УДК 342.721
DOI https://doi.org/10.32782/2307-1745.2024.71.4

Тополевський Р. Б.,
кандидат юридичних наук, доцент,
старший науковий співробітник Львівської лабораторії прав людини
імені академіка Петра Рабіновича
Науково-дослідного інституту державного
будівництва та місцевого самоврядування
Національної академії правових наук України

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ У КОНТЕКСТІ СТАНДАРТІВ ЄВРОПЕЙСЬКОГО СОЮЗУ

Анотація. У статті проаналізовано особливості правового регулювання персональних даних в Україні в контексті відповідності стандартам Європейського Союзу (ЄС). Підкреслено, що захист персональних даних є фундаментальним аспектом прав людини в умовах інформаційного суспільства та цифрової економіки. Впровадження стандартів GDPR (General Data Protection Regulation) стало ключовим викликом для адаптації українського законодавства до європейських норм, що зумовлено євроінтеграційними процесами.

Досліджено основні принципи оброблення персональних даних, визначені в GDPR, включаючи законність, прозорість, цільове обмеження, мінімізацію даних, їх точність, обмеження строків зберігання, цілісність і конфіденційність. Акцент зроблено на правах суб'єктів даних, таких як право на доступ, виправлення, забуття, обмеження обробки та перенесення даних.

У статті детально проаналізовано проблеми, з якими стикається українська правова система у процесі імплементації Загального регламенту захисту даних (GDPR). Однією з ключових перешкод є відсутність незалежного органу, відповідального за контроль дотримання стандартів захисту персональних даних, що є фундаментальною вимогою GDPR. Наразі ці функції покладені на Уповноваженого Верховної Ради України з прав людини, можливості якого обмежені як фінансовими ресурсами, так і функціональними повноваженнями.

Важливою проблемою є також обмеженість фінансових і людських ресурсів, необхідних для впровадження нових стандартів. Багато підприємств, особливо малий і середній бізнес, не готові до значних витрат, пов'язаних із забезпеченням відповідності нормам GDPR. Це стосується, зокрема, впровадження технічних та організаційних заходів, найму відповідальних осіб та реалізації нових процедур обробки даних.

Окрім того, спостерігається низький рівень обізнаності бізнесу та громадськості щодо вимог GDPR. Висвітлено необхідність проведення масштабних інформаційних кампаній, спрямованих на підвищення обізнаності населення про права у сфері захисту персональних даних.

Акцентовано на важливості підготовки фахівців, здатних виконувати функції уповноважених осіб із захисту персональних даних. Рекомендовано запровадження системи інформаційної підтримки, що включає консультації, розробку методичних матеріалів і надання практичних рекомендацій бізнесу щодо інтеграції європейських стандартів.

Автор пропонує поетапну імплементацію GDPR, що включає прийняття законодавчих змін, поступове підвищення штрафів за порушення стандартів, а також створення системи консультаційної підтримки для суб'єктів обробки даних. Наголошено на необхідності гармонізації українського законодавства зі стандартами ЄС для посилення правового захисту громадян та розвитку цифрової економіки.

Підкреслюється важливість інтеграції норм GDPR у правову систему України як інструменту забезпечення прозорості, безпеки даних та відповідності міжнародним стандартам.

Ключові слова: захист персональних даних, GDPR, Україна, інформаційні права, права суб'єктів даних.

Постановка проблеми. Захист персональних даних в умовах інформаційного суспільства став однією із ключових передумов захисту прав людини. Обмеження свавільного збирання та обігу даних про особу необхідне як для того, щоб не дати державі можливості отримувати про особу надмірну інформацію, так і для того, щоб зменшити можливості шахраїв. Адже, за відсутності належного правового захисту, масове автоматизоване оброблення персональних даних дозволяє отримувати про людину не лише ту інформацію, якою особа володіє і самостійно поширює (або намагається приховати), але й ту, існування якої вона навіть не підозрює, яка, однак, може бути створена внаслідок спеціального оброблення персональних даних та поєднання тих, які зберігаються в різних реєстрах даних.

