

## ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЗА НАЦІОНАЛЬНИМ ТА ЄВРОПЕЙСЬКИМ ЗАКОНОДАВСТВОМ

### COMPARATIVE CHARACTERISTICS OF PERSONAL DATA PROTECTION UNDER NATIONAL AND EUROPEAN LEGISLATION

Дяковський О.С., к.ю.н.,  
докторант кафедри публічного права  
Державний податковий університет

У статті проаналізовано захист персональних даних за європейським та національним підходом їх відмінності та спільні риси. Визначено, що захист персональних даних в Європейському Союзі є одним із ключових факторів дотримання прав людини, оскільки порушення даного захисту може негативно впливати на суб'єкта персональних даних тому належне збирання, зберігання, використання та подальше видалення даних відіграє важливу роль.

У зв'язку із необхідністю удосконалення відповідного захисту персональних даних було прийнято Регламент Європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року 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, далі за текстом GDPR або Регламент Європейського союзу) котрий здійснює регулювання даних по сьогоднішній час, що свідчить про актуальність даного дослідження. Здійснено опрацювання будови GDPR його статей регулювання, органів нагляду та їх повноважень у сфері захисту персональних даних.

Спеціальний національний закон у сфері захисту персональних даних визначає межі використання персональних даних, закріплює загальні та спеціальні вимоги до обробки персональних даних, права суб'єктів персональних даних та інші положення у даній сфері. Серед прав суб'єктів персональних даних передбачено видалення даних на підставі рішення суду.

Відтак, для того щоб видалити персональні дані суб'єкту даних необхідно звернутися до суду та отримати відповідне судове рішення котре повинно набрати законної сили, що вказує про наявність часового проміжку порушеного права та утворення негативних наслідків для суб'єкта персональних даних.

У статті також досліджено наявність регулювання права на забуття як критерію захисту персональних даних, здійснено дослідження порівняння відповідальності у формі накладення штрафів за порушення законодавства у даній сфері. Встановлено, що за європейським підходом відповідальність є більшою та може застосовуватися у формі суми штрафу або у процентному співвідношенні залежності від обставин справи та ступеня допущеного порушення.

**Ключові слова:** захист персональних даних, право на забуття, накладення штрафу, стандарт, наглядовий орган, оператор, контролер, відповідальність за порушення, рішення, регламент, видалення, знищення даних.

The article analyzes the protection of personal data according to the European and national approach, their differences and common features. It has been determined that the protection of personal data in the European Union is one of the key factors in the observance of human rights, since the violation of this protection can have a negative impact on the subject of personal data, therefore, the proper collection, storage, use and further reduction of data play an important role.

In connection with the need to improve the corresponding protection of personal data, the Regulation of the European Parliament and the Council (EU) 2016/679 of April 27, 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data was adopted, and on repeal of Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as GDPR or European Union Regulation), which regulates data to date, which indicates the relevance of this study.

A study of the structure of the GDPR, its regulatory articles, supervisory bodies and their powers in the field of personal data protection was carried out.

A special national law in the field of personal data protection defines the limits of the use of personal data, establishes general and special requirements for the processing of personal data, the rights of personal data subjects and other provisions in this field. Among the rights of personal data subjects is the deletion of data based on a court decision.

Therefore, in order to delete the personal data of the data subject, it is necessary to apply to the court and obtain an appropriate court decision, which must enter into force, indicating the existence of a time interval of the violated right and the formation of negative consequences for the subject of personal data.

The article also examines the existence of regulation of the right to be forgotten as a criterion for the protection of personal data, a study of the comparison of responsibility in the form of imposing fines for violations of the law in the successful field is carried out. It was established that according to the European approach, the responsibility is greater and can be applied in the form of a fine or as a percentage, depending on the circumstances of the case and the degree of the committed violation.

**Key words:** protection of personal data, right to be forgotten, imposition of a fine, standard, supervisory body, operator, controller, responsibility for violation, decision, regulation, deletion, destruction of data.

**Постановка проблеми.** Проаналізувавши чинне законодавство у сфері захисту персональних даних було виявлено відсутність нормативного закріплення права на забуття, крім того в процесі видалення або знищення персональних даних виникають складнощі, що вказує про необхідність здійснення порівняння та дослідження даної проблеми із чинним законодавством Європейського союзу та органами контролю у даній сфері. Вказані обставини зумовлюють дослідження даної проблематики.

