УДК 341.174

***О. О. Шевчук***
*аспірант кафедри порівняльного і європейського права*
*Інституту міжнародних відносин*
*Київського національного університету імені Тараса Шевченка*

## ДОГОВІРНІ МЕХАНІЗМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЄВРОПЕЙСЬКОМУ СОЮЗІ

Стрімкий технологічний розвиток і глобалізація призводять до нових труднощів у захисті персональних даних. Зріс обмін персональними даними між публічними та приватними суб'єктами, зокрема фізичними особами, асоціаціями та підприємствами на рівні Європейського Союзу. Масштаби збирання та спільного використання персональних даних суттєво зросли. Для того, щоб забезпечити послідовний рівень захисту персональних даних фізичних осіб у всьому Союзі та запобігти виникненню розбіжностей, що ускладнюють вільний рух персональних даних у межах внутрішнього ринку, необхідно, щоб Регламент забезпечував правову визначеність і прозорість для суб'єктів господарювання, зокрема мікропідприємств, малих і середніх підприємств; надавав фізичним особам у всіх державах-членах однаковий рівень прав і обов'язків, що мають юридичну силу, і обов'язків для операторів і процесорів, забезпечував постійний моніторинг опрацювань персональних даних і належні санкції у всіх державах-членах, а також дієву співпрацю між наглядовими органами різних держав-членів.

Стаття ставить за мету виробити чітке розуміння щодо ефективності наявних договірних механізмів захисту персональних даних у Європейському Союзі та запропонувати шляхи їх удосконалення.

Питанню функціонування договірних механізмів захисту персональних даних у Європейському Союзі (далі – ЄС) присвячені численні праці вітчизняних і європейських науковців. Дослідженню окремих питань приділяли увагу такі фахівці та вчені, як М. Лаббок, Н. Флірі, А. Марошч, П. Г. Мехіа, М. Бунда, Д. Гебель, Т. Хікман.

Регламент Європейського Парламенту і Ради ЄС 2016/679 (далі – Регламент) про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних був затверджений 27 квітня 2016 р. і набуде чинності 25 травня 2018 р. Регламент замінює Директиву 95/46/ЄС щодо захисту даних у зв'язку з обробкою персональних даних і вільним обігом цих даних.

Метою Регламенту є забезпечити сталий і високий рівень захисту фізичних осіб і усунути перешкоди для потоків персональних даних у межах Союзу; рівень захисту прав і свобод фізичних осіб у сфері опрацювання таких даних повинен бути однаковим у всіх державах-членах [1]. Необхідно забезпечувати послідовне й одноманітне застосування правил щодо захисту фундаментальних прав і свобод фізичних осіб у сфері опрацювання персональних даних у всьому Союзі [2].

Захист, передбачений цим Регламентом у зв'язку з опрацюванням персональних даних, поширюється на фізичних осіб незалежно від їхнього громадянства чи місця проживання [3]. Цей Регламент не поширюється на опрацювання персональних даних, що стосуються юридичних осіб і підприємств, заснованих як юридичні особи, які містять інформацію про найменування, організаційно-правову форму юридичної особи й контактну інформацію юридичної особи [4].

Термін «персональні дані» як у Директиві, так і в Регламенті визначається як «будь-яка інформація, що стосується ідентифікованої фізичної особи або особи, яку можна ідентифікувати («суб'єкт даних»)».

На відміну від Директиви, яка не містить положень щодо порушення даних, Регламент містить визначення терміна «порушення персональних даних» і встановлює обов'язок інформування як наглядових органів, так і осіб, які є суб'єктом таких даних. Згідно з Регламентом порушенням персональних даних є «порушення захисту, наслідком якого є випадкове або протизаконне знищення, втрата, зміна, несанкціоновані розголошення або доступ до персональних даних, які передаються, зберігаються або обробляються іншим чином» [5].