Стан дослідження. В умовах формування інформаційного суспільства та цифрової економіки зростає роль досліджень присвячених як окремим питанням інформаційних прав так і, зокрема, захисту персональних даних з теоретичної та практичної сторони. Саме тому ця проблематика викликає зацікавленість дослідників. Серед них, зокрема: М. Бем, І. Городиський, Г. Саттон, О. Родіоненко, Н. Головацький, М. Шабатура, Р. Салашник, К. Врублевська-Місюна, В. Тичина, В. Брижко, Т. Гуржій, А. Петрицький, М. Міщук, О. Москаленко, О. Обушенко та багато інших. Ці дослідники приділили суттєву увагу вивченню правового регулювання захисту персональних даних. Разом із тим, у зв'язку з євроінтеграцією все ще залишається проблема відповідності національного законодавства стандартам Європейського Союзу у сфері захисту персональних даних.

Мета статті полягає у з'ясуванні особливостей правового регулювання персональних даних в Україні з урахуванням відпо-

відності стандартам Європейського Союзу, висвітлити проблему, яка пов'язана з імплементацією Загального регламенту захисту даних в українську правову систему.

Виклад основного матеріалу. Правовий захист персональних даних в Європі пройшов довгий шлях. Тут і практика Європейського суду з прав людини за статтею 8 Європейської конвенції з прав людини, і рішення Конституційного суду Угорщини щодо права особи знати про те, де зберігаються її дані і які саме. В цьому відношенні прийняття в Європейському Союзі Загального регламенту захисту даних (англ. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679) (далі – GDPR) дозволило підняти питання захисту персональних даних на вищий рівень [1].

Як справедливо зазначають К. Врублевська-Місюна та В.Тичина: «захист персональних даних – це вміння балансувати між інформаційною відкритістю та закритістю, між двома прагненнями: максимально розширити доступ громадян до невтаємниченої публічної інформації (державної, наукової, освітньої, персональної тощо) і водночас максимально захистити інформацію приватного змісту»[2, с. 154]

Прийняття GDPR сприяло вирішенню проблемних питань щодо Європейського Союзу та Сполучених Штатів Америки щодо обміну персональними даними [3, p. 12].

Директива обмежує передачу персональних даних громадян держав, які входять до Європейського Союзу до держави, які не входять до ЄС за винятком, коли ці країни забезпечують належний рівень захисту [4, с. 1013].

Важливість GDPR для української правової системи стала очевидною саме внаслідок зобов'язань України наближення українського законодавстводо законодавства ЄС в межах виконання Угоди про асоціацію між Україною та ЄС. Це стосувалося і захисту персональних даних

GDPR не лише встановлює відповідні стандарти в межах ЄС, але й зачіпає інші держави, які ведуть обмін персональними даними з державами-членами ЄС. Відповідно таким чином задано певний стандарт поводження з персональними даними. Або законодавство вашої країни належним (в сенсі GDPR) захищає персональні дані, або ви не можете в подальшому отримувати персональні дані від держав-членів ЄС.

Сучасний стан оброблення персональних даних в Україні в контексті європейських правових стандартів стикається з низкою проблем. Серед них, зокрема, невідповідність чинного законодавства про захист персональних даних і GDPR. Разом із тим, відповідний законопроєкт по зміні законодавства про захист персональних даних відповідно до вимог GDPR розглядається Верховною Радою України [5].

