DOI: https://doi.org/10.71404/PPSS.2025.3.18

НАГЛЯДОВИЙ ОРГАН У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ: СТАНДАРТИ НЕЗАЛЕЖНОСТІ ТА ПЕРСПЕКТИВИ ІНСТИТУЦІЙНОЇ РЕФОРМИ В УКРАЇНІ

Дмитро Ігорович КОСТЮК,

аспірант НДІ приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України

Серед усіх аспектів гармонізації законодавства України у сфері захисту персональних даних з правом Європейського Союзу (далі – ЄС) питання інституційної незалежності наглядового органу є найбільш концептуально гострим. Воно безпосередньо стосується не лише технічних вимог GDPR, а й більш фундаментальних питань про межі виконавчої влади, ефективність механізмів захисту прав громадян у цифровому публічному просторі та готовність держави до повноцінної участі у спільному цифровому ринку ЄС.

GDPR у статті 51 вимагає від кожної держави-члена утворення одного або кількох незалежних наглядових органів, відповідальних за моніторинг застосування законодавства про захист персональних даних [1]. Ключовою є вимога повної незалежності: орган має діяти без будь-яких зовнішніх втручань, мати власний бюджет, право наймати та звільняти персонал, а його члени мають бути захищені від дострокового звільнення. Стаття 52 GDPR прямо встановлює, що члени наглядового органу при виконанні своїх обов'язків не звертаються за інструкціями та не приймають їх від будь-якої третьої сторони. Практика Суду справедливості ЄС, зокрема у справі «Комісія проти Австрії» (C-614/10, 2012) та у справі «Комісія проти Угорщини» (C-288/12, 2014), підтвердила, що навіть опосередкований або потенційний вплив уряду на наглядовий орган є несумісним із вимогами права ЄС [2].

Наглядові органи у країнах ЄС наділені широким колом повноважень: проводити розслідування за власною ініціативою або за скаргами громадян, видавати попередження та обов'язкові приписи, тимчасово або постійно забороняти обробку персональних даних, а також накладати адміністративні штрафи до 20 мільйонів євро або 4 % річного світового обороту суб'єкта обробки. Не менш важливою функцією є участь у Європейській раді із захисту даних (EDPB). Саме через EDPB забезпечується однакове застосування GDPR на всій території ЄС та вирішуються транскордонні справи щодо операторів, які здійснюють обробку персональних даних у кількох країнах одночасно. Для України, яка прагне до інтеграції у цифровий простір ЄС, участь у подібних механізмах є практичною необхідністю, а не лише формальною вимогою.

В Україні нагляд у сфері захисту персональних даних здійснює Уповноважений Верховної Ради України з прав людини [3]. Ця модель є проблематичною з кількох взаємопов'язаних причин. По-перше, Уповноважений є парламентським омбудсменом із широким правозахисним мандатом, що охоплює значно більше питань, ніж захист персональних даних, що об'єктивно розпорошує ресурси та увагу між широким колом функцій і унеможливлює формування спеціалізованої інституційної компетентності у відповідній сфері. По-друге, орган не має спеціалізованого апарату для виявлення та розслідування порушень, позбавлений повноважень самостійно ініціювати перевірки суб'єктів обробки та не може накладати санкції, що фактично унеможливлює практичне правозастосування [4]. По-третє, і це найбільш принципово, Уповноважений не має ефективних примусових механізмів щодо органів виконавчої влади та підпорядкованих їм структур, які є найбільшими операторами персональних даних у країні. Результатом є ситуація, коли найбільш масштабна обробка персональних даних в Україні залишається фактично поза дієвим наглядом.

Показовою є і статистика правозастосування: кількість адміністративних справ, порушених за статтею 188-39 КУпАП на підставі матеріалів Уповноваженого, є мінімальною, що є симптомом не відсутності порушень, а нездатності чинної інституційної моделі їх виявляти та реагувати на них. Нарешті, відсутність статусу повноцінного наглядового органу у розумінні GDPR унеможливлює участь України у механізмах одного вікна та взаємної допомоги між наглядовими органами держав ЄС, що є практично необхідним в умовах транскордонної обробки персональних даних українських громадян, зокрема у зв'язку з перенесенням частини державних реєстрів на хмарні сервери у країнах ЄС в умовах воєнного стану.

Аналіз інституційних моделей наглядових органів у країнах ЄС, що мають схожий із Україною правовий контекст і пройшли шлях євроінтеграції, дає підстави для конкретних пропозицій. Польське Управління із захисту персональних даних (Urząd Ochrony Danych Osobowych, UODO), утворене у 2018 році, є моделлю спеціалізованого незалежного органу, що поєднує нормативно-методичні, наглядові та правозастосовні функції [5]. Аналогічні за структурою органи функціонують у Чехії (Úřad pro ochranu osobních údajů), Литві, Латвії та Естонії. Спільними рисами успішних моделей є: чітко визначений спеціалізований мандат, захищений від скорочення бюджет, конкурсний порядок призначення керівництва, широкі повноваження щодо розслідування та санкцій, а також розвинена практика методичного керівництва для суб'єктів обробки.

Для України оптимальною є модель спеціалізованого Агентства із захисту персональних даних, утвореного як центральний орган виконавчої влади зі спеціальним статусом за аналогією до Антимонопольного комітету України або Національного агентства з питань запобігання корупції. Такий орган має поєднувати повноваження

щодо нормативного регулювання, нагляду, розгляду скарг та накладення санкцій щодо всіх категорій суб'єктів обробки, як приватних, так і публічних, включаючи органи виконавчої влади. Принципово важливим є закріплення дієвих механізмів захисту незалежності його керівництва від політичного впливу: конкурсний порядок призначення на основі фахових критеріїв, вичерпний перелік підстав для звільнення та достатній строк повноважень. Першочерговим кроком у цьому напрямі є внесення змін до Закону України «Про захист персональних даних» [6] у частині визначення статусу та повноважень наглядового органу із чітким закріпленням вимог незалежності, що відповідають стандарту статті 52 GDPR.

Утворення незалежного спеціалізованого наглядового органу у сфері захисту персональних даних є ключовою інституційною передумовою як ефективного захисту прав громадян, так і виконання євроінтеграційних зобов'язань України. Жодні інші законодавчі зміни не матимуть практичного ефекту без дієвого органу, здатного забезпечити їх реалізацію. Відповідна інституційна реформа є невідкладним пріоритетом адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління України.

Список використаних джерел:

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

2. Court of Justice of the European Union. Case C-288/12, Commission v. Hungary, Judgment of 8 April 2014. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0288

3. Теремецький В. І. Загальна характеристика охорони бази персональних даних за законодавством України. Право і безпека. 2015. № 2 (57). С. 171–176.

4. Теремецький В. І. Суб'єкти відносин, пов'язаних з персональними даними. Підприємництво, господарство і право. 2015. № 11. С. 3–5.

5. Urząd Ochrony Danych Osobowych (UODO). About the President of the Personal Data Protection Office. URL: https://uodo.gov.pl/en/484/874

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text