

## ПИТАННЯ ЦИВІЛЬНОГО, ГОСПОДАРСЬКОГО ТА ТРУДОВОГО ПРАВА

УДК 347.77

DOI <https://doi.org/10.32850/LB2414-4207.2024.34.05>

### ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ У ЄС: НОВІ ПРАВИЛА ДЛЯ ОНЛАЙН РІТЕЙЛЕРІВ

**Волинець Віталій Валентинович,**  
[orcid.org/0009-0003-0714-236X](https://orcid.org/0009-0003-0714-236X)  
доктор юридичних наук,  
професор кафедри  
готельно-ресторанної справи  
(Київський університет туризму  
економіки і права, м. Київ, Україна)

Статтю присвячено розвитку онлайн ритейлу, який нерозривно пов'язаний із захистом персональних даних. Для функціонування успішного бізнесу недостатньо надати споживачам товар, не потурбувавшись про захист їх конфіденційних даних. В Європейському Союзі цьому питанню відводиться особливе значення, а тому усвідомлюючи значну загрозу і очевидні наслідки, було введено нові регуляторні обмеження, які мають ефективно забезпечувати надійний захист конфіденційної інформації. Одним із таких революційних кроків у сфері онлайн торгівлі став прийнятий у 2016 році Загальний регламент захисту даних (GDPR). Введений в дію Регламент значно посилив вимоги щодо обробки та захисту персональних даних в країнах ЄС.

Впровадження нових стандартів вплинуло на онлайн ритейлерів не лише підвищенням рівня прозорості у зборі та обробці даних клієнтів, але й забезпеченням прав користувачів на доступ і видалення їхньої інформації. Зважаючи на розвиток цифрових технологій, посилюється і вплив кіберзагроз на сферу онлайн торгівлі. Такі нововведення спрямовані на зміцнення довіри споживачів і збереження їхніх прав у цифровій економіці. Порушення нових норм може призвести до суттєвих фінансових санкцій та зашкодити репутації компаній. В рамках цього особлива увага приділяється механізмам отримання згоди користувачів та їхньому праву на захист особистих даних.

Таким чином, впровадження цих правил є актуальним і необхідним питанням для адаптації бізнесу до сучасних вимог у сфері захисту інформації. Своєчасна імплементація нових норм допомагає забезпечити відповідність міжнародним стандартам і підвищити конкурентоспроможність онлайн ритейлерів на міжнародному ринку. Разом з тим, необхідність дослідження цієї теми обумовлена швидким розвитком цифрових технологій і зростанням обсягу персональних даних, що обробляються в процесі співпраці з онлайн ритейлерами. Важливо зрозуміти, як нові правові вимоги впливають на бізнес-процеси. Дослідження ефективності впровадження нових правил допоможе

виявити головні виклики та знайти шляхи для підвищення конкурентоспроможності онлайн ритейлерів на міжнародному економічному ринку. Головним чином цьому сприятимуть вже впроваджені в дію нормативно-правові акти, які встановлюють правові рамки для прозорого і безпечного використання даних, підвищуючи відповідальність онлайн ритейлерів за збереження конфіденційності інформації. Завдяки цьому, бізнес не лише стане ще ближчим до міжнародних стандартів, але й зміцнить довіру споживачів до онлайн платформ. Ця обставина є визначальним фактором успіху на ринку онлайн торгівлі.

**Ключові слова:** e-commerce, онлайн ритейлери, регламент GDPR, кібербезпека, конфіденційність даних, правове забезпечення, безпека.