Варто зазначити, що GDPR застосовується до юридичних осіб за межами ЄС, якщо вони обробляють дані громадян ЄС. В цьому відношенні українські підприємці, які надають послуги особам, які проживають на території ЄС повинні забезпечувати дотримання цих стандартів. Разом із тим, залишається проблемою умови дотримання стандартів GDPR, зокрема щодо того, як повідомляти про витоки даних та виконувати запити на видалення персональних даних. Більше того, значна кількість керівників українських підприємств та підприємців не усвідомлюють необхідності дотримання GDPR, поки не зіткнуться з судовими позовами. Очевидно, що в рамках європейської інтеграції існує необхідність проведення як з боку держави, так і з боку громадських організацій та ВНЗ відповідних освітніх зусиль щодо стандартів GDPR. Так, І. Похиленко пропонує підвищити обізнаність громадян про їхні права у сфері захисту персональних даних, використовуючи різні цифрові додатки, наприклад, «Дію» [6, с. 98]. Хоча варто зазначити, що сама обробка персональних даних системою «Дія» може становити порушення стандартів захисту персональних даних.

Тим не менше, якщо припустити, що підприємства знатимуть про ці стандарти і будуть їх виконувати – це потягне понесе певні витрати на запровадження стандартів GDPR та створення процедур відповідності GDPR. Існує необхідність навчання та виділення функціоналу особи, відповідальної за захист персональних даних. Потрібне також запровадження не лише правових, але і технічних та організаційних заходів [7, с. 55]. Особливо ця проблема постає у випадку малих компаній та фізичних осіб-підприємців, які нерідко не забезпечують дотримання стандартів GDPR як через вартість, так і через необізнаність та обмежений доступ до консультацій та підтримки щодо стандартів GDPR.

Таким чином, існує необхідність інтегрованого навчання цих стандартів представників українських компаній, які б виконували функції особи, уповноваженої на захист персональних даних за участі органів влади, вищих навчальних закладів та громадських об'єднань та забезпечення подальшого консультування з цих питань. А так само йдеться про розроблення відповідних внутрішніх політик та положень, які б забезпечували виконання GDPR та гарантували безпеку даних.

Сучасний «інформаційний ринок» в Україні все ще не готовий виконувати вимоги стандартів «право на забуття» та передачі даних. Разом із тим, попри наявність певних проблем щодо дотримання стандартів захисту персональних даних, прийняття відповідних документів щодо політики роботи з персональними даними та розміщення їх юридичними особами на своїх сайтах стає поширеним явищем.

Однак GDPR стосується не лише підприємницької діяльності, але і, інших сфер, зокрема журналістики [8, с. 54]. Так, ч. 1 ст. 85 GDPR передбачає, що «Держави-члени повинні на законодавчому рівні узгодити право на захист персональних даних відповідно до цього Регламенту з правом на свободу вияву поглядів та свободу інформації, в тому числі, опрацювання для цілей журналістики та цілей наукової, художньої чи літературної діяльності [GDPR].

В розумінні Загального регламенту захисту даних (GDPR) «персональні дані» це будь-яка інформація, яка стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи. Тут варто відзначити, що на відміну від Закону України «Про захист персональних даних», перераховані чіткі критерії, які визначають дані, що віднесені до конкретної ідентифікації особи.

Так, суб'єкти, які здійснюють оброблення персональних даних в ЄС (або, які отримують персональні дані з ЄС) мають обробляти дані законно та правомірно, зокрема на основі явно вираженої згоди особи. При цьому має бути забезпечена відповідна прозорість оброблення персональних даних для особи,

чиї дані обробляються, інакше кажучи як сама інформація, так і повідомлення про її оброблення мають бути стислими і зрозумілими для особи. Крім того особі має бути надана інформація не лише про саму операцію щодо опрацювання даних, алей про мету такого опрацювання. Існують також спеціальні вимоги щодо якості персональних даних. Йдеться, зокрема про їх відповідність та релевантність меті оброблення. Саме зберігання даних не повинно бути необмеженим, а якість зберігання має гарантувати їхню безпеку від неналежного доступу або зміни.

