

## МІЖНАРОДНЕ ПРАВО

УДК 340.134 (477+061.1 ЄС): 351.822.009.6

DOI 10.30970/vir.2019.46.0.10373

### ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ПРАВІ ЄВРОПЕЙСЬКОГО СОЮЗУ

**Ірина Яворська, Михайло Микісвич**

*Львівський національний університет імені Івана Франка,  
вул. Університетська, 1, м. Львів, Україна, 79000, тел. (032)239-41-99,  
e-mail: irynayavorska@hotmail.com, mmedulaw@gmail.com*

Досліджено засади формування політики Європейського Союзу у сфері захисту персональних даних, визначено поняття таких даних, правові засади захисту персональних даних в рамках ЄС, основні положення Загального регламенту (англ. General Data Protection Regulation, GDPR 2016/679) щодо захисту персональних даних усіх осіб в межах Європейського Союзу та Європейської економічної зони, який охоплює широкий спектр питань, пов'язаних з захистом персональних даних.

У статті досліджено сферу застосування Регламенту щодо захисту персональних даних, визначено винятки із сфери його застосування.

Враховуючи приналежність дітей до особливої категорії володільців персональних даних також зазначено, що саме захисту персональних даних дітей Регламент приділяє особливу увагу. Діти можуть бути менш обізнаними про відповідні ризики, наслідки та гарантії, а також про свої права щодо опрацювання персональних даних.

Окремо розглядаються принципи захисту персональних даних, що деталізуються у Регламенті, такі як принцип прозорості, «право бути забутим».

У статті аналізується допустимий порядок збирання персональних даних, їх обробки. В цьому контексті важливе значення відводиться процедурі надання згоди особи на обробку її персональних даних. Істотну роль відіграють форми вираження надання згоди на обробку персональних даних особи.

**Ключові слова:** персональні дані; захист персональних даних; обробка персональних даних; ідентифікація особи.

25 травня 2018 р. набрав чинності Регламент Європейського Парламенту та Ради ЄС щодо захисту персональних даних. Необхідність прийняття акту викликана зростанням обміну персональними даними між публічними та приватними суб'єктами, в тому числі фізичними особами, асоціаціями та підприємствами на рівні Союзу. Також стрімкий технологічний розвиток та

незворотні глобалізаційні процеси обумовлюють зростання масштабів збирання та обміну персональними даними приватних фізичних осіб.

Право на приватність закріплене ще у Загальній декларації прав людини і громадянина 1948 року. Право на недоторканість приватного життя людини з кожним роком набуває особливого значення. Конвенція 1950 року про захист прав людини та основних свобод передбачає право кожного на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Конвенція № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28.01.81 р. спрямована на захист фізичних осіб від зловживань, вчинених під час обробки персональних даних. Її завданням є забезпечення врегулювання транскордонного переміщення персональних даних [2].

В Загальній декларації прав людини і громадянина проголошено, що ніхто не може піддаватися свавільному втручанням в особисте та сімейне життя.

Так, одним із перших міжнародних документів на території Європейського Союзу, що містив пряме визначення терміну «персональні дані» була Конвенція «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28 січня 1981 року (дата ратифікації Україною: 06.07.2010 року, дата набрання чинності для України: 01.01.2011 року). У Главі 1 даної конвенції (стаття 2, пункт «а») міститься наступне визначення:

«Персональні дані – це будь-яка інформація, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною».

Наступним документом, що нормативно закріпив визначення цього поняття була Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року (далі «Директива 95/46/ЄС»). Так, у статті 2 Глави 1 закріплено: «персональні дані означають будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити («суб'єкт даних»). Особою, яку можна встановити, є така, яка може бути встановленою прямо чи непрямо, зокрема, за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості».

Відповідно до права Європейського Союзу, національні органи держав-членів закликають до співпраці та обміну персональними даними для надання їм можливості виконувати свої обов'язки або завдання від імені органу в іншій державі-члені. Таким чином, сферою застосування Регламенту є не лише ЄС, він також поширює свою дію на експорт даних за межі ЄС, проте його не застосовують в ході діяльності, що виходить за межі дії права Союзу.

Регламент регулює не лише порядок обробки персональних даних, але і процедуру їх переміщення та спрямовує свою дію на забезпечення високого рівня захисту персональних даних. Він поширює свою дію на опрацювання персональних даних повністю чи частково із застосуванням автоматизованих та до опрацювання персональних даних із застосуванням неавтоматизованих засобів, які формують частину картотеки або призначені для внесення до картотеки.

