УДК 347, 342
DOI https://doi.org/10.32782/2524-0374/2025-10/49

РОЗВИТОК ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ КРІЗЬ ПРИЗМУ РОЗВИТКУ ПРАВА ЄС

GENERAL ASPECTS OF REGULATION OF PERSONAL DATA PROTECTION: COMPARATIVE LEGAL ANALYSIS OF EUROPEAN AND UKRAINIAN LEGISLATION

Тимошенко О.А., к.ю.н., доцент,
професор кафедри права
Приватний вищий навчальний заклад «Європейський університет»
orcid.org/0000-0003-0006-1949

Стаття пропонує аналіз загальних положень правового інституту захисту персональних даних у праві Європейського Союзу та України з акцентом на структуроутворюючі елементи режиму: дефініції, сферу дії (матеріальну й територіальну), принципи оброблення, правові підстави, права суб'єкта персональних даних, підзвітність володільця/розпорядника, інституційну архітектуру нагляду, санкційний механізм та правила транскордонних передавань. Дослідження виходить із того, що Загальний регламент про захист даних (GDPR) виступає як загальний закон для всієї екосистеми персональних даних, тоді як нові європейські інструменти – Регламент (ЄС) 2025/327 про Європейський простір даних про здоров'я (EHDS) та Регламент (ЄС) 2023/2854 («Data Act») – діють як спеціальні закони у відповідних доменах, не змінюючи базових вимог законності, прозорості, мінімізації та підзвітності. Автор показує, що українське законодавство відтворює значну частину європейських засад (законність, цільове обмеження, точність, безпека), однак потребує нормативного підсилення у площинах підзвітності як автономного обов'язку (реєстри операцій, політики збереження/видалення, оцінки впливу, повідомлення про інциденти, «приватність за задумом/за замовчуванням»), деталізації мінімізації та строків зберігання, доктринально вивіреного тесту «законного інтересу», процесуалізації прав суб'єкта персональних даних (перенесення, стирання/«право на забуття», заперечення, гарантії щодо автоматизованих рішень), а також уніфікації тріади транскордонних передавань («адекватність – належні гарантії – винятки»). Окремо обґрунтовано, що наглядово-санкційна модель GDPR із повним циклом засобів впливу та шкалою пропорційності забезпечує дієвий ефект. На цьому тлі імплементація законопроєкту № 8153 розглядається як ключ до конвергенції з правом ЄС: термінологічне узгодження, закріплення підзвітності, посилення повноважень наглядового органу, типізація складів порушень і запровадження стримувальних адміністративних штрафів, а також секторальна синхронізація з EHDS та «Data Act». Практичний результат полягає у формуванні доказової, ризик-орієнтованої моделі відповідності, здатної підвищити реальний рівень захисту приватності, правову визначеність для учасників оброблення та створити передумови для майбутньої оцінки адекватності у відносинах Україна – ЄС.

Ключові слова: персональні дані, Загальний регламент про захист даних (GDPR), принципи оброблення, підзвітність, права суб'єкта персональних даних, законний інтерес, транскордонні передавання, нагляд і санкції, Європейський простір даних про здоров'я (EHDS), Регламент «Data Act», законопроєкт № 8153.

The article offers a comparative legal analysis of the general provisions of the personal-data protection regime in European Union and Ukrainian law, focusing on its structuring elements: definitions, scope (material and territorial), processing principles, legal bases, data-subject rights, accountability of controllers/processors, the institutional architecture of supervision, the sanctions mechanism, and rules on cross-border transfers. The study proceeds from the premise that the General Data Protection Regulation (GDPR) functions as the overall framework for the personal-data ecosystem, while the newer EU instruments – the European Health Data Space Regulation (Regulation (EU) 2025/327, EHDS) and the Data Act (Regulation (EU) 2023/2854) – operate as sector-specific and horizontal instruments in their respective domains without displacing the baseline requirements of lawfulness, transparency, minimisation, and accountability. The analysis shows that Ukrainian legislation reproduces a significant part of the European tenets (lawfulness, purpose limitation, accuracy, security) but requires normative strengthening of accountability as an autonomous duty (records of processing, retention/erasure policies, impact assessments, breach notification, privacy by design/default), fuller detailing of minimisation and storage-limitation standards, a doctrinally sound legitimate-interest test, proceduralisation of data-subject rights (portability, erasure/"right to be forgotten", objection, safeguards for automated decision-making), and harmonisation of the cross-border transfer triad (adequacy – appropriate safeguards – derogations). The article further argues that the GDPR's supervisory-sanction model – combining a complete set of corrective powers with a graduated scale of proportionate, effective and dissuasive administrative fines – ensures practical effectiveness. Against this backdrop, the implementation of Draft Law No. 8153 is framed as the key vehicle of convergence with EU law: terminological alignment, entrenchment of accountability, strengthening of the supervisory authority's powers, typification of infringements and the introduction of dissuasive fines, as well as sectoral synchronisation with the EHDS and the Data Act. The practical result is an evidence-based, risk-oriented compliance model capable of enhancing the real level of privacy protection, legal certainty for processing actors, and the preconditions for a future EU adequacy assessment in EU – Ukraine relations.

