

**Марченко В. Б.**

*к. ю. н., доцент*

*ДВНЗ «Київський національний економічний університет  
імені Вадима Гетьмана», м. Київ*

## **ОКРЕМІ ЕКОНОМІКО-ПРАВОВІ АСПЕКТИ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ GDPR**

Як відомо, 25 травня 2018 року набув чинності Загальний регламент захисту даних ЄС № 2016/679 (GDPR) [1]. Прийняття документа спричинило появу в Україні цілої низки публікацій та коментарів, які практично одноставно проголошують його незаперечним благом для особи та суспільства у цілому. У даній публікації ми спробуємо розглянути окремі критичні аспекти у зв'язку із прийняттям Регламенту 679 (GDPR).

Перш за все, слід згадати про політико-правові зобов'язання України у стосунках із Європейським Союзом. Відповідно до ст.15 «Захист персональних даних» Угоди про асоціацію з Європейським Союзом [2] договірні сторони беруть на себе взаємне зобов'язання співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, включаючи відповідні документи Ради Європи. Отже, законодавчий аспект європейської асоціації України передбачає форму співробітництва у сфері захисту персональних даних у напрямі найвищих, зокрема, європейських стандартів. Таким чином, прийняття Регламенту 679, очевидно, має певним чином вплинути на законодавчі зміни в Україні.

Слід відзначити, що відповідно до Угоди інтенсивність руху України в бік законодавства ЄС різниться залежно конкретних сфер. Так законодавча асоціація України, зокрема, у сферах поштових та кур'єрських послуг, телекомунікаційних, фінансових та транспортних послуг, електронної торгівлі, державних закупівель (відповідно ст.ст.114, 124, 133, 138, 140, 153 Угоди) передбачає такі форми як адаптація, сумісність, наближення, приведення у відповідність, узгодження, впровадження, імплементація. Таким чином, наближення законодавства України до пра-

ва ЄС відбувається у визначених сферах та порядку, і не передбачає прямих зобов'язань України щодо запровадження європейських правил у сфері захисту персональних даних. Форма співробітництва з ЄС у сфері законодавства про захист персональних даних передбачає досить широкі рамки, які дають змогу обирати варіанти: від прямого перенесення європейських норм до креативної їх обробки відповідно до українських умов та інтересів українських суб'єктів.

Важливим є питання, чи зачепить Регламент 679 діяльність українських суб'єктів і яким чином. Деякі автори стверджують, що Регламент 679 має екстериторіальну дію [3]. Однак, на нашу думку, з таким висновком не слід поспішати. Норма п.2 ст.3 GDPR [1] каже, що Регламент 679 застосовується до обробки персональних даних відповідних суб'єктів, які знаходяться в ЄС, оброблених контролером або обробником, які не засновані в ЄС, якщо діяльність з обробки пов'язана з: (а) пропозицією товарів чи послуг суб'єктам даних в ЄС, незалежно чи вимагається оплата від цього суб'єкта даних або (б) моніторингом їх дій, оскільки їх дії мають місце всередині ЄС. Таким чином, український суб'єкт дійсно підлягатиме дії Регламенту 679, але за умови, що здійснюватиме вищезазначену діяльність всередині ЄС.

Важливим є питання, чи є філософія правового захисту персональних даних, яка реалізується Регламентом 679 однозначним благом для особи і суспільства у цілому. Оприлюднені факти і оцінки свідчать, що вплив зазначеного нормативного документа на здійснення господарської діяльності далеко не завжди є однозначним [4]. Так, для деяких компаній вступ у дію Регламенту 679 є рівнозначним їх закриттю з причини високої вартості впровадження вимог GDPR. Зокрема, компанія Uber Entertainment, яка робить онлайн-ігри, припинила роботу її гри Super Monday Night Combat саме через GDPR. Застосувавши інший підхід, компанія Gravity Interactive, виробник ігор Ragnarok та Dragon Saga, заблокувала європейцям доступ до її ігор. Через нове регулювання зачинила свою соціальну мережу для однокласників чеська інтернет-компанія Seznam.cz. Адже відповідно до правил GDPR за їх порушення регулятори можуть накласти штрафні санкції у розмірі до €20 млн. (\$25 млн.) або до

4% річного обсягу продажів.

