR.pdf.

7. Брижко В.М. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і пра*во. № 3 (18). 2016. С. 45.

8. Хартія фундаментальних прав Європейського Союзу від 07.12.2000. URL: http://zakon.rada.gov.ua/go/994_524.

9. Договір про функціонування Європейського Союзу від 07.02.1992, 25.03.1957. URL: http://zakon.rada.gov.ua/go/994_b06.

10. Обробка персональних даних відповідно до європейських правил. URL: https://www.smartsolutions.ua/ua/obrobka-personalnix-danix-vidpovidno-do-evropejskix-pravil-analiz-general-data-protection-regulation.