УДК: 343.4
DOI https://doi.org/10.24144/2307-3322.2026.93.4.28

ГАРМОНІЗАЦІЯ КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА УКРАЇНИ ЗІ СТАНДАРТАМИ ЄС У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Семчук Н.О.,
кандидатка юридичних наук,
старша наукова співробітниця
відділу проблем кримінальної юстиції та кримінології
Інституту держави і права
імені В.М. Корецького НАН України
ORCID: 0000-0002-9357-9108

Семчук Н.О. Гармонізація кримінального законодавства України зі стандартами ЄС у сфері захисту персональних даних.

Статтю присвячено дослідженню ролі та місця кримінального права у системі забезпечення загального рівня захисту персональних даних в Україні в умовах євроінтеграційних процесів.

Актуальність теми зумовлена необхідністю приведення вітчизняного законодавства у відповідність до стандартів Європейського Союзу, зокрема, Регламенту (ЄС) 2016/679 (GDPR).

Дослідження ґрунтується на комплексному аналізі правової природи персональних даних як самостійного об'єкта правової охорони. Автор наголошує, що для отримання статусу країни з адекватним рівнем захисту даних Україна має продемонструвати наявність не лише адміністративних, а й дієвих кримінально-правових механізмів. У межах дослідження проаналізовано положення статті 45 GDPR, яка визначає критерії оцінки правової системи третіх країн, включаючи роль кримінального права та доступ публічної влади до даних. Особливу увагу приділено критичному аналізу чинної статті 182 Кримінального кодексу України. Доведено, що її диспозиція, орієнтована на захист «недоторканності приватного життя», не повною мірою охоплює специфіку правопорушень у сфері захисту персональних даних, що створює розрив між українським правом та міжнародними стандартами. Розробляючи диспозицію запропонованої статті 182-1 КК України, автор пропонує запровадити санкції за незаконне транскордонне передання даних та протиправну торгівлю персональними даними.

У своїй роботі автор порівнює досвід Польщі та Південної Кореї у сфері захисту даних. Наприклад, у Польщі кримінальні покарання прописані прямо в профільному законі, а корейська модель, яку Євросоюз визнав однією з найкращих у світі, вдало поєднує спеціальний закон та норми Кримінального кодексу.

Аналізуючи українські реалії, автор зауважує, що сучасні ініціативи (зокрема, законопроєкт № 8153) роблять великий акцент на збільшенні штрафів, але не приділяють уваги змінам до кримінального законодавства. Тому в статті пропонується доповнити Кримінальний кодекс України новою статтею 182-1. Такий крок допоможе створити дійсно надійну систему захисту даних, яка відповідатиме європейським стандартам і допоможе Україні інтегруватися до ЄС.

Ключові слова: персональні дані, кримінальне право, GDPR, євроінтеграція, захист приватності, адекватний рівень захисту, стаття 182 КК України, законопроєкт № 8153, міжнародний досвід.

Semchuk N.O. Harmonization of Ukraine's criminal legislation with EU standards in the field of personal data protection.

The article is devoted to the study of the role and place of criminal law in the system of ensuring a general level of personal data protection in Ukraine amidst European integration processes.

The relevance of the topic is driven by the necessity of aligning national legislation with European Union standards, particularly Regulation (EU) 2016/679 (GDPR). The study is based on a comprehensive analysis of the legal nature of personal data as an independent object of legal protection. The author

emphasizes that to obtain the status of a country with an adequate level of data protection, Ukraine must demonstrate the presence of not only administrative but also effective criminal law mechanisms.

As part of the research, the provisions of Article 45 of the GDPR, which defines the criteria for assessing the legal systems of third countries – including the role of criminal law and public authorities' access to data – are analyzed. Particular attention is paid to a critical analysis of the current Article 182 of the Criminal Code of Ukraine. It is proven that its disposition, focused on protecting the «inviolability of private life,» does not fully encompass the specifics of personal data protection offenses, creating a gap between Ukrainian law and international standards.

Developing the disposition for the proposed Article 182-1 of the Criminal Code of Ukraine, the author suggests introducing sanctions for illegal cross-border data transfer and the unlawful trade of personal data.