## LEGAL SECURITY OF DATA PRIVACY IN THE EU: NEW RULES FOR ONLINE RETAILERS

**Volynets Vitalii Valentynovych,**

[orcid.org/0009-0003-0714-236X](https://orcid.org/0009-0003-0714-236X)

Doctor of Juridical Sciences, Professor  
at the Department of Restaurant Service  
in Hotels

(Kyiv University of Tourism, Economics  
and Law, Kyiv, Ukraine)

The article is devoted to the development of online retail, which is inextricably linked with the protection of personal data. To run a successful business, it is not enough to provide products to consumers without worrying about protecting their confidential data. In the European Union, this issue is given special importance, and therefore, realizing the significant threat and obvious consequences, new regulatory restrictions were introduced, which should effectively ensure reliable protection of confidential information. One of these revolutionary steps in the field of online trade was the General Data Protection Regulation (GDPR) adopted in 2016. The enacted Regulation significantly strengthened the requirements for the processing and protection of personal data in EU countries.

The introduction of new standards affected online retailers not only by increasing the level of transparency in the collection and processing of customer data, but also by ensuring users' rights to access and delete their information. Taking into account the development of digital technologies, the influence of cyber threats on the sphere of online trade is also increasing. Such innovations are aimed at strengthening consumer confidence and preserving their rights in the digital economy. Violation of the new regulations can lead to significant financial sanctions and damage the reputation of companies. As part of this, special attention is paid to mechanisms for obtaining consent of users and their right to protection of personal data.

Thus, the implementation of these rules is an urgent and necessary issue for business adaptation to modern requirements in the field of information protection. Timely implementation of new norms helps ensure compliance with international standards and increase the competitiveness of online retailers on the international market. At the same time, the need to research this topic is due to the rapid development of digital technologies and the growth of the amount of personal data processed in the process of cooperation with online retailers. It is important to understand how new legal requirements affect business processes. The study of the effectiveness of the implementation of new rules will help identify the main challenges and find ways to improve the competitiveness of online retailers in the international economic market. Mainly, this will be facilitated by the already implemented legal acts, which establish a legal framework for transparent and safe use

of data, increasing the responsibility of online retailers for maintaining the confidentiality of information. Thanks to this, the business will not only become even closer to international standards, but also strengthen consumer trust in online platforms. This circumstance is a determining factor of success in the online trade market.

**Key words:** e-commerce, online retailers, GDPR regulation, cyber security, data privacy, legal protection, security.

Розвиток онлайн торгівлі нерозривно пов'язаний із низкою процесів, які відрізняють цей вид бізнесу від традиційного. Вибираючи товар в мережі інтернет і переходячи за посиланням на інші сайти, споживач не може бути впевненим, що цей процес безпечний і що це ніяким чином не вплине на втрату його персональних даних. Будь-яка онлайн платформа повинна створити максимум безпеки для своїх споживачів та для себе особисто, оскільки втрата даних тягне за собою значні фінансові обмеження. Актуальність даного дослідження зумовлена тим, що для ефективного функціонування бізнесу необхідне підсилене правове забезпечення конфіденційності даних як споживачів так і надавачів комерційних послуг в мережі Інтернет. Дослідження правового питання забезпечення конфіденційності даних позитивно вплине не лише на європейське законодавство, а й стане підґрунтям для формування глобальних стандартів захисту персональної інформації, сприяючи розробці ефективних правових механізмів, забезпечуючи безпеку даних на міжнародному рівні.

Дослідженням питання конфіденційності даних у ЄС займалися вітчизняні науковці В. Іванов [1], М. Бем та І. Городинський [6], Ю. Мала [7], В. Сталіров [8] та інші. Незважаючи на розробленість теми, питання щодо правового забезпечення конфіденційності даних у ЄС залишається відкритим і потребує доопрацювання.

**Мета дослідження** – полягає у розкритті особливостей правового забезпечення конфіденційності даних у ЄС, в частині встановлення нових правил для онлайн ритейлів.

Завданнями дослідження є встановлення нормативно-правових актів, які вплинули на формування законодавства ЄС у сфері захисту персональних даних. Важливо розкрити зміст Регламенту GDPR, його правові та практичні аспекти. В процесі дослідження необхідно розглянути функції ритейлерів щодо захисту своїх конфіденційних даних та персональних даних користувачів. Підбити висновки опрацьованих завдань та визначити перспективи подальших досліджень.