Key words: personal data, GDPR, processing principles, accountability, data-subject rights, legitimate interest, cross-border transfers, supervisory authorities, administrative fines, European Health Data Space (EHDS), Data Act, Draft Law No. 8153 (Ukraine).

Постановка проблеми. Нині проблематика захисту права на приватність має системний і міждисциплінарний характер, оскільки цифровізація соціально-економічних процесів зумовлює експоненційне зростання масивів персональних даних, що циркулюють між приватним і публічним секторами та виходять за юрисдикції конкретних держав. Така ситуація вимагає підвищену увагу до врегулювання відносин, пов'язаних із збереженням, обробкою, використанням, захистом персональних даних: від чіткості дефініцій і принципів обробки – до реальної підзвітності володільців/розпорядників, ефективності наглядових механізмів і дієвості процесуальних гарантій для суб'єктів персональних даних. Відправною точкою сучасної європейської моделі виступає Загальний регламент про захист даних (GDPR), що набув чинності 25 травня 2018 року та заклав екстериторіальні стандарти поводження з персональними даними для глобальних обробників [1].

Для України, що послідовно реалізує курс на європейську інтеграцію, означений вектор передбачає не лише формальне імплементування «загальної частини» GDPR у національне законодавство, а й методичне зближення з новими секторальними та горизонтальними інструментами ЄС, зокрема з EHDS та Data Act. Відповідно триває оновлення законодавства України про захист персональ-

них даних, спрямоване на гармонізацію з GDPR, підвищення рівня підзвітності, безпеки обробки та якості транскордонних передавань. У такому контексті наше дослідження зосереджується на загальних аспектах регулювання: понятійно-категоріальному апараті, принципах і правових підставах обробки, матеріальній і територіальній дії, правах суб'єкта персональних даних, підзвітності володільців/розпорядників та інституційній архітектурі нагляду – із системним порівнянням між правом ЄС (GDPR у взаємодії з EHDS та Data Act) і чинним/реформованим правом України. Такий підхід дає змогу ідентифікувати рівень нормативної конвергенції та виокремити «вузли» гармонізації, критично важливі для охорони здоров'я, функціонування державних реєстрів і розвитку цифрових ринків даних. Тому актуальність тематики цього наукового дослідження, насамперед, визначається загальною активізацією імплементаційних та гармонізаційних механізмів удосконалення законодавства України, центральне місце в яких займає правовий інститут персональних даних, їх обробки, використання, захисту.

Аналіз останніх досліджень і публікацій. У вітчизняній юридичні літературі тематика цієї наукової праці є недостатньо дослідженою. Окремі аспекти правового забезпечення персональних даних становили предмет наукового пошуку таких вітчизняних вчених як І.М. Городиський, О.А. Заярний, А. Кодинець, О. Орлюк, А. Погребна, О.В. Солодовник та ін., проте інтенсивність розвитку персональних даних, їх людиноцентричність та чутливість вимагають осучаснення наукових досліджень, а також вироблення ефективних науково обґрунтованих рекомендацій щодо удосконалення як правового забезпечення персональних даних, так і практики їх захисту, в тому числі крізь призму відповідних порівняльно-правових досліджень.

