DOI https://doi.org/10.36059/978-966-397-601-3-170

ІМПЛЕМЕНТАЦІЯ GDPR ЯК ПРАВОВИЙ МЕХАНІЗМ ВЗАЄМОДІЇ УКРАЇНИ ТА ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Костянтин ФОТУЛ
студент юридичного факультету
ДВНЗ «Ужгородський національний університет»
м. Ужгород, Україна

Відповідність національного законодавства України правовим стандартам Європейського Союзу є надзвичайно важливою в умовах євроінтеграції України. Загальний регламент про захист даних (GDPR – General Data Protection Regulation) з 2018 року визначає загальні правила обробки персональних даних у ЄС. Захист персональних даних є одним із основних елементів цифрового правопорядку ЄС. Для України впровадження GDPR є не лише технічним юридичним завданням, а й стратегічним пріоритетом, оскільки це дозволить їй співпрацювати з ЄС у цифровій сфері та гарантувати вільний транскордонний потік даних. Аналіз правових механізмів такої імплементації дозволяє визначити як досягнутий прогрес, так і наявні прогалини у національному регулювання регулюванні.

Процес європейської інтеграції України вимагає системного наближення національного законодавства до acquis communautaire Європейського Союзу, зокрема в цифровій сфері. Одним із ключових елементів є забезпечення високого рівня захисту персональних даних, що є основою довіри в цифровій економіці та вільного руху даних. Загальний регламент про захист даних (GDPR – Regulation (EU) 2016/679), прийнятий Європейським Парламентом і Радою 27 квітня 2016 року та чинний з 25 травня 2018 року, встановлює єдині, високі стандарти обробки персональних даних у всьому Європейському Союзі[1]. GDPR не лише захищає фундаментальні права і свободи фізичних осіб, зокрема право на приватність (ст. 8 Хартії основних прав ЄС), але й сприяє розвитку єдиного цифрового ринку, усуваючи бар'єри для транскордонного обміну даними.

Для України імплементація принципів GDPR набуває стратегічного значення. Це не просто технічне завдання гармонізації норм, а необхідна умова для визнання Україною як «третьої країни з адекватним рівнем захисту персональних даних» відповідно до ст. 45 GDPR. Таке визнання дозволить українським компаніям, державним органам та громадянам безперешкодно передавати персональні дані до ЄС без додаткових

гарантій (наприклад, стандартних договірних положень чи обов'язкових корпоративних правил), що суттєво полегшить співпрацю в IT-секторі, електронній комерції, банківській сфері, охороні здоров'я та інших галузях[1]. Крім того, це посилить інвестиційну привабливість України як цифрового хабу для європейських компаній, особливо в умовах війни та післявоєнної реконструкції.

Правовою основою такого зближення є Угода про асоціацію між Україною та ЄС від 2014 року (ратифікована Законом України № 1678-VII), зокрема ст. 15 та Додаток XVII, які зобов'язують Україну наблизити своє законодавство до стандартів ЄС у сфері захисту персональних даних, включаючи впровадження принципів Конвенції Ради Європи № 108 (ратифікована Україною) та її модернізованого Протоколу 108[2]. Ці міжнародні зобов'язання підкріплюються європейською політикою розширення та звітом Єврокомісії про Україну (Ukraine Report 2025 та оновленнями 2026), де прогрес у сфері захисту даних оцінюється як частковий, але з рекомендаціями прискорити реформи[3]

Загальна характеристика GDPR включає його екстериторіальну дію (ст. 3): регламент застосовується не лише до компаній в ЄС, але й до будь-яких контролерів та операторів за межами Союзу, якщо вони обробляють дані суб'єктів з ЄС (наприклад, через пропозицію товарів/послуг або моніторинг поведінки). Структура GDPR охоплює 11 глав і 99 статей: принципи обробки даних (ст. 5 – законність, прозорість, обмеження цілей, мінімізація, точність, обмеження зберігання, цілісність і конфіденційність, підзвітність); права суб'єктів даних (ст. 12-23 – доступ, виправлення, видалення, обмеження обробки, портативність, заперечення, заборона автоматизованого прийняття рішень); обов'язки контролерів та операторів (ст. 24-43 – призначення Data Protection Officer (DPO), оцінка впливу на захист даних (DPIA), повідомлення про порушення протягом 72 годин, ведення реєстрів обробки); нагляд та санкції (ст. 51-84 – незалежні наглядові органи (DPA), співпраця через EDPB, штрафи до 20 млн євро або 4% глобального річного обороту)[4].

В Україні основним нормативним актом залишається Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI (зі

[1] Ukraine Report 2025. European Commission. Directorate-General for Neighbourhood and Enlargement Negotiations.

[2] Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Офіційний вісник України, 2014, № 75.

[3] Regulation (EU) 2016/679 (GDPR), arts. 5, 12–22, 24–43.

[4] Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (чинна редакція).