**Результати.** Онлайн простір це сфера, яка вабить до себе онлайн користувачів. Реалізація товарів через e-commerce має низку переваг, серед яких зручність і доступність товарів і послуг, широкий вибір продукції, можливість порівняння цін, а також зниження витрат на логістику та обслуговування. Крім того, електронна комерція забезпечує швидкий доступ до ринків товарів і послуг по всьому світу, дозволяючи підприємствам розширювати свою клієнтську базу без географічних обмежень. Онлайн платформи також сприяють підвищенню рівня обслуговування клієнтів завдяки можливості цілодобового доступу до товарів та послуг.

За період розвитку онлайн торгівлі поширеного явища набув онлайн ритейл. Його зміст полягає в тому, що великі супермаркети чи інтернет магазини, купуючи товари за оптовими цінами, продають їх з певної націнкою. Ритейл це певна «різниця» в ціні, яку встановлює магазин для того, щоб вигідно продати товар. Онлайн ритейл – це вид продажу товару через віртуальні магазини та сторінки в соціальних мережах. Купівля здійснюється у формі безготівкових навантажень. Це зручно як для продавців так і для споживачів, оскільки не потрібно фізично йти до магазину і вибирати товар, витрачаючи на це власні ресурси і час.

В умовах онлайн торгівлі і купівлі товарів через інтернет використовуються безготівкові розрахунки, тому досить важливо, щоб під час розрахунків шахраї не скористалися персональними даними клієнта і не заволоділи цінною інформацією. Персональні дані – це відомості або сукупність відомостей про фізичну особу, яка ідентифікована чи може бути ідентифікована завдяки певному набору інформації. До персональної може бути віднесена будь яка інформація, за якою особу можна ідентифікувати серед всіх інших осіб. Зокрема це ПІБ, вік, гендерна приналежність, номер та серія документів, адреса електронної пошти, номер телефону, IP адреса тощо. Законодавство захищає персональні дані від безпідставної обробки. В рамках цього людина, аби здійснити якусь операцію із наданням персональних даних, має дати згоду на їх обробку, інакше це вважатиметься порушенням законодавства і може мати негативні наслідки [1].

Європейський Союз виступає рушійною силою у сфері правового регулювання захисту персональних даних. В Хартії основних прав Європейського Союзу від 7 грудня 2000 року закріплено право на приватність як основну цінність [2]. Ст. 7 Хартії гарантує право на приватність, а ст. 8 – встановлює гарантії захисту персональних даних. Так, відповідно до ст. 8 Хартії, персональні дані повинні оброблятися відповідно до встановлених правил для конкретних цілей і лише на підставі згоди суб'єкта даних чи інших законних підстав, визначених законодавством. Разом з тим, стаття 8 дає право доступу до своїх персональних даних та право на їх виправлення, вказуючи, що захист цих даних має здійснюватися під наглядом незалежного органу [2].

Саме ЄС одним із перших звернув увагу на захист персональних даних і на основі цього було створено низку нормативно-правових актів, які б врегульовували це питання. Таким документом була й Директива 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [3]. Цей міжнародно-правовий документ був одним із найфункціональніших у сфері регулювання захисту персональних даних, а також слугував взірцем для розробки інших нормативно-правових документів, які регулювали подібні питання.

Директива 95/46 ЄС [3] повністю відповідала потребам розвитку тогочасного економічно-бізнесового поля. Однак, незважаючи на її функціональні можливості, досить скоро розвиток і удосконалення технологічних процесів, поява нових сфер регулювання, а також обсягів автоматизованої обробки персональних даних призвели до появи нових питань, вирішення яких мало стати неминучим для продовження розвитку онлайн бізнесу. У зв'язку з цим постала потреба в розробці нового регулювання на рівні Європейського Союзу, яке б розширювало та доповнювало положення Директиви, запроваджуючи додаткові гарантії для суб'єктів даних і встановлюючи нові вимоги для володільців і розпорядників персональних даних. В рамках цих питань у 2007 році ЄС підписує Лісабонський договір [4]. Положення договору визначало право кожного на захист своїх персональних даних, надаючи Європейській Раді та Парламенту повноваження встановлювати спільні правила обробки персональних даних для всіх держав-членів ЄС.