In this work, the author compares the experiences of Poland and South Korea in the field of data protection. For instance, in Poland, criminal penalties are prescribed directly within the specialized law, while the Korean model – recognized by the European Union as one of the best in the world – successfully combines a special act with the norms of the Criminal Code.

Analyzing Ukrainian realities, the author notes that current initiatives (specifically Draft Law No. 8153) place significant emphasis on increasing fines but neglect changes to criminal legislation. Therefore, the article proposes supplementing the Criminal Code of Ukraine with a new Article 182-1. This step will help create a truly reliable data protection system that meets European standards and facilitates Ukraine's integration into the EU.

Key words: personal data, criminal law, GDPR, European integration, privacy protection, adequate level of protection, Article 182 of the CC of Ukraine, Draft Law No. 8153, international experience.

Постановка проблеми. У контексті європейської інтеграції Україна має забезпечити рівень захисту персональних даних, еквівалентний стандартам ЄС, зокрема таким, що були покладені в основу Імплементаційного рішення Комісії (ЄС) 2022/254 [1] щодо визнання належного рівня захисту в Республіці Корея. Важливою складовою такого рівня є не лише наявність ефективних адміністративних та регуляторних механізмів, а й дієва система кримінально-правових санкцій, здатних забезпечити реальну превенцію найбільш небезпечних порушень у сфері обробки персональних даних.

Метою дослідження є аналіз сучасного стану кримінально-правового регулювання відносин у сфері захисту персональних даних, виявлення прогалин у чинному законодавстві України та розробка пропозицій щодо вдосконалення норм Кримінального кодексу в умовах євроінтеграції

Стан опрацювання проблематики. В зв'язку з тим, що зараз формується новий підхід до відповідальності за порушення у сфері захисту персональних даних, заснований на побудові комплексної міждисциплінарної системи їх захисту, це питання поки що є мало дослідженим. Питанню приділяли увагу, зокрема, О. Братасюк [2, с. 42], А.В. Кебус [3, с. 52], О. А.Трегуб, Т. С. Гудіма [4, с. 50], Б. Якименко [5, с. 68], Н. Ментюх, О. Шевчук [6, с. 4] та ін. Проте ця проблематика потребує новітніх підходів, відповідної аналітики, та розробки нових механізмів застосування як на рівні законодавства, так і на рівні теорії.

Виклад основного матеріалу. Основним нормативно-правовим актом Європейського Союзу у сфері захисту персональних даних, який встановлює уніфіковані вимоги в межах Європейського Союзу та Європейської економічної зони, є Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільний рух таких даних і про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» (далі – GDPR). Відповідно до GDPR, зокрема, пунктів 104 і 105 преамбули, статей 5–7, 9, 45–47, 49 [7], держава, яка не є членом Європейського Союзу (у випадку України є кандидатом у члени), може отримати статус країни, що забезпечує належний (адекватний) рівень захисту персональних даних, і до якої персональні дані можуть вільно передаватися з території Європейського Союзу одразу після ухвалення такого рішення, без очікування повного членства.

Стаття 45 GDPR визначає параметри, за якими Україна могла б отримати рішення про адекватний рівень захисту персональних даних ще до повного завершення процедури вступу до ЄС [7]. Такі параметри включають, серед іншого: верховенство права, повагу до прав людини та основоположних свобод, відповідне законодавство як загального, так і галузевого характеру, зокрема, у сфері публічної безпеки, оборони, національної безпеки та кримінального права, а також доступ

органів публічної влади до персональних даних, разом із практикою застосування такого законодавства, правилами захисту даних тощо.

В даній статті ми обмежимося лише положеннями щодо безпосереднього захисту персональних даних за допомогою кримінально-правових засобів. Питання ролі кримінального права в забезпечення кібербезпеки, публічної безпеки, оборони, національної безпеки та ін. в аспекті можливого отримання Україною імплементаційного рішення Комісії ЄС щодо визнання належного рівня захисту, будуть висвітлені в наступних роботах.

Ухвалення рішень про адекватність вирішальне значення має не формальне існування кримінально-правових заборон, а їхня спроможність забезпечити реальний стримуючий ефект. Саме тому в Імплементаційному рішенні Комісії (ЄС) 2022/254 [1] детально аналізуються не лише види санкцій, а й фактична практика їх застосування, кількість накладених штрафів, кримінальних проваджень, масштаб покарань та коло суб'єктів, до яких вони застосовуються.