**Аналіз останніх досліджень.** Аналіз правового регулювання персональних даних у ЄС знайшов своє відображення у чисельних наукових доробках вчених. Відтак, І. Сопілко [8, с. 75] вивчав міжнародно-правовий досвід захисту персональних даних, актуальні проблеми захисту персональних даних досліджував О. Бринцев [6, с. 45].

Дослідження права на забуття у правовій системі Європейського союзу здійснювалося П. Сухорильським [7, с. 91] та іншими. Разом з тим, аналіз права захисту персональних даних за складовою ЄС та національною шляхом порівняння вченими не було достатньо досліджено.

**Формулювання цілей статті.** Метою дослідження є аналіз захисту персональних даних за національним та європейським законодавством, з урахуванням практики Суду ЄС та наукових напрацювань у даній сфері.

**Виклад основного матеріалу.** Варто зазначити, що регулювання персональних даних в Європейському союзі здійснюється на підставі Регламенту Європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року 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) [1].

В свою чергу регламент здійснює своє застосування в Європейському союзі з 25 травня 2018 року, містить 11 глав котрі включають: загальні положення, принципи, права суб'єкта даних, контролера та оператора, передавання персональних даних до третіх країн або міжнародних організацій, незалежні наглядові органи, співпрацю і послідовність, засоби правового захисту, відповідальність і санкції, положення про спеціальні ситуації опрацювання, делеговані акти та імплементаційні акти, прикінцеві положення та 99 статей регулювання.

Регламент Європейського Союзу зазначає серед іншого наступні терміни контролера та оператора:

– контролер означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних; якщо цілі та засоби такого опрацювання визначаються законодавством Союзу чи держави-члена, контролер або спеціальні критерії його призначення може бути передбачено законодавством Союзу чи держави-члена;

– оператор означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, який опрацює персональні дані від імені контролера [1].

З метою функціонування роботи контролера та оператора в частині опрацювання персональних даних призначають співробітника з питань захисту даних котрий наділений завданнями щодо інформування та надання рекомендацій контролеру та оператору щодо їхніх обов'язків, здійснювати моніторинг відповідно до цього Регламенту, співпрацювати із наглядовим органом, надавати необхідні консультації.

Проаналізувавши Регламент ЄС можна зазначити, що документ містить норми щодо регулювання діяльності Європейської ради із захисту даних. Даний орган має завдання у сфері консультування, надання рекомендацій, настанов, сприяє обміном знаннями, здійснює проведення навчання з метою застосування Регламенту та спрямований нагляд за захистом персональних даних та в своїй діяльності є незалежний.

В своїй будові складається з голови одного наглядового органу кожної держави-члена та Європейського інспектора із захисту даних або їхніх відповідних представників, представлення ради здійснюється головою для роботи ради передбачений секретаріат.

З метою реалізації положень регламенту кожна держава-член на законодавчому рівні повинна забезпечити заснування кожного наглядового органу із визначенням умов та правила призначення та строк повноважень наглядового органу.

Для виконання регламенту наглядовий орган серед іншого уповноважений розглядати скарги подані суб'єктом даних та проводити розслідування із правом застосування накладення адміністративних штрафів.

Додатково захист даних здійснюється Європейським інспектором із захисту даних котрий відповідає за контроль дотримання та забезпечення застосування положень цього Регламенту і Регламенту (ЄС) 2018/1725 стосовно захисту фундаментальних прав і свобод фізичних осіб у зв'язку з опрацюванням оперативних персональних даних Євроюстом, і надання Євроюсту і суб'єктам даних поради щодо всіх питань стосовно опрацювання оперативних персональних даних [2].

Порівнюючи захист персональних даних за національним та європейським законодавством варто зазначити, що Регламент Європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року 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) [1] був при-

йнятий 27 квітня 2016 року та введений в дію з 25 травня 2018 року в той час національний Закон України «Про захист персональних даних» був прийнятий 01 червня 2010 року та набрав чинності 01 січня 2011 року [3].