Порівняно з Директивою 95/46/ЄС Регламент накладає на процесорів і операторів даних суворіші обмеження в аспекті захисту даних, одночасно конкретизуючи вимоги щодо належних стандартів такого захисту. Регламент також уперше впроваджує спеціальні норми, які регламентують порядок повідомлення про порушення даних.

За визначенням Регламенту оператором є «фізична або юридична особа, орган державної влади, відомство чи інший орган, який самостійно або спільно з іншими визначає мету й засоби оброблення персональних даних». Отже, оператор – це організація, що приймає рішення щодо заходів з оброблення, незалежно від того, чи здійснює вона таке оброблення сама.

Стаття 24 покладає на оператора відповідальність за забезпечення дотримання вимог

Регламенту під час оброблення. Оператор має «вживати належних технічних і організаційних заходів» для забезпечення не лише дотримання вимог, але й здатності продемонструвати заходи, які ним уживаються.

На оператора покладається також особлива відповідальність за такі дії:

– здійснення аналізу впливу на захист даних, коли застосовуваний вид оброблення «може призвести до виникнення суттєвої загрози правам і свободам осіб», і впровадження належних технічних запобіжників;

– гарантування захисту прав суб'єкта даних, наприклад, шляхом видалення даних, виконання вимог інформування й повідомлення, а також ведення документування діяльності з оброблення;

– виконання обов'язків перед наглядовим органом (інформування про порушення даних і консультування перед початком оброблення).

Регламент дозволяє оператору підтверджувати факт виконання ним вимог Регламенту шляхом дотримання кодексу поведінки й стандартів сертифікації, схвалених наглядовим органом у відповідних державах-членах.

Для того, щоб мати можливість підтвердити відповідність цьому Регламенту, оператор повинен ухвалити норми внутрішньої політики та забезпечити застосування інструментів, що відповідають, зокрема, принципам захисту даних за призначенням і захисту даних за замовчуванням [6].

В аспекті всіх заходів з оброблення оператор має забезпечити за замовчуванням оброблення персональних даних у спосіб, що гарантує особам захист прав, якими вони наділені на підставі Регламенту.

Це вимагає від оператора таких дій:

а) під час визначення способу оброблення даних і під час самого оброблення вживати належних технічних і організаційних заходів (зокрема псевдонімізацію) із метою забезпечення наявності необхідних запобіжників на виконання вимог законодавства;

б) уживати належних технічних і організаційних заходів для забезпечення за замовчуванням оброблення лише тих персональних даних, які є необхідними для досягнення певної мети.

Оператор зобов'язаний мати документальні записи всіх категорій заходів з оброблення, які здійснюються від його імені, зокрема документацію про будь-яку передачу таких даних за кордон, а також про технічні чи організаційні заходи із забезпечення належного рівня захисту. Окрім того, під час виконання цих завдань оператор має співпрацювати з контрольним органом, якому вони підпорядковані.

Регламент розмежовує відповідальність і обов'язки оператора й процесора даних, зобов'язуючи оператора залучати лише тих процесорів, які забезпечують «достатні гарантії впровадження належних технічних і організаційних заходів» на виконання вимог Регламенту й для захисту прав суб'єктів даних. Процесор також має вжити всіх заходів, що передбачені нормами статті 32 Регламенту, яка визначає стандарти безпечного оброблення.

Згідно з положеннями статті 32, подібними до статті 17 Директиви, оператор і процесор зобов'язані «впроваджувати належні технічні й організаційні заходи», ураховуючи «останні досягнення технічного прогресу», а також «характер, межі, обставини й цілі обробки, ризики й загрози для прав і свобод фізичних осіб». Однак на відміну від Директиви Регламент дає конкретні поради щодо видів захисних заходів, які можуть розглядатися, «виходячи з наявних ризиків», зокрема такі:

– псевдонімізація й шифрування персональних даних;

– здатність до постійного забезпечення конфіденційності, цілісності, доступності й стійкості систем і послуг з оброблення;

– здатність до своєчасного відновлення доступу до персональних даних у разі аварії на обладнанні або технічної несправності;

– процедура регулярного тестування, оцінки й аналізу ефективності технічних і організаційних заходів для забезпечення захисту обробки.