Метою статті є критичний аналіз стану правового забезпечення персональних даних в Україні та ЄС, обґрунтування шляхів посилення адаптованості вітчизняного правового забезпечення персональних даних до права ЄС. Задля ефективного досягнення мети пропонуємо окреслити наступні завдання наукового дослідження: 1) охарактеризувати специфіку сучасного етапу розвитку правового забезпечення персональних даних в Україні та ЄС; 2) визначити вектори адаптації законодавства України до правових стандартів ЄС в сфері захисту персональних даних.

Виклад основного матеріалу дослідження. Після набрання чинності GDPR у правовій системі Європейського Союзу відбувається інтенсивна нормотворча активізація, спрямована як на галузеву конкретизацію режимів обробки даних, так і на горизонтальне унормування їх обігу. Насамперед Регламент (ЄС) 2025/327 про Європейський простір даних про здоров'я (European Health Data Space, EHDS), офіційно оприлюднений 5 березня 2025 року та такий, що набрав чинності 26 березня 2025 року, встановлює детальну нормативну модель первинної обробки електронних медичних даних (надання медичної допомоги) та вторинної обробки (наукові дослідження, формування публічної політики, регуляторні/наглядові цілі) [2]. Регламент імплементує інституційний механізм через створення компетентних органів доступу до даних (Health Data Access Bodies) із адміністративно-процедурними повноваженнями щодо надання дозволів на вторинне використання, установлює вимоги до правових підстав доступу та використання, процедурні гарантії заявників і володільців наборів даних, а також технічні й організаційні заходи безпеки. У межах EHDS інституціоналізовано трансєвропейські платформи MyHealth@EU (для транскордонного обміну з метою надання медичної допомоги) та HealthData@EU (для вторинного використання даних), що функціонують на засадах сумісності та стандартизації. EHDS застосовується без шкоди для Загального регламенту про захист даних: GDPR виконує роль загального закону щодо персональних даних, тоді як EHDS є спеціальним законом у сфері даних про здоров'я, передбачаючи, обов'язки щодо анонімізації, обмеження цілей, мінімізації даних, контролю доступу та обліку операцій обробки.

Регламент (ЄС) 2023/2854 («Data Act») є горизонтальним актом прямої дії, який установлює гармонізовані правила справедливого доступу до даних та їх використання у відносинах між бізнесом і споживачами, між суб'єктами господарювання, а також між бізнесом і публічною владою. Регламент охоплює, зокрема, дані, згенеровані пов'язаними послугами, і визначає суб'єктний склад (надавач даних, користувач даних, постачальник послуг обробки даних), імперативні вимоги до доступу (недискримінаційність, розумність, прозорість умов), перелік несправедливих договірних умов (які вважаються недійсними), а також обов'язки щодо «перемикання» між постачальниками хмарних послуг та вимоги до інтероперабельності й технічної доступності інтерфейсів/АПІ. Будь-які операції з персональними даними в межах «Data Act» допустимі лише за наявності належної правової підстави й дотримання всіх гарантій приватності. Регламент починає застосовуватися з 12 вересня 2025 року, доповнюючи, а не замінюючи, європейський режим захисту персональних даних [3].

Право на приватність і, кореспондуюче до нього, право на захист персональних даних має конституційне закріплення, зокрема у положеннях ст. 32 Конституції України, де встановлено загальну заборону втручання в особисте й сімейне життя, окреслюючи допустимі межі такого втручання виключно у випадках, передбачених Конституцією [4]. Такий підхід у своїх засадничих рисах узгоджується з міжнародними стандартами захисту приватності та персональних даних, однак як норма прямої дії він потребує подальшої законодавчої конкретизації на рівні спеціального регулювання. З огляду на необхідність врегулювання, був ухвалений Закон України «Про захист персональних даних», який заклав системні засади правового режиму оброблення, визначив суб'єктний склад (володільці та розпорядники), права суб'єктів персональних даних та інструменти контролю і нагляду [5].