Дані обставини вказують, що Регламент має ширше регулювання та права суб'єктів персональних даних в силу розвитку правовідносин у даній сфері та часу прийняття документу. Серед даних відмінностей котре впливає на захист персональних даних є закріплення права на забуття персональних даних.

Право на забуття (право бути забутим, англ. right to be forgotten) – право людини, що дозволяє їй вимагати за певних умов видалення своїх особових даних із загального доступу через пошукові системи, тобто посилань на ті дані, які, на її думку, можуть завдати їй шкоди [9].

В той час Європейський суд з прав людини при здійсненні правосуддя та розгляді справ підтвердив наявність права на забуття, зокрема це підтверджується рішенням суду в справі № 57292/16 HURBAIN v. Belgium котра розглядалась щодо заявника – власника щоденної газети «Le Soir», яким його зобов'язали знеособити дані статті в електронному архіві із згадкою повного імені водія, який у 1994 році був притягнутий до відповідальності за ДТП, у результаті якої потерпілий загинув. Таке рішення було обгрунтовано правом особи на забуття [5].

Право на забуття закріплене ст. 17 Регламенту Європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року 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) [1].

Поряд з цим національне законодавство в своїй побудові не містить права на забуття. Суб'єкт персональних даних серед іншого має право: пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних, пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними, звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду, а також видалення або знищення персональних даних можливо у відповідності до ст. 15 Закону України «Про захист персональних даних» на підставі судового рішення котре набрало законної сили в частині видалення або знищення персональних даних [3].

З системного аналізу вказаної вище ст. 15 Закону ми можемо спостерігати формулювання судового рішення, що означає умови застосування судочинства та судового процесу, оскільки судовий процес характеризується наявністю стадій: відкриття провадження (спрошеного чи загального), призначення справи та розгляд по суті, дослідження доказів, судові дебати та прийняття судового рішення. Таким чином прийняття рішення є завершальною стадією судового процесу, що вказує про наявність необхідного часу для розгляду справи.

Також умовою видалення або знищення персональних даних є набрання законної сили даного судового рішення, що також вказує про необхідність часу для його набрання, що складає 30 днів, або розгляду відповідної апеляційної скарги та прийняття рішення щодо даної скарги.

За період розгляду судових спорів в частині видалення або знищення персональних даних для суб'єкта персональних даних відносно якого відбуваються судові спори можуть наставити негативні наслідки тому реалізація права на забуття може зменшити наявність порушених прав та судових спорів.

Проте чинний Закон України «Про захист персональних даних» [3] не передбачає правової концепції на забуття персональних даних, що вказує про необхідність внесення відповідних змін до національного законодавства в даній частині, що впливає на захист персональних даних.

Варто також погодитися із позицією Сухорильського П., що право бути забутим передбачає можливість особи вимагати у певних обставинах знищення даних про неї, передусім у мережах інтернет – ресурсів. Зазначене право також відоме під назвами «право на забуття», «право на стирання», «право забувати» тощо [7, с. 91].

Досліджуючи порівняння захисту персональних даних варто зазначити, що в національному законодавстві та в законодавстві Європейського союзу передбачена як спільна риса адміністративна відповідальність у вигляді штрафу за порушення законодавства у даній сфері як критерій захисту даних.

Проте, відмінною є сума стягнення адміністративного штрафу, що накладається на суб'єкта правопорушення та механізм накладення стягнення. За європейським стандартам передбачених Регламентом адміністративні штрафи застосовуються в грошовому еквіваленті або процентному співвідношенні.

Отже за порушення GDPR, поширюється застосування адміністративних штрафів сумою до 10000000 євро або, у випадку підприємства, до 2% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою, також за більш складні правопорушення передбачена відповідальність адміністративного штрафу сумою до 20000000 євро або, у випадку підприємства, до 4% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою [1].

За національним підходом як приклад за порушення в частині неповідомлення або несвочасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей – тягнуть за собою накладення штрафу.

За судовою практикою призначення штрафу відбувається в розмірі, що складає 5 100 грн., на користь держави. Приблизно за змістом міра адміністративної відповідальності у вигляді штрафу передбачена за невиконання законних вимог Уповноваженого Верховної Ради України з прав людини.