Саме ці принципи оброблення персональних даних описані в статті 5 GDPR:

1. *Законність, справедливість і прозорість обробки.* Йдеться про те, що персональні дані можуть оброблятися лише на основі однієї з передбачених статтею 6 правових підстав (згода, виконання контракту, законодавче зобов'язання тощо), При цьому самі дані мають оброблятися добросовісно, а суб'єкти даних повинні бути явно повідомлені про обробку даних.

2. *Цільове обмеження*. Персональні дані повинні збиратися лише для чітких, визначених і законних цілей. Їх подальша обробка має відповідати цим цілям або бути сумісною з ними. При цьому обробка задля суспільних інтересів, наукового чи історичного дослідження або статистичних цілей вважаються сумісними.

3. *Мінімізація даних*. Обробляються тільки ті дані, які необхідні для досягнення цілей опрацювання. Надмірне збирання або зберігання даних є порушенням.

4. *Точність даних.* Дані мають бути точними та оновлюватися за потреби. Неточні або застарілі дані потрібно видаляти чи виправляти.

5. *Обмеження зберігання.* Дані можуть зберігаються лише протягом того часу, який необхідний для досягнення мети обробки. Однак, для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей можливе подальше зберігання даних з вжиттям певних заходів, зокрема анонімізацією.

6. *Цілісність і конфіденційність*. Персональні дані повинні бути захищені від несанкціонованого доступу, незаконної обробки, ненавмисної втрати, знищення чи пошкодження.

Ці принципи є основоположними для будь-якого суб'єкта, який оброблятиме персональні дані громадян ЄС, незалежно від місця його знаходження.

GDPR значну увагу приділяє гарантуванню прав суб'єктів персональних даних. Йдеться, перш за все про право особи на періодичний доступ до своїх персональних даних (в тому числі цілі оброблення, період оброблення, логіка та наслідки оброблення на основі профайлінгу). В тому випадку, коли дані є неточними або неповними передбачене права на виправлення персональних даних. За певних обставин, особа може реалізувати «право на забуття» (інакше право на видалення персональних даних) або право на обмеження опрацювання. Окремо варто зазначити право на мобільність, тобто права отримати свої дані у структурованому, загальновживаному і машиночитаному форматі та без обмежень передати їх іншому контролеру персональних даних. GDPR передбачає, за певних умов, право особи заперечувати проти оброблення своїх персональних даних.

Таким чином, існує необхідність інтеграції цих правових положень як в законодавство України, так і у відповідну юридичну практику.

Йдеться не лише про відповідні зміни законодавства, але й про запровадження відповідних процедур, які б дозволяли здійснювати належний контроль за їхнім виконанням, а так само притягати відповідних суб'єктів до юридичної відповідальності. Зокрема, необхідно передбачити можливість реалізації згаданих вище прав особи щодо персональних даних, передбачених в GDPR (право на доступ до даних, право на виправлення, право на забуття тощо).

Хоча законодавство про захист персональних даних прийняте і працює, однак механізм контролю за його дотриманням далекий від ідеалу, оскільки цей обов'язок покладено на Уповноваженого Верховної Ради з прав людини, а його можливості обмежені. GDPR передбачає, що контроль за дотриманням прав людини здійснює незалежний орган влади. Уповноважений з прав людини загалом відповідає вимозі незалежності. Разом із тим, Законопроєкт пропонує створення такого колективного незалежного органу. Однак, на нашу думку, під час воєнного стану створення такого органу зіштовхується як з нестачею коштів для його функціонування, так і з незалежністю.

Важливим питанням залишається поступовість імплементації GDPR в законодавство про захист персональних даних. Йдеться перш за все про те, що норми нового закону мали б набувати чинності кількома етапами: 1) запровадження стандартів GDPR та добровільне виконання цих норм; 2) створення відповідного незалежного органу захисту персональних даних та розробка ним методичних рекомендацій щодо виконання стандартів GDPR (як м'яке право); 3) надання консультацій цим органом; 4) притягнення до відповідальності порушників, при цьому розміри штрафів мають підніматися поступово – від символічного розміру штрафу до такого, коли він почне сприйматися серйозно тими суб'єктами, які зобов'язані забезпечити гарантування безпеки персональних даних.