Дискусії щодо необхідності загальноєвропейського регулювання обробки та захисту персональних даних почало свій шлях у 2009 році за ініціативи Європейської комісії. Нормативним документом, який би визначав всебічне регулювання питання захисту персональних даних і їх обробки, став Загальний регламент про захист персональних даних (General Data Protection Regulation, GDPR, надалі – Регламент) [5]. Проект цього документа був опублікований Європейською комісією для обговорення у січні 2012 року, а саме ухвалення на рівні ЄС відбулося 14 квітня 2016 року. 25 травня 2018 року Регламент GDPR набрав чинності [6, с. 26].

Як зазначає вітчизняна дослідниця Ю. Мала, сфера впливу регламенту GDPR поширюється на весь ринок, що функціонує в ЄС. Його впровадження підвищує рівень захисту конфіденційних відомостей як серед споживачів, так і серед надавачів онлайн послуг. GDPR [5] – це документ, що містить 99 статей, які визначають захист даних громадян Євросоюзу і разом з цим, призначені для компаній та організацій, які займаються збором та обробкою персональних даних. Дія Регламенту поширюється на всі компанії, інтернет-сайти, комерційні і некомерційні платформи, які обробляють особисту інформацію громадян ЄС, незалежно від місцезнаходження чи проживання. Для того, щоб працювати на онлайн-ринку ЄС, компанії необхідно запровадити юридичні, організаційні та технічні заходи для захисту персональних даних.

Стаття 13 Регламенту GDPR [5] визначає обставини, які зобов'язують компанії наймати Data Protection Officer (DPO), – внутрішнього співробітника, який відповідає за запровадження заходів безпеки та моніторингу діяльності ритейлерів щодо виконання ними вимог регламенту.

Дослідниця вказує, що діяльність Регламенту GDPR ґрунтується на 6 принципах. Відповідно до ст. 5 Регламенту першим принципом є законність та прозорість. Ритейлери збирають особисту інформацію про клієнтів на законних підставах і публічно повідомляють про це за допомогою Політики конфіденційності. Інформація щодо процесу збору, обробки та зберігання інформації має бути легкодоступною і повною.

Наступним принципом є визначення конкретних цілей. Відповідно до цього, ритейлер має пояснити споживачу для чого збирається інформація і як зібрані дані будуть використовуватися надалі. Визначені ритейлерами цілі повинні бути вичерпними і стосуватися надання послуг чи продажу товару.

Збір та обробка персональних даних має проводитися лише для комерційної діяльності і заявлених компанією цілей. Цей принцип означає, що ритейлери повинні збирати стільки інформації, скільки потрібно для використання її в комерційних цілях. Ще один принцип – точність та оновлення даних, визначає особливості гарантування правдивості даних. Відповідно до цього принципу ритейлери дозволяють споживачам видаляти чи виправляти некоректно введену інформацію.

Принцип обмеженого терміну зберігання передбачає, що тривалість зберігання інформації про надані персональні дані встановлено чіткими часовими рамками, відповідно до часу виконання конкретних задач. Це означає, що надання персональних даних і їх обробка відзначається конкретною метою, після вирішення якої необхідність в зберіганні таких даних втрачається.

Шостим принципом Регламенту, відповідно до статті 5 є забезпечення конфіденційності та безпеки. Ритейлери захищають дані від незаконної обробки та випадкової втрати. У випадку, коли такі дані з якоїсь причини було втрачено, клієнта повідомляють про цей факт протягом 3-денного терміну [7].