Оператор і процесор, які дотримуються або затвердженого кодексу поведінки, або стандартів затвердженого механізму сертифікації, як зазначено в статтях 40 і 42, можуть використовувати ці інструменти як доказ дотримання стандартів безпеки, установлених Регламентом.

Оператор несе відповідальність за дії процесора, якого він обирає, а також за дотримання принципів оброблення персональних даних, визначених Регламентом.

Згідно з визначенням Регламенту процесором є «фізична або юридична особа, орган державної влади, відомство чи інший орган, який обробляє персональні дані від імені оператора». Інакше кажучи, у той час як оператор є особою, яка приймає рішення щодо здійснення оброблення, процесор є будь-якою особою, найнятою оператором для здійснення оброблення. Процесора, який діє як оператор або виходить за межі своїх повноважень, наданих йому оператором, Регламент розглядає як оператора щодо такого оброблення, і на нього поширюються положення, які застосовуються до оператора.

Обираючи процесора, оператор має залучати лише тих процесорів, які надають достатні гарантії своєї здатності вжити належних технічних і організаційних заходів, необхідних для виконання вимог Регламенту. Наприклад, оператор, який застосовує юридично зобов'язальні корпоративні правила або положення типового договору як належний засіб захисту даних під

час їхньої передачі за кордон, має обтяжувати обов'язком дотримання таких правил або умов також залученого ним процесора.

Оператор також не має нехтувати здійсненням аналізу впливу на захист даних до обрання процесора. Положення Преамбули визнають такий аналіз доцільним в будь-якому разі, але особливо важливим у разі роботи сторін із конфіденційними персональними даними. Якщо оператор бажає залучити саме цього процесора, найліпшим рішенням буде попередня консультація з відповідним наглядовим органом із захисту даних.

Оцінювання впливу на захист даних вимагається в таких випадках:

– систематичне та масштабне оцінювання персональних аспектів, що стосуються фізичних осіб, яке ґрунтується на автоматизованому опрацюванні (зокрема профайлінгу[1]) та на якому ґрунтуються рішення, що мають юридичні наслідки відносно фізичної особи чи подібним чином істотно впливають на фізичну особу;

– широкомасштабне опрацювання спеціальних категорій даних, указаних у статті 9 (1), і персональних даних про судимості й кримінальні злочини, що вказані в статті 10;

– систематичний і широкомасштабний моніторинг зони, що знаходиться в публічному доступі [7].

Ключовою відмінністю Регламенту від Директиви є покладання прямих обов'язків на процесора. Опрацювання процесором має регулюватися договором або іншим нормативно-правовим актом згідно із законодавством ЄС або держави-члена, пов'язувати зобов'язальними відносинами процесора відносно оператора та встановлювати предмет і тривалість опрацювання, характер і цілі опрацювання, тип персональних даних і категорії суб'єктів даних, обов'язки та права оператора.

Як і оператор, процесор може підтвердити факт виконання вимог шляхом дотримання кодексу поведінки чи стандартів механізму сертифікації або шляхом застосування типових положень, затверджених Єврокомісією.

Також упроваджується ланцюгова система повідомлення процесором про випадки порушення персональних даних: процесор інформує оператора про порушення даних, оброблених без необґрунтованих затримок, після чого оператор інформує відповідний контрольний орган. За можливості таке повідомлення надається не пізніше ніж протягом 72 годин після отримання інформації про порушення, а в разі виникнення суттєвої загрози для суб'єкта даних оператор без необґрунтованих затримок інформує про порушення даних суб'єкта таких даних.

