ПРИНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

ШЕВЧУК Олександр Олександрович - кандидат юридичних наук, асистент кафедри міжнародного права Навчально-наукового інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

УДК 341.171
ORCID: 0009-0009-7697-2950
DOI: https://doi.org/10.32782/NP.2024.1.35

18 грудня 2015 року Комітет постійних представників у Європейському Союзі (КПП) затвердив текст, узгоджений з Європейським Парламентом щодо реформи захисту персональних даних у Європейському Союзі і вже 14 квітня 2016 року Європейський Парламент схвалив узгоджений текст Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року «Про захист фізичних осіб стосовно обробки особистих даних і про вільне переміщення таких даних», скасувавши попередню Директиву 95/46/ЄС про захист даних 1995 року [1]. Регламенту (ЄС) 2016/679 набрав чинності після дворічного перехідного періоду і вступив у силу в травні 2018 року.

Прийняття Регламенту (ЄС) 2016/679 свідчить про новий підхід ЄС до захисту основних прав та свобод осіб, зокрема тих, що стосуються захисту приватного життя, включаючи право на захист персональних даних та надання особам більшого контролю над своїми персональними даними і зробить їх більш захищеними в світі соціальних мереж, онлайн-банкінгу та грошових переказів.

Особливого значення тема захисту персональних даних набуває для України. Договір про асоціацію між Україною та Європейським Союзом вимагає приведення законодавства України у відповідність до європейських стандартів, що стосується також сфери захисту персональних даних. Гармонізація українського законодавства до європейських стандартів у сфері захисту персональних даних шляхом імплементації Регламенту (ЄС) 2016/679 є одним із ключових завдань України відповідно до пункту 11 Плану заходів з виконання Угоди про асоціацію, затвердженого Постановою Кабінету Міністрів України від 25 жовтня 2017 р. № 1106.

Метою цієї статті є аналіз принципів обробки персональних даних відповідно до Регламенту (ЄС) 2016/679 та їх ключовий влив на формування будь-якої системи захисту і обробки персональних даних.

Методологічна основа дослідження базується переважно на загальнонаукових і спеціально-юридичних методах, підходах, принципах дослідження. Зокрема, використано діалектичний, феноменологічний, аксіологічний, порівняльно-правовий, формально-логічний, формально-юридичний, модельний, прогностичний та інші методи.

У результаті сформовано низку наукових положень. Регламент (ЄС) 2016/679 підтримує підхід попередньої Директиви 95/46, визначаючи принципи (законність, чесність та прозорість, обмеження обробки персональних даних метою, мінімізація даних, обмеження зберігання персональних даних в часі, цілісність та конфіденційність, точність, підзвітність), які слід дотримуватися в будь-якому контексті обробки персональних даних. Проте, Регламент (ЄС) 2016/679 розширює та конкретизує положення стосовно деяких принципів обробки персональних даних, зокрема, принципів прозорості та мінімізації даних, а також вимога щодо конфіденційності даних тепер чітко визначені як принципи захисту даних.

Ключові слова: Європейський Союз, Україна, захист персональних даних, обробка персональних даних, принципи захисту персональних даних, Директива 95/46/ЄС, Регламент (ЄС) 2016/679.

Постановка проблеми

Розділом ІІІ Угоди про асоціацію передбачається співробітництво між Україною та ЄС у сфері юстиції, свободи та безпеки. Згідно зі статтею 15 Угоди про асоціацію, «Україна та Європейський Союз погодились співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи».

Для інтеграції України до Єдиного цифрового ринку Європейського Союзу важливим є максимальне наближення положень національного законодавства до європейських вимог у сфері захисту персональних даних.

Гармонізація українського законодавства до європейських стандартів у сфері захисту персональних даних відбувається шляхом імплементації Регламенту (ЄС) 2016/679 і передбачена пунктом 11 Плану заходів з виконання Угоди про асоціацію. У цьому контексті варто наголосити, що основою для формування будь-якої системи захисту і обробки персональних даних на національному рівні є належне нормативне закріплення і дотримання принципів обробки персональних даних передбачених Регламентом (ЄС) 2016/679.