Вітчизняний дослідник В. Сталіров наводить технічні та організаційні заходи безпеки, які мають проводити ритейлери для того, щоб виконувати вимоги Регламенту і бути повноцінними учасниками на ринку. Так, задля забезпечення високого рівня безпеки, до функцій ритейлерів відносять:

- псевдонімізацію і шифрування;
- забезпечення конфіденційності та цілісності, доступності й стійкості систем та сервісів обробки персональної інформації клієнтів;
- здатність в найкоротші терміни відновити доступність даних;
- регулярне тестування заходів безпеки [8].

Наведені заходи безпеки впроваджуються і виконуються ритейлерами для того, щоб відповідати вимогам законодавства ЄС. Недотримання GDPR Регламенту може нести

в собі негативні наслідки для ритейлерів, зокрема штрафи чи можливість працювати. Сума штрафу в основному залежить від розміру завданих збитків, кількості потерпілих і ступеню винуватості компанії. Максимальний розмір штрафу, за словами Ю. Малої, 746 млн євро було накладено на найбільшу світову платформу електронної комерції Amazon, коли виявилось, що компанія використовувала персональні дані користувачів для проведення рекламних кампаній без їх згоди [7].

Досить часто Регламент критикують за його надмірну суворість викладених положень, що наче б то ускладнює саму обробку персональних даних у певних сферах, зокрема й в комерції. Зважаючи на це, деякі міжнародні дослідники наголошують на тому, що цей акт містить набір узгоджених правил захисту персональних даних для успішного використання в ЄС, визначаючи, тим самим, простір для юридичної визначеності як серед ритейлерів, так і серед споживачів [9, с. 12].

Доречно зазначити, що саме захист конфіденційності даних є однією з головних проблем для більшості ритейлерів, оскільки це трудомісткий і фінансово затратний процес. Навіть такі великі маркетплейси як Temu зіштовхується з пильною увагою регуляторів до збору та використання персональних даних. У 2023 році компанію звинуватили в порушенні зберігання та використання конфіденційних даних. Буцім то компанія збирала конфіденційну інформацію без згоди користувачів. Експерти з питань приватності висловили занепокоєння з цього приводу, однак компанія всі заперечення відкинула, наполягаючи на тому, що вона не збирає дані клієнтів та не використовує їх без відома. Водночас регулятор рекомендував споживачам, купляючи товар в інтернеті, не завантажувати застосунок ритейлерів, а заходити через перевірені браузері. Таким чином є шанс не втратити свої конфіденційні дані, помилково натиснувши на якесь посилання [10].

Найближчим часом у ЄС цифровий простір має стати більш безпечним та прозорим. Для цього по всій території ЄС застосовуватимуться Акти про цифрові послуги (DSA). Цей акт запроваджує нові правила для модернізації контенту, конфіденційності та прозорості користувачів. Нові зобов'язання в ЄС які зобов'язують ритейлерів дотримуватися правил, щодо запобігання поширенню шкідливого контенту, заборон чи обмеження певних методів таргетування на користувачів, обмін внутрішніми даними з регуляторами та пов'язаними з ним науковцями.

Наразі цей акт стосується маркетплейсів, які мають понад 45 млн користувачів у ЄС. Починаючи від лютого 2023 року вони поширюються на всі маркетплейси незалежно від їх розміру. Будь який ритейлер, що порушує встановлене ЄС законодавство в частині захисту персональних даних, автоматично загрожує штраф у розмірі до 6% від їх глобального обороту. Якщо такі порушення систематичні – порушникам можуть повністю заборонити діяльність в Європі [11].

Дослідження правового регулювання конфіденційності даних визначено низкою нормативно-правових актів, прийнятих ЄС для врегулювання важливих питань. Ефективна діяльність ритейлерів пов'язана із намірами заробити більше коштів, залучаючи при цьому значну кількість споживачів. Необхідність дотримання законодавства ЄС у сфері захисту конфіденційних даних вплине не лише на спроможність ритейлерів функціонувати на міжнародному ринку, але й бути перспективним гравцем, виконуючи всі відповідні правила, прийняті ЄС. Наразі питання правового забезпечення захисту конфіденційності даних є нагальним питанням, що потребує удосконалення, оскільки на міжнародній арені з'являються нові й нові виклики, вирішення яких має вплинути не лише на загальні умови ведення онлайн бізнесу, але й забезпечити сталу роботу, пов'язані із захистом даних.