Це пов'язане як з тим, що в умовах воєнного стану неможливо здійснити належне створення нового незалежного органу, так і з тим, що призначення великих штрафів може створити корупціогенну ситуацію, коли буде простіше заплатити хабар особі, що перевірятиме дотримання норм законодавства, аніж забезпечити виконання стандартів GDPR. Можна також в цьому відношенні пригадати ситуацію з ліквідованою Державною службою України з питань захисту персональних даних, яку навряд чи можна було вважати незалежним органом, оскільки вона підпорядковувалася Кабінету міністрів України. Безпосередньо перед тим, як мали бути набути чинності високі штрафи цей орган виявився паралізованим надмірним обсягом кореспонденції, яку всі надсилали в останній момент для того, щоб уникнути штрафів, в якій окрім повідомлень про ведення реєстрів персональних даних нерідко містилися самі персональні дані, оскільки контролери персональних даних погано розуміли, яку саме інформацію слід надавати.

Це однак жодною мірою не означає, що існує можливість відкласти прийняття закону, який би запроваджував стандарти GDPR в українську правову систему. Однак питання запровадження нового незалежного органу і суворих штрафів повинно здійснюватися поступово.

Варто зазначити, що йдеться перш за все не про тих контролерів персональних даних, які безпосередньо працюють з ЄС, оскільки в країнах ЄС вони можуть підлягати набагато серйознішим штрафам, в тому числі за порушення принципів обробки персональних даних, як це передбачено в статті 5(2)

GDPR. Так, у «Справі Google LLC» французький орган з захисту персональних даних (CNIL) за скаргами приватних позивачів (суб'єктів даних) наклав штраф у розмірі 50 млн євро за невиконання зобов'язання щодо прозорості та поінформованості і нездатність отримати належну правову основу для обробки даних. Штраф у справі «Google LLC» є набільшим штрафом GDPR із досі накладених; та у справі «Deutsche Wohnen SE» німецький орган з захисту персональних даних наклав штраф у розмірі 14,5 млн євро за неможливість встановити систему зберігання даних, яка б могла видалити дані, які вже не потрібні для цілей обробки. Оскільки порушник намагався виправити порушення і орган з захисту персональних даних не зміг довести, що порушення призвело до витоку чи іншого несанкціонованого розголошення остаточна сума була знижена від попередньої [9, с. 11].

Висновки. Вирішення проблем правового регулювання персональних даних в Україні задля забезпечення стандартів Європейського Союзу передбачає необхідність комплексного підходу. Йдеться не лише про прийняття нового законодавства та створення незалежного спеціалізованого органу захисту персональних даних, але й про розвиток та поширення освітніх програм у цій сфері. Крім цього вважаємо за необхідне створення системи інформаційно-консультаційної підтримки контролерів обробки персональних даних, яке включало б як розроблення відповідного методичного забезпечення з боку органу захисту персональних даних, так і правників як науковців, так і практиків. Вважаємо, що запровадження поступового підняття штрафів за порушення норм законодавства про захист персональних даних буде більш ефективним, аніж одноразове встановлення надмірно високих штрафів.