Кримінальне право в цьому контексті розглядається як дієвий інструмент, який гарантує, що найбільш небезпечні порушення не можуть бути зведені лише до адміністративного правопорушення або фінансового ризику для бізнесу.

В Україні всі правопорушення щодо захисту персональних даних, за які передбачена кримінальна відповідальність, містяться в Кримінальному кодексі [8]: ст. 182, 361-2, 362. Закон забороняє: незаконний збір, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконне її змінення; несанкціоновані дії з інформацією, що обробляється в комп'ютерах та електронно-обчислювальних машинах [8], а також адміністративна відповідальність за ст. 188-39–188-40 Кодексу України про адміністративні правопорушення.

Для ілюстрації того, як вирішуються питання кримінальних санкцій за порушення у галузі захисту персональних даних всередині ЄС, можна взяти приклад Польщі. Основним нормативним актом Польщі у сфері захисту персональних даних є GDPR [7]. Проте деякі додаткові та специфічні положення регулюються окремим національним законом. «Закон Польщі про захист персональних даних» (далі – Закон Польщі) містить 176 статей [9]. Статті Закону Польщі не мають заголовків, але поділені на 14 розділів: загальні положення, призначення інспектора з питань захисту персональних даних, умови та порядок акредитації органів сертифікації, розробка та затвердження кодексів поведінки, умови акредитації суб'єкта контролю за дотриманням кодексів, керівник офісу, провадження у справах про порушення правил захисту персональних даних, європейська адміністративна співпраця, моніторинг дотримання положень щодо захисту персональних даних, цивільна відповідальність і судочинство, положення про адміністративні та кримінальні санкції, перехідні та адаптаційні положення, заключні положення.

В контексті кримінального права, Закон Польщі [9] в ст. 107 передбачає відповідальність для тих, «хто обробляє персональні дані, хоча така обробка не є допустимою або особа не уповноважена на їх оброблення». Якщо діяння, стосується даних, що розкривають расове або етнічне походження, політичні погляди, релігійні чи світоглядні переконання, належність до професійних спілок, генетичних даних, біометричних даних, що обробляються з метою однозначної ідентифікації фізичної особи, даних, що стосуються стану здоров'я, сексуального життя або сексуальної орієнтації, покарання буде вищим.

Натомість, відповідно до імплементаційного рішення Комісії (ЄС) 2022/254 (п. 126-128) [1] в Кореї кримінально-правові норми щодо захисту персональних даних містяться в кількох документах. В першу чергу це базовий Закон Кореї про захист персональної інформації, який встановлює кримінальне покарання за: використання персональних даних або передання таких даних третій стороні без необхідної згоди; обробка чутливої інформації всупереч забороні, встановленій статтею 23(1) цього Закону; недотримання вимог безпеки, що призвело до втрати, викрадення, розголошення, підроблення, зміни або пошкодження персональних даних; невжиття необхідних заходів щодо виправлення, видалення або призупинення обробки персональних даних; а також незаконне передання персональних даних до третьої країни.

Окрім кримінальних санкцій, передбачених Законом Кореї про захист персональної інформації, неправомірне використання персональних даних може також становити склад кримінального правопорушення відповідно до Кримінального кодексу. Це стосується, зокрема, порушення таємниці листування, документів або електронних записів (стаття 316), розголошення інформації, що становить професійну таємницю (стаття 317), шахрайства з використанням комп'ютерів (стаття 347-2), а також привласнення майна та зловживання довірою (стаття 355) [1].

Проаналізувавши в сукупності різноманітні заходи забезпечення виконання положень про захист персональних даних, у тому числі санкції, Комісія доходить висновку, що корейська система забезпечує ефективне застосування правил захисту персональних даних на практиці, тим самим гарантуючи рівень захисту, який за своєю суттю є еквівалентним рівню, передбаченому в ЄС.

Система захисту персональних даних в Україні наразі зосереджена в межах ст. 182 КК України («Порушення недоторканності приватного життя»), тобто фокусується на «втручанні в особисте життя», тоді як сучасні процеси вимагають додаткового захисту власне самих процесів обробки [8].