Проте правове забезпечення персональних даних в Україні на сьогодні має в певній мірі застарілий характер та не позбавлене системи юридико-технічних недоліків. Зокрема, цілком вірними є критичні зауваження Г. Саттона та А. Погребної щодо правової моделі захисту персональних даних в Україні. Г. Саттон підкреслює насамперед надмірний «реєстраційно-формальний» характер захисту, внутрішню колізійність норм, невизначеність ролей володільця та розпорядника персональних даних, суперечливість вимог до згоди й слабкість санкційної рамки, що робить закон «важким для виконання» [6, с. 39-45]. А. Погребна, зі свого боку, окреслює програму доопрацювань, які є нагальними та практично витребуваними, а саме: а) уніфікація дефініцій і кодифікація принципів оброблення персональних даних; б) удосконалення процесуальності та реальної забезпечуваності прав суб'єкта персональних даних; в) запровадження ризик-орієнтованої підзвітності; г) посилення інституційної спроможності наглядового органу; д) подальша гармонізація з європейськими стандартами, що включає в себе вироблення і реалізацію відповідної дорожньої карти [7]. Сукупно ці позиції збігаються у висновку про незавершену інституціоналізацію національного режиму та необхідність переходу від декларативності до ефективної, підзвітної моделі з узгодженими дефініціями і дієвими процедурами.

У відповідь на цю проблематику В. Головченко пропонує власну національну модель, що інтегрує конституційні засади й європейські стандарти, обґрунтовуючи концепт «розподіленого конституційного захисту»: гарантії приват-

ності та захисту персональних даних вибудовуються через системне тлумачення низки положень Конституції, без необхідності окремої «спеціальної» статті [8]. У цій логіці Конституція виконує роль загального закону, тоді як закон про захист персональних даних – спеціального закону, який операціоналізує права суб'єкта, обов'язки володільця/розпорядника, механізми ризик-орієнтованої підзвітності та нагляд. Узагальнюючи, доктринально виправданою є інтегрована модель, що поєднує конституційне ядро з детальним спеціальним регулюванням, узгодженим із європейською парадигмою (зокрема стандартами GDPR. – *Прим. авт.*), що у поєднанні є умовою реальної ефективності та передбачуваності правозастосування.

У контексті попередньо окресленої нормативної динаміки Європейського Союзу підхід О.В. Солодовника до питання посилення правового забезпечення персональних даних в Україні по суті інтерпретує європейську модель захисту персональних даних як правозахисну конструкцію, що виходить із базису фундаментальних прав і високих стандартів приватності та поширює свою дію поза межі ЄС завдяки екстратериторіальним критеріям, в тому числі і на Україну. Ключовою опорою цієї моделі є детально вибудуваний понятійний апарат і чітке розмежування ролей учасників оброблення, яке супроводжується матеріальними та процесуальними гарантіями для суб'єкта персональних даних і підвищеними стандартами підзвітності для володільця та розпорядника. Науковець робить висновок, що GDPR виконує функцію загального закону для всього масиву персональних даних, формуючи рамкові вимоги законності, прозорості, мінімізації, обмеження метою, безпеки та відповідальності [9, с. 42].

Не можемо не зазначити, що принципи, закріплені у статті 5 GDPR, виконують функцію «скрижалі» правового режиму оброблення персональних даних і задають матеріально-правові обов'язки володільця та розпорядника в кожній окремій операції. Йдеться про законність, справедливість і прозорість; цільове обмеження; мінімізацію; точність; обмеження строків зберігання; цілісність і конфіденційність (безпеку), а також про метапринцип підзвітності, що покладає на володільця обов'язок довести відповідність усім попереднім засадам [1]. У практичній площині це означає необхідність ведення реєстрів операцій, затвердження політик збереження та видалення, періодичного контролю точності й актуальності персональних даних, впровадження належних технічних і організаційних заходів безпеки та забезпечення внутрішнього аудиту.

Спираючись на ідеї М.В. Бема та І.М. Городиського щодо розриву між рівнями регулювання після прийняття GDPR, варто погодитись та додати, що такий розрив в цілому позитивно впливає на практику захисту персональних даних, поєднуючи санкційну та наглядову (превентивну) складові. На переконання вчених, ключова відмінність полягає в архітектурі відповідальності та наглядового забезпечення: у GDPR розділ VI інституалізує незалежні наглядові органи з широким інструментарієм примусових заходів (попередження, догани, обов'язкові приписи щодо приведення операцій у відповідність, видалення/виправлення, заборона оброблення, призупинення передавання до третіх країн, адміністративні штрафи), тоді як розділ VIII формалізує засоби правового захисту, деліктну відповідальність і санкції, встановлюючи чітко типізовані склади порушень і верхні межі штрафів за порушення майже кожної статті регламенту. Така інфраструктура створює реальний дієвий ефект: санкції мають превентивну й стримувальну дію, а нагляд – процесуальну спроможність швидко відновлювати законність [10, с. 241-242]. Натомість, Закон України «Про захист персональних даних» [5] хоч і фіксує базові вимоги до оброблення та кола суб'єктів, проте не забезпечує співмірної з європейською моделі організації відповідальності, оскільки відсутні деталізовані склади правопорушень, інструментарій примусу наглядового органу є вужчим, а санкційна рамка – недостатньо стримувальною й прогнозованою.