У разі порушення персональних даних оператор даних зобов'язаний інформувати наглядовий орган, «уповноважений згідно зі статтею 55», який скоріше за все (з огляду на положення статті 56(1)) є наглядовим органом держави-члена, в якій знаходиться головне або єдине підприємство оператора. Повідомлення надається «без необґрунтованих затримок і за можливості не пізніше ніж протягом 72 годин після отримання інформації про порушення». Якщо протягом 72 годин повідомлення не надане, оператор мусить надати «умотивоване пояснення» затримки.

Стаття 33(1) містить ключовий виняток з обов'язку інформування наглядового органу: повідомлення не є обов'язковим, якщо «порушення персональних даних, імовірно, не призведе до виникнення загрози порушення прав і свобод фізичних осіб».

Повідомлення на адресу наглядового органу має містити принаймні такі відомості: опис характеру порушення персональних даних, зокрема кількості й категорій суб'єктів даних, в яких містяться персональні дані; контактну інформацію особи, відповідальної за захист даних; «описання ймовірних наслідків порушення персональних даних»; викладення пропозицій оператора з виправлення порушення, зокрема будь-яких заходів із пом'якшення негативних наслідків. Якщо вся інформація не може бути надана одразу, вона може надаватися поетапно.

Коли процесор даних стикається з порушенням персональних даних, він має інформувати оператора, але окрім цього відповідно до положень Регламенту не несе будь-яких зобов'язань із повідомлення чи інформування. У разі встановлення оператором факту, що порушення персональних даних «імовірно, призведе до виникнення суттєвої загрози правам і свободам осіб», він зобов'язаний повідомити про факт порушення персональних даних також суб'єктів даних. Згідно з вимогами статті 34 це здійснюється «без необґрунтованих затримок».

Регламент передбачає винятки із цього обов'язку інформування суб'єктів даних у таких обставинах: 1) оператор задіяв відповідні технічні й організаційні інструменти захисту, і такі інструменти було застосовано до персональних даних, на які вплинули порушення персональних даних, зокрема ті, що унеможливлюють розуміння персональних даних будь-якою особою, яка не має дозволу на доступ до них (шифрування); 2) після порушення персональних даних оператор вживає заходів із «забезпечення неможливості настання несприятливих наслідків і суттєвої загрози правам і свободам

[1] Профайлінг означає будь-яку форму автоматизованого опрацювання персональних даних, що складається з використання персональних даних для оцінювання окремих персональних аспектів, що стосуються фізичної особи, зокрема для аналізу або прогнозування аспектів, що стосуються продуктивності суб'єкта даних на роботі, для аналізу економічної ситуації, здоров'я, особистих переваг, інтересів, надійності, поведінки, місцезнаходження або пересування.

суб'єктів даних»; 3) у разі «необхідності докладання надмірних зусиль» для інформування суб'єктів даних надається право застосування альтернативних способів інформування.

У разі інформування оператором відповідного наглядового органу про порушення персональних даних й його повноваження з інформування суб'єктів даних обмежуються здатністю державного наглядового органу, згідно з положеннями статті 34(4), висунути вимогу такого інформування або дійти висновку про відсутність у цьому потреби з огляду на обставини [8].

Регламент вимагає від оператора й процесора впровадження належних технічних і організаційних заходів для забезпечення пропорційності рівня захисту персональних даних наявним ризикам, наприклад, застосовуючи псевдонімізацію й шифрування, забезпечуючи конфіденційність систем оброблення й застосування процедур із регулярної перевірки ефективності цих заходів.

Оператор несе відповідальність за шкоду, завдану обробленням «у порушення» вимог Регламенту. Процесор, з іншого боку, несе відповідальність «лише за невиконання обов'язків, спеціально покладених Регламентом на процесора, або за дії, що виходять за межі законних інструкцій оператора чи суперечать їм». Інакше кажучи, особи, які висувають процесору претензії на підставі Регламенту, окрім факту шкоди й загального недотримання вимог мають довести ще одну обставину – порушення процесором спеціальних вимог закону або своїх договірних зобов'язань. Після встановлення факту невиконання вимог на оператора й процесора покладається тягар доказування відсутності в завданій шкоді їхньої провини.