Література:

1. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**.** Regulation (EU) 2016/679. The European Parliament and of the Council. 27 April 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
2. Врублевська-Місюна К.М., Тичина В.П. Міжнародно-правові стандарти захисту інформації про особу. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2022. Випуск 74: частина 2. С. 149–154.
3. European Commission. (2017). EU – U.S. Privacy Shield. First annual Joint Review. Article 29 Data Protection Working Party. 17/EN WP 255. 28 November 2017. URL: https://ec. europa.eu/newsroom/just/redirection/document/48782
4. Єсімов С., Сопільник Р., Ковалів М. Скриньковський Р. Гарантії прав людини та громадянина при забезпеченні інформаційної безпеки. *Traektoriâ Nauki = Path of Science.* 2018. Vol. 4. № 5. С. 1008–1016. URL: http://dspace.lvduvs.edu.ua/handle/1234567890/4
5. Проект Закону про захист персональних даних. № 8153 від 25.10.2022. URL: https://itd.rada.gov.ua/ billInfo/Bills/ Card/40707.
6. Похиленко І.С. Правове регулювання захисту персональних даних/ *Юридичний вісник*. № 4 (69), 2023. С. 94–99. URL: https://repositary.knuba.edu.ua/server/api/core/bitstreams/c8d1205c81c6-4eb9-b57d-e5b6fd363a43/content
7. Шабатура М. М., Салашник Р. О. Аналіз методів захисту персональних даних за українським законодавством і GDPR. Український журнал інформаційних технологій. 2021, т. 3, № 2. С. 51–57. https://doi.org/10.23939/ujit2021.02.051
8. Skrypnyk, R. Problems in ensuring the proper implementation of personal data processing for journalistic purposes in the Ukrainian and European Union law. *SOCRATES Rīgas Stradiņa universitātes Juridiskās fakultātes elektroniskais juridisko zinātnisko rakstu žurnāls / SOCRATES Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law*. 2023. № 3. P. 52–59. http://dx.doi.org/10.25143/socr.27.2023.3.52-59
9. Аналіз законодавства про захист персональних даних України. підготовлений АО «Саєнко Харенко». 14 вересня 2020. URL: https://ecpl.com.ua/wp-content/uploads/2020/09/UKR_09142020_CEP_Finalnyy-zvit.pdf

Topolevskyi R. Features of Personal Data Regulation in Ukraine in the Context of European Union Standards

Summary. The article analyzes the peculiarities of personal data regulation in Ukraine in the context of compliance with the standards of the European Union (EU). It highlights that the protection of personal data is a fundamental aspect of human rights in the conditions of the information society and digital economy. The implementation of GDPR (General Data Protection Regulation) standards has become a key challenge for adapting Ukrainian legislation to European norms, driven by the processes of European integration.

The study examines the core principles of personal data processing outlined in GDPR, including legality, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. Emphasis is placed on the rights of data subjects, such as the right to access, rectification, erasure ("right to be forgotten"), restriction of processing, and data portability.

The article thoroughly explores the challenges faced by the Ukrainian legal system in implementing GDPR. A major obstacle is the absence of an independent body responsible for monitoring compliance with personal data protection standards, which is a fundamental GDPR requirement. Currently, these functions are delegated to the Ukrainian Parliament Commissioner for Human Rights, whose capacities are limited both financially and functionally.

Another significant issue is the limited financial and human resources required to implement new standards. Many businesses, particularly small and medium-sized enterprises, are unprepared for the substantial costs associated with ensuring GDPR compliance, such as implementing technical and organizational measures, hiring responsible individuals, and establishing new data processing procedures.

There is a low level of awareness among businesses and the public regarding GDPR requirements. The article highlights the necessity of large-scale information campaigns aimed at raising public awareness of rights in the field of personal data protection.

The importance of training specialists capable of performing the functions of data protection officers is emphasized. It is recommended to introduce an information support system, including consultations, methodological material development, and practical advice for businesses on integrating European standards.

The author proposes a phased implementation of GDPR, involving legislative changes, gradual increases in fines for non-compliance, and the creation of a consultation support system for data controllers. The necessity of harmonizing Ukrainian legislation with EU standards is stressed to enhance citizens' legal protection.

The integration of GDPR norms into Ukraine's legal system is emphasized as a tool for ensuring transparency, data security, and compliance with international standards.

Key words: personal data protection, GDPR, Ukraine, information rights, data subject rights.