Позицію М.В. Бема та І.М. Городиського можна звести до висновку про невідповідності, коли чинна українська модель притягнення до відповідальності у сфері захисту персональних даних є реактивною та малоефективною: адміністративна відповідальність, по суті, застосовується лише у випадку невиконання припису Уповноваженого Верховної Ради України з прав людини за результатами перевірки (складання протоколу за ч. 2 ст. 188-39 КУпАП відтерміноване до стадії ігнорування припису) [11]. Науковці проаналізували судову практику, та зробили висновки, що практика таких проваджень поодинока й здебільшого стосується ненадання суб'єктові доступу до власних персональних даних; а у разі відсутності незаконного поширення або порушення порядку доступу володільцю, як правило, загрожує лише припис [10, с. 246]. Така конфігурація нівелює превентивну й стримувальну функції права, не гарантує належного захисту приватного життя відповідно до статті 8 Конвенції про захист прав людини і основоположних свобод [12] та конституційних приписів, і загалом заохочує формальний, а не ризик-орієнтований захист.

Натомість GDPR закріплює протилежну за логікою модель: розділ VI інституціоналізує незалежні наглядові органи з широким інструментарієм примусу (попередження, догани, обов'язкові приписи щодо приведення оброблення у відповідність, видалення/виправлення даних, заборона оброблення, призупинення передавання до третіх країн, значні адміністративні штрафи), а розділ VIII детально встановлює засоби правового захисту, підстави відповідальності та санкції. Стаття 83 GDPR типізує порушення й визначає верхні межі штрафів за порушення майже кожної матеріальної та процедурної норми, водночас формулюючи принципи індивідуалізації стягнення [1]. На цьому тлі український закон виглядає надто загальним: невизначеність формулювань та широка дискреція володільця персональних даних у способах організації оброблення ускладнюють побудову дієвої санкційної рамки й не створюють достатнього стримувального ефекту. У результаті, як зауважують автори, можливість накладення стягнення переважно за незаконне поширення персональних даних або за невиконання припису спонукає частину володільців ігнорувати інші обов'язки, розраховуючи на мінімальні наслідки.

Реформа українського законодавства про захист персональних даних за законопроєктом № 8153 [13] (прийнятим за основу 20.11.2024 [14]) має характер комплексної імплементації законодавства ЄС та спрямована на усунення системних розривів між національною «загальною частиною» і моделлю GDPR. Таке реформування включає в себе:

– по-перше, уніфікацію правових дефініцій («персональні дані», «обробка», «володілець/розпорядник», «спільні володільці», «спеціальні категорії персональних даних») і узгодження сфери дії з екстратериторіальними критеріями GDPR;

– по-друге, кодифікацію принципів і правових підстав обробки за європейським зразком (законність, справедливість і прозорість; цільове обмеження; мінімізація; точність; обмеження строків зберігання тощо), в тому числі передбачено спеціальний режим для чутливих категорій даних;

– по-третє, розширення та процесуалізацію права суб'єкта персональних даних (доступ, виправлення, стирання/«право на забуття», обмеження, перенесення, заперечення, гарантії щодо автоматизованих рішень), закріплюючи вимоги до змісту повідомлення, строків реагування і засобів судового та адміністративного захисту тощо.

– по-четверте, переведення національної моделі з формально-реєстраційної логіки на парадигму підзвітності, тобто фіксацію обов'язку володільця та розпорядника доводити належність обробки до вимог закону;

– по-п'яте, запровадження наглядової та санкційної складових, зокрема посилення інституційної спроможності компетентного органу (Уповноваженого Верховної Ради України з прав людини), закріплення процесуальних повноважень для інспекцій і приписів, запровадження інструментів негайного припинення неправомірної обробки тощо [15].