**Висновки.** Дослідження встановило, що ключовим нормативно-правовим актом ЄС у сфері захисту персональних даних наразі є Регламент GDPR. Цей документ

є найбільш притомні серед тих, що приймалися до цього, регулюючи лише окремі питання захисту конфіденційності даних споживачів і ритейлерів. Ритейлери наразі виконують важливу функцію у забезпеченні захисту як власних конфіденційних даних, так і персональних даних користувачів. Продовжуючи власну діяльність вони повинні забезпечувати ефективні заходи безпеки, прозорість та стабільність, а також дотримання всіх інших принципів, визначених регламентом GDPR.

В подальших дослідженнях планується спрямувати зусилля на аналіз практичних аспектів, пов'язаних із викликами, що виникають в ритейлерів під час впровадження регламенту GDPR, а також вивчення впливу нових технологій, зокрема штучного інтелекту та блокчейну, як елементів впливу на захист персональних даних. Окрім цього планується розглянути питання адаптації законодавства до нових викликів, пов'язаних із кібербезпекою та захистом даних в електронній комерції.

### Список використаних джерел:

1. Іванов В. Захист персональних даних під час використання онлайн-форм. 2023. URL: <https://vkr.ua/publication/zakhist-personalnikh-danikh-pid-chas-vikoristannya-online-form> (дата звернення: 27.08.2024).
2. Хартія основних прав Європейського Союзу від 07 грудня 2000 р. URL: <https://ccl.org.ua/posts/2021/11/hartiya-osnovnyh-prav-yevropejskogo-soyuzu> (дата звернення: 27.08.2024).
3. Директива 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року.
4. Лісабонський договір 2007. URL: <https://infocenter.rada.gov.ua/uploads/documents/29057.pdf> (дата звернення: 26.08.2024).
5. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: [https://zakon.rada.gov.ua/laws/show/984\\_008-16#Text](https://zakon.rada.gov.ua/laws/show/984_008-16#Text) (дата звернення 23.08.2024 р.).
6. Бем М., Городинський І. Захист персональних даних: правове регулювання та практичні аспекти. «К.І.С.», 2021. 160 с. URL: [https://ombudsman.gov.ua/storage/app/media/uploaded-files/Handbook\\_Pers\\_Data\\_Protect\\_2021.pdf](https://ombudsman.gov.ua/storage/app/media/uploaded-files/Handbook_Pers_Data_Protect_2021.pdf) (дата звернення: 25.08.2024).
7. Мала Ю. Правила GDPR: як українським компаніям обробляти персональні дані громадян ЄС. «STALIROV&CO», 2023. URL: <https://stalirov.lawyer/uk/posts/reglamenti-gdpr-v-ukrayini> (дата звернення: 27.08.2024).
8. Сталіров В. Gdpr compliance: що це та кому потрібно виконати умови регламенту про захист персональних даних? «STALIROV&CO», 2022. URL: <https://stalirov.lawyer/uk/posts/gdpr-dlya-ukrayins-kih-it-kompanij> (дата звернення: 26.08.2024).
9. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2020. С. 34.
10. Історія компаній: як китайський маркетплейс Temu за два роки вийшов на світовий ринок. 2024. URL: <https://ua-retail.com/2024/08/yak-kytayskyu-marketpleys-temu-za-dva-roky-vuyshov-na-svitovu-riven/> (дата звернення: 26.08.2024).
11. ЄС: нові правила регулювання IT-платформ. Lex Inform, 2023. URL: <https://lexinform.com.ua/v-sviti/yes-novi-pravy-la-regulyuvannya-it-platform/> (дата звернення: 26.08.2024).