Цей Регламент не застосовують до питань захисту фундаментальних прав і свобод або вільного потоку персональних даних, пов'язаних з діяльністю поза межами законодавства Союзу, наприклад, діяльністю щодо національної безпеки. Цей Регламент не застосовують до опрацювання персональних даних державами-членами у ході діяльності щодо спільної зовнішньої та безпекової політики Союзу [1].

Також сфера застосування регламенту не поширюється на доопрацювання персональних даних фізичною особою у ході суто особистої або побутової діяльності, а, отже, жодним чином не пов'язаної з професійною або комерційною діяльністю. Особисту або побутову діяльність може становити ведення кореспонденції та зберігання адрес, або ведення соціальних мереж і онлайн-діяльності, розпочатої у контексті такої діяльності. Проте цей Регламент застосовують до контролерів і операторів, які надають засоби для опрацювання персональних даних для такої особистої або побутової діяльності.

Прийняття Регламенту ґрунтується, як зазначено у ньому, на положеннях Хартії ЄС про основні права та положеннях Договору про функціонування Європейського Союзу [5], якими закріплено право особи на захист своїх персональних даних. Регламент спрямовано на формування простору свободи, безпеки та справедливості, економічного союзу, підтримання добробуту громадян. Метою прийняття регламенту є: гармонізація захисту фундаментальних прав і свобод під час опрацювання даних; забезпечення вільного руху персональних даних між державами-членами.

Фізичні особи, як це закріплено у п. 7 Регламенту повинні мати контроль щодо власних персональних даних. Як зазначено у Регламенті його прийняття також було обумовлено необхідністю забезпечити однакове регулювання в рамках усіх держав-членів ЄС, в однаковій мірі забезпечивши захист персональних даних, що не могло бути виконаним у зв'язку з застосуванням директиви, яка була по-різному гармонізованою у державах членах. Така відмінність у рівнях захисту виникає внаслідок відмінностей в ході імплементації та застосування Директиви 95/46/ЄС [1]. Регламент дозволяє також регулювання національним правом. Так, якщо опрацювання персональних даних здійснюють для відповідності встановленим законом зобов'язанням, для виконання завдання суспільних інтересів або для здійснення офіційних повноважень, покладених на контролера, державам-членам необхідно дозволити мати або вводити положення національного законодавства для більш детального уточнення застосування норм цього Регламенту.

На захист фізичних осіб у зв'язку з опрацюванням персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування за вчинення злочинів або для виконання кримінальних покарань, у тому числі захисту від або запобігання загрозам громадській безпеці та вільному руху таких даних, поширюється застосування спеціального нормативно-правового акта Союзу. Відповідно, цей Регламент не можна застосовувати до опрацювання даних для таких цілей. Проте питання щодо опрацювання персональних даних, яке здійснюють органи публічної влади

згідно з цим Регламентом, у разі їх використання для таких цілей, підлягає врегулюванню уточненим спеціальним нормативно-правовим актом Союзу, зокрема Директивою Європейського Парламенту і Ради (ЄС) 2016/680 (2).

Проте, Регламент не поширює свою дію на діяльність державних органів з розкриття злочинів. Щодо діяльності судових органів, оскільки дія цього Регламенту поширює свою дію на їх діяльність, відповідно до п. 20 Регламенту у законодавстві Союзу або держав-членів можна чітко визначити операції і процедури опрацювання, пов'язані з опрацюванням персональних даних судами та іншими судовими органами. Компетенція наглядових органів не повинна поширюватися на опрацювання персональних даних у ситуаціях, коли суди діють як судові органи, для збереження їхньої незалежності у ході виконання ними судових функцій, у тому числі в процесі вироблення й ухвалення рішень.

Особливу увагу Регламент приділяє захисту персональних даних дітей, оскільки діти потребують особливого захисту в питанні персональних даних, оскільки вони можуть бути менш обізнаними про відповідні ризики, наслідки та гарантії, а також про свої права щодо опрацювання персональних даних.

Регламент враховує усі фундаментальні права та свободи і принципи, визнані у Хартії, як це передбачено в Договорах, зокрема щодо поваги до приватного та сімейного життя, житла та спілкування, захисту персональних даних, свободи думки, совісті та віросповідання, свободи вияву поглядів та свободи інформації, свободи підприємництва, права на дієвий засіб правового захисту та справедливий суд, а також - культурного, релігійного та мовного різноманіття.

Право на захист персональних даних не є абсолютним правом, воно повинно розглядатися у зв'язку з його функцією у суспільстві та бути збалансованим з іншими фундаментальними правами відповідно до принципу пропорційності.