змінами). Він визначає поняття персональних даних, принципи їх обробки, права суб'єктів (доступ, згода, блокування, видалення), обов'язки володільців та розпорядників, а також роль Уповноваженого Верховної Ради України з прав людини як наглядового органу[5]. Конституційна основа – ст. 32 Конституції України, яка забороняє збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, передбачених законом.

Порівняльний аналіз українського законодавства та GDPR виявляє як досягнення, так і значні прогалини. Позитивні аспекти: запровадження принципів законності та прозорості обробки, права суб'єктів на доступ, виправлення та видалення даних, обов'язок повідомляти про витоки в окремих випадках. Однак розбіжності суттєві: термінологія не відповідає GDPR (володілець/розпорядник замість контролер/оператор/процесор); відсутність чіткого розмежування ролей; недостатня незалежність наглядового органу (Уповноважений ВРУ поєднує функції омбудсмена з багатьма іншими); санкції значно нижчі (максимум кілька тисяч гривень); відсутність обов'язкового DPO, DPIA, портативності даних, детального регулювання автоматизованого профілювання та прийняття рішень; слабке регулювання транскордонних передач (немає чітких механізмів adequacy чи SCC[6]

Інституційний механізм імплементації в Україні передбачає посилення ролі Уповноваженого ВРУ з прав людини, але для повної відповідності GDPR необхідне створення незалежного спеціалізованого наглядового органу (аналог DPA), з повноваженнями розслідувати скарги, накладати штрафи та співпрацювати з EDPB. Це один із ключових пунктів критики з боку Ради Європи та Єврокомісії[7].

Практичні виклики імплементації багатогранні. Технічні: брак сучасних систем шифрування, анонімізації, логування в державних реєстрах та бізнесі. Адміністративні: недостатня підготовка посадових осіб, відсутність культури compliance. Фінансові: високі витрати на впровадження заходів (особливо для МСБ). Правозастосовні: мінімальна судова практика, низька обізнаність громадян про свої права. Досвід країн Центральної та Східної Європи (Польща, країни Балтії – Естонія, Латвія, Литва) показує ефективність поетапного підходу: 1) масове навчання бізнесу та держслужбовців; 2) поступове впровадження законодавчих змін; 3) створення сильного незалежного DPA; 4) кампанії з підвищення цифрової грамотності населення; 5) співпраця з EDPB та бізнес-асоціаціями [8]

[5] Data Protection Laws and Regulations Ukraine 2025-2026. ICLG.

[6] Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (№ 108) та Протокол про внесення змін (108+).

[7] European Data Protection Board. Guidelines and decisions (2025–2026).

[8] Аналітичні матеріали Центру політико-правових реформ та EU4Digital (2024–2026).

Перспективи законодавчих змін пов'язані з законопроєктом № 8153 «Про захист персональних даних» (реєстр. 25.10.2022). Він був прийнятий у першому читанні 20 листопада 2024 року, включений до порядку денного сесії постановою № 4775-IX від 10 лютого 2026 року та зараз готується до другого читання з урахуванням зауважень експертів Ради Європи, бізнесу та громадськості. Проєкт передбачає: гармонізацію термінології з GDPR; розширення прав суб'єктів (портативність, заперечення); введення незалежного регулятора; обов'язкове призначення DPO в певних випадках; оцінку впливу; повідомлення про порушення; штрафи до рівня, наближеного до GDPR (до 150 млн грн для юросіб); чіткі правила транскордонних передач[9]. Водночас критика стосується потенційних обмежень для журналістів та громадських організацій (наприклад, обов'язок попереджати про зйомку в публічних місцях), що потребує доопрацювання для балансу між захистом даних та свободою слова.

Імплементація принципів GDPR є обов'язковою умовою глибокої євроінтеграції України, забезпечення адекватного рівня захисту персональних даних за європейськими стандартами та розвитку цифрової економіки. Чинне законодавство 2010 року суттєво застаріло і потребує комплексного оновлення – зокрема в частині прав суб'єктів даних, механізмів відповідальності контролерів/операторів, незалежності наглядового органу, розмірів санкцій, регулювання нових технологій (AI, big data, автоматизоване прийняття рішень). Необхідне не лише формальне приведення норм у відповідність до acquis ЄС, а й реальне правозастосування: ефективна робота наглядового органу, судова практика, підвищення цифрової правосвідомості бізнесу, держави та громадян. Успішна імплементація дозволить Україні отримати статус «третьої країни з адекватним рівнем захисту» від Єврокомісії (наразі такого рішення немає, на відміну від Великобританії, Японії, Південної Кореї тощо), що відкриє нові можливості для транскордонної співпраці, інвестицій в IT, електронної комерції та післявоєнної цифрової реконструкції країни.

[9] Проект Закону про захист персональних даних № 8153 (перше читання 20.11.2024, підготовка до другого читання станом на 2026). Верховна Рада України. https://itd.rada.gov.ua/billInfo/Bills/Card/40707