У кримінальному праві України об'єктом охорони залишається переважно приватне життя особи, тоді як у європейській та корейській моделях сам порядок обробки персональних даних визнається самостійною правовою цінністю. Порушення процедур збору, зберігання, доступу, передачі чи знищення персональних даних визнається суспільно небезпечним навіть за відсутності безпосереднього втручання в інтимну сферу життя особи. Саме такий підхід відповідає логіці GDPR [7], у якому законність процесу обробки є первинною умовою допустимості будь-якої подальшої роботи з даними.

Особливістю сучасних порушень у сфері персональних даних є те, що вони найчастіше пов'язані не з діями окремих осіб, а з системними зловживаннями в межах великих організацій – державних органів, банків, телекомунікаційних операторів, IT-компаній, маркетингових платформ. У таких випадках адміністративні штрафи нерідко сприймаються як прийнятні операційні витрати. Лише загроза персональної кримінальної відповідальності посадових осіб здатна змінити управлінську поведінку та стимулювати реальні інвестиції в кібербезпеку, комплаєнс та внутрішні механізми контролю. Без кримінальної відповідальності адекватний рівень захисту неможливий концептуально.

У цьому сенсі кримінальне право забезпечує, щоб порушення, які виходять за межі звичайних регуляторних відхилень і набувають ознак зловживання владою, умисного ігнорування закону або системної експлуатації персональних даних, отримували найвищий рівень державної реакції. Без такого елементу система не може вважатися повною та здатною гарантувати «еквівалентний» рівень захисту у розумінні статті 45 GDPR [7].

Проте специфіка складу цього кримінального правопорушення суттєво відрізняється від міжнародних стандартів захисту даних за суб'єктними та об'єктивними ознаками. Водночас проєкт Закону №8153 [10], пропонуючи революційне збільшення фінансових санкцій у ст. 59, ігнорує кримінально-правовий аспект, та не пропонує відповідних змін до кримінального законодавства.

У практиці Європейської Комісії адекватність не зводиться до наявності формально правильного законодавства або системи адміністративних штрафів, а передбачає існування повного спектра засобів примусу, які дозволяють диференціювати відповідальність залежно від тяжкості діяння. Якщо правопорушення у сфері обробки персональних даних можуть тягнути за собою виключно адміністративні чи цивільно-правові наслідки, то держава фактично прирівнює системні, умисні та масштабні зловживання до технічних або процедурних помилок, що суперечить принципу пропорційності та ідеї стримувального ефекту санкцій.

Адміністративні штрафи, навіть надзвичайно високі, залишаються інструментом регуляторного впливу, а не виразом найвищого ступеня державного осуду. Вони ефективні щодо порушень комплаєнс-характеру, але принципово недостатні для реагування на умисну торгівлю базами даних, масові витоки, саботаж перевірок наглядового органу, приховування інцидентів безпеки чи незаконну транскордонну передачу даних у юрисдикції з нижчим рівнем захисту. За відсутності кримінально-правових санкцій такі дії залишаються у площині допустимого «регуляторного ризику», що підриває саму ідею особливої цінності персональних даних як об'єкта правової охорони.

Саме тому в імплементаційних рішеннях Комісії ЄС кримінальне право розглядається як структурний елемент системи адекватності, а не як факультативне доповнення. Корейський приклад демонструє, що наявність кримінальних норм у базовому законі про захист персональних даних та в Кримінальному кодексі стала одним із аргументів на користь визнання її системи «по суті еквівалентною» європейській. Це означає, що адекватність оцінюється не лише через регуляторні механізми, а через спроможність держави застосувати найсуворіші засоби юридичного примусу у випадках грубих та умисних посягань на режим обробки даних.

За відсутності кримінального блоку конструкція адекватності є асиметричною: вона має превентивний і компенсаційний рівні (адміністративна та цивільна відповідальність), але позбавлена

карального рівня, який у теорії права є необхідним для завершеності механізму правового захисту. Така система є функціонально неповною. Без кримінально-правового компонента «адекватність» перетворюється з комплексної правової категорії на суто регуляторний стандарт.