Таким чином за європейським підходом порівняно з національним спостерігається підвищена відповідаль-

ність контролера та оператора та інших суб'єктів за порушення та невідповідність стандартам GDPR котра може збільшуватися в залежності від допущених порушень.

Відповідно до розділу III ст. 15 Угоди про асоціацію між Україною та Європейським Союзом зазначено, що сторони домовились співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи [4].

У зв'язку із набранням чинності Регламенту національне законодавство в сфері персональних даних повинно мати відповідні зміни та доповнення з метою адаптації до європейських вимог та стандартів це зумовлено також із вступом України до Європейського союзу з метою отримання його членства.

Даній позиції дотримується Бринцев О.В. котрий зазначив, що потреба у приведенні законодавства з питань захисту персональних даних до європейських вимог обумовлена також Угодою про асоціацію між Україною та Європейським союзом [6, с. 45].

**Висновки.** В ході дослідження захисту персональних даних в Європейському Союзі можна прийти до висновку, що відповідне регулювання здійснюється на підставі Регламенту GDPR котрий встановлює правила та умови збирання, використання персональних даних також містить більшу межу відповідальності у грошовому або процентному співвідношенні за порушення роботи з даними порівняно з національними штрафами.

Варто зазначити, що реалізація прав залежить від законодавчо закріпленої норми тому якщо національний закон передбачає можливість вчинення дії відповідний ризик вчинення або не вчинення залежить від суб'єкта котрий здійснює дану дію особисто так і через відповідні органи державної влади.

Закріплення в національному законодавстві права на забуття та підвищення рівня адміністративних стягнень у формі штрафів надасть можливість зменшити порушення у даній сфері.

Перспективи подальших досліджень. Розвиток європейського законодавства та практика його застосування у сфері персональних даних свідчать про необхідність здійснення досліджень даної категорії прав.

#### ЛІТЕРАТУРА

1. 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): Регламент Європейського парламенту і Ради від 27 квітня 2016 року № 2016/679 Законодавство Європейського Союзу: URL: [https://zakon.rada.gov.ua/laws/show/984\\_008-16#n207](https://zakon.rada.gov.ua/laws/show/984_008-16#n207) (дата звернення 25.08.2023).
2. Про Агентство Європейського Союзу з питань співпраці у сфері кримінального правосуддя (Євроюст), та про заміну і скасування Рішення Ради 2002/187/ЮВС) : Регламент Європейського парламенту і Ради від 14.11.2018 № 2018/1727 URL: [https://zakon.rada.gov.ua/laws/show/984\\_014-18#Text](https://zakon.rada.gov.ua/laws/show/984_014-18#Text) (дата звернення: 25.08.2023).
3. Про захист персональних даних : Закон України від 13.04.2012 № 4651-VI. *Верховна Рада України. Законодавство України.* URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення 25.08.2023).
4. Угода про асоціацію між Україною з однієї сторони та Європейським Союзом, Європейським співтовариством з атомної енергетики і їхніми державами членами, з іншої сторони: Міжнародний документ від 27.06.2014 р.№ 984\_011. URL: [https://zakon.rada.gov.ua/laws/show/984\\_011#n132](https://zakon.rada.gov.ua/laws/show/984_011#n132) (дата звернення 25.08.2023).
5. Case of Hurbain v. Belgium (Requête no 57292/16) 22 juin 2021/ European Court of Human Rights HUDOC [Ukrainian Translation] summary by the Supreme Court of Ukraine URL: <https://hudoc.echr.coe.int/ukr?i=001-210467>.
6. Бринцев О.В. Актуальні проблеми захисту персональних даних в Україні. Збірник наукових праць НДІ ПЗІР НАПрН. 2021 № 5. С. 45.
7. Сухорильський П. Право бути забутим у правовій системі Європейського Союзу: реалії, проблеми та перспективи. Наука міжнародного права на рубежі століть. Тенденції розвитку та трансформації : спеціальне видання наукових статей / за наук. ред. В. Релецького. Львів : ЛНУ імені Івана Франка, 2016. С. 90–101.
8. Сопілко І. Міжнародно-правовий досвід захисту персональних даних. *Юридичний вісник.* 2014. № 4. С. 70–75.
9. Право на забуття. Вікіпедія. URL: <https://uk.wikipedia.org/wiki>.