Крім того, Україна є стороною Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108). У травні 2018 року Рада Європи прийняла Протокол CETS № 223, яким було внесено зміни до Конвенції 108. Модернізована Конвенція 108+ враховує більшість викликів, спричинених розвитком інформаційних і комунікаційних технологій та посилює вимоги щодо її імплементації. Таким чином, перед Україною постало питання ратифікації вказаного Протоколу, та приведенням законодавства у відповідність до вимог оновленої Конвенції 108+.

Аналіз останніх досліджень і публікацій

Теоретичною основою для цієї статті є наукові розробки вітчизняних та зарубіжних учених. Зпоміж робіт вітчизняних науковців, які досліджували особливості правового регулювання захисту персональних даних у Європейському Союзі слід виділити праці таких учених: Л. Олексюк, Ю. Деркаченко, В. Брижко, В. Пилипчук, О. Баранов, К. Мельник, В. Венгер, І. Городиський та М. Бем.

Серед зарубіжних учених, які акцентують свою увагу на питаннях захисту персональних даних слід згадати таких дослідників, як: С. Уорен, Л. Брендіс, Т. Хікман, Д. Габель, А. Маєрс, Д. Футтер, Р. Хеймес та інші.

Проте, сучасний науковий доробок свідчить про необхідність продовження вивчення, комплексного аналізу і дослідження принципів обробки персональних даних.

Метою цієї статті є аналіз принципів обробки персональних даних відповідно до Регламенту (ЄС) 2016/679 та їх ключовий влив на формування будь-якої системи захисту і обробки персональних даних.

Методологічна основа дослідження базується переважно на загальнонаукових і спеціально-юридичних методах, підходах, принципах дослідження. Зокрема, використано діалектичний, феноменологічний, аксіологічний, порівняльно-правовий, формально-логічний, формально- юридичний, модельний, прогностичний та інші методи.

Виклад основного матеріалу

Регламент (ЄС) 2016/679 має на меті встановити єдині правила щодо захисту персональних для всіх держав-членів ЄС задля зменшення юридичної роздробленості, складності та невизначеності, що існували між державами-членами відповідно до Директиви про захист даних 95/46, а також зміцнити права суб'єктів даних у цифровому середовищі, задля підвищення рівня контролю осіб над своїми персональними даними. Крім того, зміни в законодавстві ЄС, пов'язані з прийняттям Регламенту (ЄС) 2016/679, значно спрощують роботу бізнесу та транснаціональним компаніям, що знаходяться на території Європейського Союзу.

Важливо також підкреслити, що Регламент ЄС 2016/679 має екстериторіальну дію і застосовується до всіх суб'єктів, які обро-

бляють персональні дані резидентів і громадян ЄС, незалежно від їх юрисдикції.

Дія Регламенту ЄС 2016/679 вже поширюється на українські компанії, якщо:

- Компанія здійснює діяльність у ЄС (постачання товарів, виконання робіт, надання послуг резидентам ЄС); або
- У компанії є працівники - громадяни чи резиденти ЄС; або
- Компанія має представництво в ЄС; або
- Компанія використовує хмарні системи, сервери розташовані в ЄС; або
- Компанія здійснює моніторинг діяльності своїх клієнтів та покупців у ЄС (наприклад, маркетингові дослідження).

Тому в окремих випадках українські компанії також повинні забезпечити, щоб вони мали інфраструктуру та технічні можливості для безпечної передачі та обробки персональних даних і дотримуватись положень Регламенту (ЄС) 2016/679 щодо принципів обробки персональних даних у ЄС.

Для більш глибокого розуміння природи походження та практичного застосування положень Регламенту (ЄС) 2016/679 важливо проаналізувати принципи обробки персональних даних.

На думку Девіда Футтера, обсяг та зміст принципів, зазначених у Регламенті (ЄС) 2016/679, аналогічний тим, що наведено в Директиві 95/46/ЄС. Зміни включають вимогу щодо прозорості та принципу підзвітності. Останній матиме суттєвий вплив, оскільки це вимагатиме, щоб компанії демонстрували відповідність Регламенту (ЄС) 2016/679 на основі конкретної документації. Наприклад, організаціям, що впроваджують нові IT-інструменти, потрібно буде проводити внутрішні перевірки відповідності Регламенту (ЄС) 2016/679, так звані «compliance check» [2]. Перевірка охоплює ключові сфери захисту персональних даних відповідно до Регламенту (ЄС) 2016/679.