Враховуючи викладене, наразі, для інтеграції в ЄС, Україні потрібно суттєво змінити підхід до санкцій за порушення у сфері захисту персональних даних. Вдалим кроком в цьому напрямку може стати доповнення Кримінального кодексу України ст. 182-1, для протидії порушенням у сфері обробки персональних даних, яка вбере в себе кращі зарубіжні (зокрема, польські та корейські) надбання.

Об'єктом ст. 182-1 має стати насамперед встановлений порядок обігу інформації, адже в ряді випадків інформація, зібрана з порушеннями (наприклад, без дотримання механізму згоди або поєднана з незаконною транскордонною передачею) може не бути строго конфіденційною або у випадках, коли приватність особи ще не порушена, але її дані вже незаконно передані в базу маркетингової компанії.

«Порядок обробки персональних даних» доцільно розглядати як самостійний об'єкт кримінально-правової охорони, відмінний від приватності та недоторканності особистого життя. Йдеться не лише про охорону інтересів конкретної фізичної особи, а про захист публічно значущого правового режиму обігу персональних даних як елементу правопорядку в цифровому суспільстві. Такий порядок охоплює встановлену законом сукупність принципів, процедур і гарантій обробки даних (законність, цільове обмеження, мінімізація, безпека, прозорість, контрольованість, підзвітність), порушення яких саме по собі створює суспільну небезпеку незалежно від того, чи настало вже безпосереднє втручання у приватне життя конкретної особи. У цьому сенсі шкода завдається не лише індивідуальним правам, а й довірі до інформаційних систем, державних реєстрів, цифрової економіки та механізмів правового регулювання загалом.

У такій концепції кримінальне право захищає не лише результат (приватність), а процес, тобто легальну архітектуру обробки персональних даних. Це відповідає підходу GDPR, де центральним є не тільки захист суб'єктивного права, а забезпечення системної відповідності всіх операцій з даними встановленим правилам. Отже, визнання «порядку обробки персональних даних» самостійним об'єктом кримінально-правової охорони дозволяє обґрунтувати криміналізацію діянь, що посягають на сам механізм правомірного обігу даних, та наближає українську модель до європейської концепції «процесуальної» охорони персональних даних як фундаментального елементу правової держави.

Нова стаття має бути спрямована власне на захист порядку обробки персональних даних від порушень з боку в першу чергу великих компаній та їх службових осіб. Найбільші витоки даних стаються через зловживання доступом у державних реєстрах або великих корпораціях. Посилена відповідальність у ч. 3 запропонованої ст. 182-1 стимулюватиме бізнес інвестувати в кібербезпеку.

Додатково варто відзначити, що Згідно з GDPR, наглядовий орган повинен мати ефективні повноваження для розслідування. Якщо особа, яка обробляє дані, не лише порушує правила, а й свідомо перешкоджає перевірці (не надає доступ до серверів, приховує факт витоку, ігнорує вимогу про видалення незаконно отриманих даних), це свідчить про високий ступінь суспільної небезпеки та прямий умисел на приховування правопорушення. Тому кримінальне право має стати гарантом виконання регуляторних рішень, а кримінальна відповідальність за невиконання розпоряджень перевіряючих є критичною для визнання України країною з адекватним рівнем захисту персональних даних.

В диспозиції даної статті має бути звернуто особливу увагу на протидію незаконній обробці персональних даних, що полягає у їх збиранні, зберіганні, використанні, поширенні або наданні доступу до них всупереч вимогам законодавства, а так само незаконній транскордонній передачі персональних даних, що заподіяли істотну шкоду правам, свободам чи інтересам особи. Кваліфікованим видом даного кримінального правопорушення можуть бути ті самі дії, вчинені щодо персональних даних про расове або етнічне походження, політичні, релігійні чи світоглядні переконання, членство в професійних спілках, генетичних, біометричних даних, даних про стан здоров'я, сексуальне життя або сексуальну орієнтацію особи (чутливі персональні дані). А особливо кваліфікованим пропонується вважати дії, передбачені частинами першою або другою цієї статті, вчинені повторно, або за попередньою змовою групою осіб, або службовою особою з використанням службового становища, або поєднані з умисним невиконанням законних розпоряджень чи

вимог посадової особи, яка здійснює контроль за дотриманням законодавства про захист персональних даних, або якщо вони спричинили тяжкі наслідки.