Висновки. Враховуючи вище зазначене, ми дійшли наступних висновків:

1) європейська модель захисту персональних даних: вибудувана навколо принципів статті 5 GDPR і розширеного каталогу прав суб'єкта, підкріплених підзвітністю володільця та розпорядника і процесуальною спроможністю наглядових органів (розділи VI, VIII, стаття 83); діє екстериторіально, спирається на триаду транскордонних передавань («адекватність – належні гарантії – винятки»); функціонує як багаторівнева система, у якій GDPR виконує роль загального закону, а спеціальні й горизонтальні акти, такі як, EHDS і Data Act забезпечують дієвий захист;

2) законодавство України потребує адаптації відповідно до стандартів ЄС, особливо в частині: термінологічного узгодження та кодифікації принципів і правових підстав; процесуалізації прав суб'єкта; переходу до підзвітності (реєстри операцій, політики збереження/видалення, приватність за задумом/за замовчування, повідомлення про інциденти); уніфікації режимів транскордонних передавань; а також посилення наглядово-санкційної архітектури.

ЛІТЕРАТУРА

1. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (Загальний регламент про захист даних, GDPR): Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27.04.2016. *Офіційний журнал Європейського Союзу.* 2016. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504
2. Про Європейський простір даних про здоров'я (European Health Data Space, EHDS) та внесення змін до Директиви 2011/24/ЄС і Регламенту (ЄС) 2024/2847: Регламент (ЄС) 2025/327 Європейського парламенту і Ради від 11.02.2025. *Офіційний журнал Європейського Союзу.* 2025. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500327
3. Про гармонізовані правила справедливого доступу до даних та їх використання і про внесення змін до Регламенту (ЄС) 2017/2394 та Директиви (ЄС) 2020/1828 (Data Act): Регламент (ЄС) 2023/2854 Європейського парламенту і Ради від 13.12.2023. *Офіційний журнал Європейського Союзу.* 2023. URL : https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng?utm_source=chatgpt.com
4. Конституція України від 28.06.1996 р. № 254к/96-ВР. 1996. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
5. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text
6. Жорж М.; Саттон Г. Аналіз Закону України «Про захист персональних даних» : DGI/DP/expertiseUKR (2012). Страсбург : Рада Європи, 2012. С. 45.
7. Погребна А. Коментар до Закону України «Про захист персональних даних». *Юридичний журнал.* 2010. № 7. URL : http://www.justinian.com.ua/article.php?id=3579
8. Головченко В. Правові основи захисту персональних даних. *Юридична газета онлайн*. 2018. № 36. URL : https://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnih-danih.html
9. Солодовник О.В. Адміністративно-правові засади захисту персональних даних: порівняльний аналіз міжнародних моделей регулювання. Аналітично-порівняльне правознавство. 2025. Т. 2. № 4. С. 340–343. URL : http://journal-app.uzhnu.edu.ua/article/view/338894/327127
10. Бем М.В., Городиський І.М. Відповідальність за порушення законодавства про захист персональних даних: проблеми відповідності законодавства України вимогам регламенту Європейського Союзу щодо захисту персональних даних (GDPR). *Право України*. 2019. № 2. С. 237-255. URL: http://jnas.nbuv.gov.ua/article/UJRN-0000976303
11. Кодекс України про адміністративні правопорушення від 18.12.1984 № 8073-X. URL : https://zakon.rada.gov.ua/laws/show/80731-10#Text
12. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. URL : https://zakon.rada.gov.ua/laws/show/995_004#Text
13. Проєкт Закону України «Про захист персональних даних»: № 8153 від 25.10.2022. Картка законопроєкту. *Офіційний вебпортал Верховної Ради України.* URL : https://itd.rada.gov.ua/billinfo/Bills/Card/40707
14. Постанова Верховної Ради України «Про прийняття за основу проєкту Закону України про захист персональних даних» від 20.11.2024 № 4065-IX. URL : https://zakon.rada.gov.ua/laws/show/4065-IX#Text .
15. Проєкт Закону України «Про захист персональних даних» від 25.10.2022 р. № 8153. *Офіційний вебпортал Верховної Ради України.* URL : blob:https://itd.rada.gov.ua/f51523c7-317b-4c21-9514-486bcedf71da

Дата першого надходження рукопису до видання: 21.10.2025
Дата прийнятого до друку рукопису після рецензування: 14.11.2025
Дата публікації: 28.11.2025