Коли оператор і процесор спільно беруть участь в одному судовому процесі, відповідальність за шкоду може бути розподілена між ними відповідно до міри відповідальності кожного за таку шкоду за умови, що суб'єкт даних отримує відшкодування в повному обсязі [9].

Ефективний захист персональних даних на всій території ЄС вимагає посилення та деталізації прав суб'єктів даних, а також обов'язків тих, хто відповідає за оброблення персональних даних; наділення їх відповідними повноваженнями для моніторингу та забезпечення дотримання правил із захисту персональних даних, застосування санкцій до порушників у державах-членах. Щодо опрацювання персональних даних, необхідного для дотримання встановлених законом зобов'язань, виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера, держави-члени повинні мати можливість зберігати чи задіювати положення національного законодавства для більш детального уточнення застосування правил цього Регламенту.

### *Література*

1. Частина 46 Преамбули Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eur-lex.europa.eu/eli/reg/2016/679/oj.
2. Частина 47 Преамбули Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eur-lex.europa.eu/eli/reg/2016/679/oj.
3. Частина 60 Преамбули Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eur-lex.europa.eu/eli/reg/2016/679/oj.
4. Частина 61 Преамбули Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eur-lex.europa.eu/eli/reg/2016/679/oj.
5. Chapter 11: Obligations of processors – Unlocking the EU General Data Protection Regulation. URL: https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection.
6. Частина 292 Преамбули Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eur-lex.europa.eu/eli/reg/2016/679/oj.
7. Стаття 35 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eur-lex.europa.eu/eli/reg/2016/679/oj.
8. Top 10 operational impacts of the GDPR: Part 1 – data security and breach notification. URL: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/.
9. Top 10 operational impacts of the GDPR: Part 7 – Vendor Management.URL: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-7-vendor-management/.

### Анотація

***Шевчук О. О.*** **Договірні механізми захисту персональних даних у Європейському Союзі.** – Стаття.

Стаття присвячена структурному аналізу договірних механізмів захисту персональних даних у Європейському Союзі. Наводяться ключові відмінності щодо механізмів захисту персональних даних за Директивою 95/46/ЄС і Регламентом (ЄС) 2016/679. Пропонується розглянути основні обов'язки та межі відповідальності оператора й процесора щодо захисту персональних даних під час їх оброблення. Розглядаються особливості повідомлення про випадки порушення системи захисту персональних даних відповідно до Регламенту.

*Ключові слова:* оператор, процесор, аналіз впливу, захист даних за призначенням, захист даних за замовчуванням, псевдонімізація, шифрування, Європейський Союз.

## Аннотация

***Шевчук А. А.*** **Договорные механизмы защиты персональных данных в Европейском Союзе.** – Статья.

Статья посвящена структурному анализу договорных механизмов защиты персональных данных в Европейском Союзе. Приводятся ключевые отличия механизмов защиты персональных данных согласно Директиве 95/46/ЕС и Регламенту (ЕС) 2016/679. Предлагается рассмотреть основные обязанности и пределы ответственности оператора и процессора по защите персональных данных при их обработке. Рассматриваются особенности оповещения о случаях нарушения защиты персональных данных согласно Регламенту.

*Ключевые слова:* оператор, процессор, анализ влияния, защита данных по назначению, защита данных по умолчанию, псевдонимизация, шифрование, Европейский Союз.



## Summary

***Shevchuk O. O.*** **Treaty mechanisms for the protection of personal data in the European Union.** – Article.

The paper is devoted to the structural analysis of contractual mechanisms of the protection of personal data in the European Union. Provides the key differences regarding the mechanisms of protection of personal data under Directive 95/46 / EC and Regulation (EC) 2016/679. It is proposed to consider the main responsibilities and limits of the responsibility of the operator and processor of the protection of personal data within processing. Features of informing about violations of personal data in accordance with the Regulations are noted.

*Key words:* operator, processor, impact analysis, data protection by design, data protection by default, pseudonymisation, encryption, European Union.