Основні принципи захисту персональних даних встановлені в статті 5 Регламенту (ЄС) 2016/679.

Принцип перший: законність, чесність та прозорість

Обробка персональних даних має відбуватися на законних підставах, чесно та прозоро по відношенню до особи, яка є їхнім об'єктом [3]. Регламент (ЄС) 2016/679 прямо встановлює, що дані повинні оброблятися «прозоро», що включає надання суб'єктам даних адекватної інформації про те, як обробляються їх дані [4].

Як відзначають спеціалісти компанії VinciWorks, яка є провідним постачальником програмного забезпечення в галузі відповідності та управління ризиками: «способи збирання даних змінюються». Вони звертають увагу, що традиційно дані збирали безпосередньо від фізичних осіб, наприклад, коли вони заповнювали відповідну форму. Наразі все частіше організація з обробки даних використовує дані, що безпосередньо не були надані особою. Спостерігається це шляхом відстеження людей у мережі Інтернет або за допомогою смарт-пристроїв; висновок з використанням алгоритмів для аналізу різноманітних даних, таких як соціальні медіа, дані про місцезнаходження та записи покупок, з метою аналізу осіб, наприклад, з точки зору їх кредитного ризику, стану здоров'я або придатності для роботи [5]. Організації необхідно забезпечити повну прозорість щодо того, як вона використовує дані, а також повинна гарантувати, щоб дані використовувались лише тим способом, який очікують особи, які надали згоду на обробку їх даних [6].

Принцип другий: обмеження обробки персональних даних

Одним із основних принципів європейського регулювання захисту даних є принцип обмеження обробки персональних даних метою. Персональні дані підлягають збиранню для чітко визначених та законних цілей та не мають оброблятися в спосіб, що не відповідає таким цілям [7]. Обробка «для іншої мети» вимагає подальшого юридичного дозволу чи згоди. Як зазначає Деббі Хейвуд, єдиним винятком з цієї вимоги є те, коли «інша мета» є «сумісною» з початковою метою [8].

Принцип обмеження обробки персональних даних метою полягає в тому, щоб запропонувати збалансований підхід, спрямований на узгодження необхідності, передбачуваності та правової визначеності стосовно цілей обробки, з одного боку, і прагматичної потреби в певній гнучкості [9].

Детлев Гебель [84] підкреслює, що особисті дані, зібрані з однією метою (наприклад, виконання договору страхування), не можуть використовуватися для нової, несумісної цілі (наприклад, створення бази даних з інформацією про суб'єкти страхування, щоб встановити більш точно ціну на свої послуги).

Необхідно погодитися з ідеями, висловленими Деббі Хейвуд та Детлевом Гебелем щодо того, що персональні дані, які зібрані з однією метою, не повинні використовуватись з іншою та вважаємо, що принцип обмеження обробки персональних даних метою призначений для встановлення межі, у якій персональні дані, що зібрані з конкретною метою, можуть бути оброблені і використані для подальшого застосування.

Також варто зазначити, що подальша обробка персональних даних для цілей архівації в інтересах суспільства, наукових та історичних досліджень або статистичних цілей не може вважатися такою, що не відповідає первинним цілям обробки. Однак при цьому виконуються положення статті 89(1) Регламенту (ЄС) 2016/679, яка визначає запобіжники та винятки щодо обробки в таких цілях [10].

Принцип третій: мінімізація обсягу даних

Персональні дані мають відповідати меті, з якою вони обробляються, та обмежуватися тими, які є необхідними для досягнення такої мети. Іншими словами, для обробки слід зберігати не більше мінімальної кількості даних [11].

Компанія з обробки даних повинна переконатися, що збирає достатньо даних, щоб досягти своєї мети, але не більше, ніж потрібно [8]. Компаніям доведеться ретельно переглянути свої операції з обробки даних, щоб розглянути питання про те, чи не обробляє вона будь-які особисті дані, які не є необхідними щодо досягнення поставлених цілей [5].