Висновки. Для України як держави-кандидата на вступ до Європейського Союзу питання кримінально-правового захисту персональних даних набуває не лише внутрішньо-правового, а й міжнародно-правового значення. Йдеться не просто про модернізацію національного законодавства, а про здатність української правової системи продемонструвати Європейській Комісії наявність цілісного, багаторівневого та ефективного механізму примусу, порівнюваного з тим, який функціонує в державах-членах ЄС та країнах, визнаних такими, що забезпечують адекватний рівень захисту.

Сучасна модель кримінально-правового захисту в Україні, яка базується переважно на ст. 182 КК України, не охоплює всього спектру правопорушень у сфері захисту персональних даних. Існуючий склад кримінального правопорушення («Порушення недоторканності приватного життя») за своїм суб'єктним та об'єктивним змістом є вужчим, ніж вимоги європейських стандартів, що може стати перешкодою для визнання Україною статусу країни з адекватним рівнем захисту даних.

Аналіз законопроєкту № 8153 свідчить про спробу радикально посилити адміністративні санкції, проте повна відсутність пропозицій щодо модернізації Кримінального кодексу створює системний розрив. Досвід Польщі та Кореї демонструє, що кримінальне право є невід'ємним елементом системи «адекватності» захисту. Корейська модель, яку Комісія ЄС визнала еквівалентною європейській, є успішним прикладом такої конвергенції.

Тому деталізація кримінальної відповідальності за порушення процедур обробки даних шляхом доповнення Кримінального кодексу України новою статтею 182-1 є важливим кроком для забезпечення системності кримінальних покарань в сфері персональних даних, що відповідатиме статусу України як кандидата на вступ до ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. On the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act (notified under document C(2021) 9316) : Commission Implementing Decision (EU) 2022/254 of 17 December 2021. *Official Journal of the European Union*. 2022. URL: http://data.europa.eu/eli/dec_impl/2022/254/oj (дата звернення: 29.01.2026).
2. Bratasyuk O. Legal basis of personal data protection in Ukraine and Germany: organizational and managerial aspect. *Visegrad Journal on Human Rights*. 2023. No. 1. P. 42–49. DOI: https://doi.org/10.61345/1339-7915.2023.1.5.
3. Кебус А.В. Кримінально-правовий захист персональних даних відповідно до законодавства України та держав Європейського Союзу. *Modern scientific journal*. 2023. № 2(2). С. 52–60. DOI: https://doi.org/10.36994/2786-9008-2023-2-7.
4. Трегуб О.А., Гудіма Т.С. Посилення захисту персональних даних в Україні у контексті зовнішньоекономічної діяльності. *Вісник Львівського торговельно-економічного університету. Юридичні науки*. 2023. № 14. С. 50–57. DOI: https://doi.org/10.32782/2616-7611-2023-14-08.
5. Yakymenko B. Formation of the institute of personal data protection and experience of its implementation in the countries of the EU. *Scientific Journal of the National Academy of Internal Affairs*. 2023. Vol. 28, no. 3. P. 68–79. DOI: https://doi.org/10.56215/naia-herald/4.2023.68.
6. Mentukh N., Shevchuk O. Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy and Security*. 2023. Vol. 1, no. 1. P. 4–17. URL: https://lpas.com.ua/web/uploads/pdf/Law,%20Policy%20and%20Security_1(1)__2023-4-17.pdf (дата звернення: 29.01.2026).
7. General Data Protection Regulation: 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 and on the free movement of such data. *Official Journal of the European Union*. 2016. L 119. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 29.01.2026).
8. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 29.01.2026).

9. O ochronie danych osobowych: Ustawa z dnia 10 maja 2018 r. *Dz.U. 2018 poz. 1000*. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000 (дата звернення: 27.01.2026).

Про захист персональних даних: проект Закону України від 25.10.2022 № 8153. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40700 (дата звернення: 27.01.2026).

Дата першого надходження рукопису до видання: 29.01.2026
Дата прийняття до друку рукопису після рецензування: 20.02.2026
Дата публікації: 5.03.2026