Навіть великі технологічні компанії типу Facebook, Google та ін. також відчули на собі вплив змін, запроваджених GDPR. Підпорядкування новим правилам потягло за собою необхідність залучення адвокатів, експертів з персональних даних, програмістів. Впровадження нового Регламенту коштувало найбільшим всесвітнім компаніям десятки мільйонів доларів.

Підсумовуючи слід відзначити, що нові правила GDPR, з одного боку, надають європейцям більше контролю над їх персональними даними, а з іншого – спричиняють ускладнення відносин у даній сфері. Компанії, бізнес яких заснований на використанні персональних даних змушені будуть або взагалі відмовитись від нього, або змінити бізнес-моделі, або вкласти значні кошти в існуючі з метою адаптації до GDPR, що імовірно спричинить тенденції до збільшення вартості відповідних послуг.

Діяльність українських компаній нові правила зачеплять лише в тій частині, в якій вона базується на використанні персональних даних суб'єктів ЄС, що в умовах євроінтеграційних тенденцій стає реальним завданням для багатьох із них. Для українського законодавця актуальним завданням на сьогодні є розробка оптимальної законодавчої моделі адаптації до правил GDPR, яка має забезпечити належний рівень захисту даних, і водночас не повинна привести до помітного подорожчання товарів і послуг та зниження доступності ведення бізнесу.

### Список використаних джерел

1. 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**) : Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016. URL: [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.119.01.0001.01.ENG](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG).

2. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Угода від 27.06.2014р. URL: [http://zakon5.rada.gov.ua/laws/show/984\\_011](http://zakon5.rada.gov.ua/laws/show/984_011).

3. Коноваленко Д. Персональні дані: захист по-європейськи. – Юридична Газета online. – 16 травня 2018. URL: <http://yur->

[gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/personalni-dani-zahist-poevropeyski.html](http://gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/personalni-dani-zahist-poevropeyski.html).

4. *Ivana Kottasová*. These companies are getting killed by GDPR. – CNNMoney (London). URL:

<http://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html>.

**Маханець Л.Л.**

*к.е.н., доцент*

**Маханець Б.О.**

*Чернівецький національний університет імені Юрія  
Федьковича, м. Чернівці*

### **ЕКОНОМІЧНА БЕЗПЕКА У ЦИФРОВІЙ ЕКОНОМІЦІ**

Цифрову економіку на даний момент розглядають як невід’ємну частину суспільства. Її особливостями є багатофакторний вплив на суспільство, оскільки інформація формує суспільний розвиток і духовну сферу людини, а засоби її подання, як технічні, так і програмні, прямо впливають на фізичний і психічний стан особистості. Завдяки цифровій економіці підвищується ефективність усіх галузей за рахунок використання інформаційних технологій; якісно і кількісно збільшуються можливості здійснення практично всіх операцій, зокрема надання/отримання різних адміністративних послуг і виконання банківських транзакцій. Однак, крім множини переваг, цифрова трансформація несе і певні ризики та загрози безпеці економіки.

Інтереси суб’єктів господарювання, які беруть участь в процесах автоматизованої взаємодії, як правило, полягають в тому, щоб певна частина інформації, що стосується їх економічних, політичних та інших сторін діяльності, конфіденційні комерційні та персональні дані були б постійно легко доступні і в той же час надійно захищені від неправомірного використання. Перекручення або фальсифікація, знищення або розголошення певної частини інформації, так само як і дезорганізація процесів її обробки і передачі, завдають серйозної матеріальної і моральної шкоди. Таким чином, вкрай гостро постає питання забезпечення інформаційної безпеки як різних держструктур, так і персональних даних та комерційних організацій.