Згідно з поглядами Тіма Хікмана та Детлева Гебеля [5], компанії повинні гарантувати, що вони обробляють лише мінімальну кількість персональних даних, необхідних для досягнення своїх законних цілей обробки. Наприклад, у зв'язку з онлайн-послугою компанія не повинна збирати особисті дані (наприклад, контактні дані), які не є обов'язково необхідними у зв'язку з наданням цієї послуги, якщо суб'єкт даних сам не вирішить надавати ці дані. Це вимагає від багатьох компаній переосмислення своєї діяльності з обробки даних. Кожна компанія повинна уважно вивчити, якою мірою вона потребує внесення змін до існуючої практики збору даних, щоб відповідати обмеженням, встановленим Регламентом (ЄС) 2016/679.

Принцип четвертий: обмеження зберігання персональних даних у часі

Персональні дані підлягають зберіганню у формі, яка уможливлює ідентифікацію суб'єкта таких даних, не довше, ніж це необхідно для цілей, з якими персональні дані обробляються. Це означає, що процес систематичного перегляду повинен проводитись із методичним очищенням баз даних. Персональні дані можуть зберігатися протягом більш тривалого терміну за умови, що вони обробляються тільки для цілей архівації в інтересах суспільства, наукових та історичних досліджень або статистичних цілей, відповідно до положень статті 89(1), та за умови застосування до них відповідних технічних та організаційних заходів [10].

Принцип п'ятий: цілісність і конфіденційність

Персональні дані підлягають обробці, під час якої забезпечується їх належний захист, у тому числі захист від несанкціонованої або незаконної обробки та від випадкової втрати, знищення або пошкодження, за допомогою належних технічних та організаційних заходів [8].

Компанії, які здійснюють обробку даних повинні оцінювати ризик, застосовувати заходи безпеки для відповідних даних і, найважливіше, регулярно перевіряти, чи такі заходи є актуальними та ефективними. Контролери несуть відповідальність за те, щоб особисті дані були захищені як від зовнішніх загроз, так і від внутрішніх [5]. Необхідно використовувати належну технічну систему безпеки для збереження персональних даних [6].

Принцип шостий: точність

Персональні дані повинні бути точними та постійно оновлюватися. Неточні або

застарілі дані слід видаляти або змінювати, а контролери даних повинні виконувати «всі розумні кроки» для дотримання цього принципу [8].

Якщо для обробки неточних даних існують очевидні ризики для суб'єктів даних, контролери несуть відповідальність за прийняття всіх необхідних заходів для забезпечення правильності персональних даних.

Регламент(ЄС) 2016/679 вказує, що видалення або виправлення неточних особистих даних повинно бути здійснено без затримки [12]. Необхідно прийняти обґрунтовані кроки, щоб забезпечити оновлення інформації та змінити її, якщо вона є неточною [6].

Варто наголосити на тому, що коли особа оновлює інформацію, компанія повинна припинити звертатися до особи, використовуючи надані раніше дані. Більше того, організації не повинні просто чекати, коли особи звертаються до них для оновлення своєї інформації, а повинні бути активними в тому, щоб забезпечити правильну інформацію про особу [6].

Принцип сьомий: підзвітність

Контролер даних несе відповідальність за дотримання принципів захисту персональних даних та має бути здатним підтвердити факт їхнього дотримання [10].

Регламент (ЄС) 2016/679 стверджує, що контролери даних повинні мати можливість продемонструвати відповідність іншим принципам захисту персональних даних. Діапазон процесів, які контролери повинні застосовувати для демонстрації відповідності, будуть різними у залежно від складності обробки, але можуть включати:

- оцінку існуючої практики та розробку структури управління конфіденційністю даних, яка може включати призначення в організації співробітника із захисту даних;
- інвентаризацію персональних даних;
- здійснення відповідних повідомлень про конфіденційність;
- використання відповідних організаційних та технічних заходів для забезпечення дотримання принципів захисту даних;
- використання оцінок впливу на конфіденційність;
- створення механізму звітності про порушення [8].

Висновки

Аналіз принципів обробки персональних даних дає можливість стверджувати, що дотримання принципів відіграє ключову роль для забезпечення належного рівня захисту і законної обробки персональних даних.

Принципи обробки персональних даних створюють правову основу, на якій базується вся система правових норм і стандартів щодо гарантування дотримання основоположного права кожної особи на приватність при здійсненні обробки її персональних даних.

Регламент (ЄС) 2016/679 загалом підтримує підхід попередньої Директиви 95/46, визначаючи принципи (законність, чесність та прозорість, обмеження обробки персональних даних метою, мінімізація даних, обмеження зберігання персональних даних в часі, цілісність та конфіденційність, точність, підзвітність), які слід дотримуватися в будь-якому контексті обробки персональних даних. Проте, Регламент (ЄС) 2016/679 розширює та конкретизує положення стосовно деяких принципів обробки персональних даних, зокрема принципів прозорості та мінімізації даних, а також вимога щодо конфіденційності даних тепер чітко визначені як принципи захисту даних.

Література

1. Regulation (EU) 2016/679 of the European Parliament and 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, and repealing Directive 95/46/EC (General Data Protection Regulation) URL: http://eur-lex.europa.eu/eli/reg/2016/679/oj

2. David Futter and Nataline Fleury "The General Data Protection Regulation". URL: https://www.ashurst.com/en/news-and-insights/legal-updates/general-data-protection-regulation/

3. Data protection principles. URL: https://www.twobirds.com/~/media/pdfs/gdpr-

pdfs/21—guide-to-the-gdpr—data-protection-principles.pdf?la=en

4. Arran Brooker Dara protection principles under the General data protection regulation. URL: http://www.cwj.co.uk/site/businessservices/corporatecommercial/Data_Protection_Principles_Under_Data_Protection_Regulation.html

5. Dr. Detlev Gabel, Tim Hickman. Chapter 6: Data protection principles – Unlocking the EU General data protection regulation. URL: https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection

6. The VinciWorks Blog. The 8 principles of the Data protection act 1998 and how GDRP will affect them. URL: http://vinciworks.com/blog/8-principles-data-protection-act-gdpr-guide/

7. Taylor and Francis Online. The new European Union General Regulation on Data Protection and the legal consequences for institutions URL: http://www.tandfonline.com/doi/full/10.1080/23753234.2016.1240912

8. Debbie Heywood, Mgr. Karin Pomaizlova "The data protection principles under the General Data Protection Regulation". URL: https://globaldatahub.taylorwessing.com/article/the-data-protection-principles-under-the-general-data-protection-regulation

9. Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

10. Data protection principles. URL: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/21—guide-to-the-gdpr—data-protection-principles.pdf?la=en

11. Concultancy.uk. Six privacy principles for General Data Protection Regulation compliance. URL: http://www.consultancy.uk/news/13487/six-privacy-principles-for-general-data-protection-regulation-compliance

12. Dr. Detlev Gabel, Tim Hickman Chapter 8: Consent Unlocking the EU General Data Protection Regulation. URL: https://www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation

Oleksandr Shevchuk, *PhD in Law assistant of the chair of international law of the Taras Shevchenko National University of Kyiv, Educational and Scientific Institute of International Relations*

DATA PROTECTION PRINCIPLES

Effective protection of personal data throughout the Union requires enhanced and detailed rights of data subjects and data protection principles. Regulation (EU) 2016/679 must ensure a consistent and high level of protection of individuals and elimination of obstacles to the movement of personal data. The level of protection of human rights and freedoms in connection with the processing of such data should be equal for all Member States. Regulation (EU) 2016/679 is an important step for strengthening the fundamental rights of citizens in the digital age and facilitating business by simplifying the rules for companies in the digital single market.

The topic of personal data protection is of particular importance for Ukraine. The Association Agreement between Ukraine and the European Union requires bringing the legislation of Ukraine in line with European standards, which also applies to personal data protection. One of the key tasks of Ukraine is harmonisation of Ukrainian legislation to European standards in the field of personal data protection through the implementation of the Regulation (EU) 2016/679 in accordance with paragraph 11 of the Action Plan No. 1106 for the implementation of the Association Agreement approved by the Cabinet of Ministers of Ukraine dated October 25, 2017.

Keywords: European Union, Ukraine, personal data protection, personal data processing, principles of personal data protection, Directive 95/46/EC, Regulation (EU) 2016/679.