Принципи захисту даних необхідно застосовувати до будь-якої інформації про фізичну особу, яку ідентифіковано чи можна ідентифікувати. Персональні дані із використанням псевдоніму, що можна приписати фізичній особі після використання додаткової інформації, необхідно розглядати як інформацію про фізичну особу, яку можна ідентифікувати.

Запити публічних органів щодо персональних даних повинні бути мотивованими та не впливати на усю картотеку даних. А згода суб'єкта щодо використання даних повинна бути чіткою та однозначною.

Опрацювання персональних даних повинно здійснюватись насамперед з дотриманням принципу прозорості, що передбачає в першу чергу знання особи про те, що її дані обробляють. Особа, чиї дані є предметом опрацювання повинна бути ознайомлена з особою контролера та знати мету збирання даних про неї. Фізичні особи також повинні знати про ризики, пов'язані зі збором даних про них. Дані повинні мати часові рамки для зберігання. Вони повинні бути конфіденційними та їх зберігання повинне забезпечувати унеможливлення доступу інших осіб. На нашу думку важливою є норма, яка передбачає встановлення щонайкоротших строків для зберігання даних. Також суб'єкт вправі мати доступ до його персональних даних та повинен володіти

інформацією у зв'язку з чим зібрані такі дані. Це право також передбачає право на виправлення персональних даних та «право бути забутим». Право «бути забутим» реалізується шляхом повідомлення суб'єктом тримання даних інших осіб, яким такі дані були передані. Це право поширюється також на осіб, що надали їх будучи дітьми.

Регламент також запроваджує принцип законності збирання персональних даних, що передбачає дотримання ряду умов під час їх збирання.

Фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами за допомогою їхніх пристроїв, додатків, інструментів чи протоколів, зокрема IP-адрес, ідентифікаторів «cookie» (реп'яшків) або інших ідентифікаторів, таких як мітки радіочастотної ідентифікації. Це може залишити підказки, які, особливо в поєднанні з унікальними ідентифікаторами та іншою інформацією, отриманою з серверів, можна використати для створення профілів фізичних осіб та їхньої ідентифікації.

Надавана особою згода на використання персональних даних повинна бути чіткою та однозначною. Контролер при цьому повинен забезпечити наявність такої згоди. А сама згода особи на надання даних повинна бути надана добровільно, не внаслідок примусових дій. Суб'єкт даних повинен мати право відкликати свою згоду в будь-який момент. Відкликання згоди не повинно впливати на законність опрацювання, що ґрунтувалося на згоді до її відкликання. Відповідно до ст. 8 Регламенту у сфері пропозиції послуг інформаційного суспільства безпосередньо дитині, опрацювання персональних даних дитини є законним, якщо дитина досягла щонайменше 16 років. Якщо дитина не досягла 16 років, таке опрацювання є законним, лише якщо та тією мірою, коли згоду надано чи її надання санкціоновано носієм батьківської відповідальності щодо дитини.

Відповідно до ст. 15 Регламенту суб'єкт даних вправі отримати від контролера підтвердження факту опрацювання його даних та інформацію щодо періоду зберігання персональних даних. Суб'єкт даних також повинен мати право на виправлення неточних персональних даних та «право бути забутим».

Стаття 28 Регламенту детально визначає повноваження операторів даних. Важливо відзначити, що опрацювання оператором повинен регулювати договір або інший нормативно-правовий акт відповідно до законодавства Союзу або держави-члена, який пов'язує оператора зобов'язальними відносинами з контролером та встановлює предмет та тривалість опрацювання, специфіку і цілі опрацювання, тип персональних даних і категорії суб'єктів даних. Існує також процедура повідомлення суб'єкта даних про порушення захисту персональних даних.

Стаття 40 Регламенту надає право асоціаціям, іншим органам, що представляють категорії контролерів або операторів готувати власні кодекси поведінки з метою уточнення застосування цього Регламенту.

Глава V регулює порядок передавання персональних даних до третіх країн або міжнародних організацій.

З метою моніторингу виконання Регламенту кожна держава-член покладає на один або декілька незалежних публічних органів відповідальність за моніторинг застосування Регламенту (ст. 51 Регламенту). Статтею 68 засновується Європейська рада із захисту даних – «Рада» як орган Союзу, що має правосуб'єктність. Кожен суб'єкт даних має право на відповідний захист відповідно до ст.79 та право на відшкодування шкоди згідно ст. 82 Регламенту.

**Висновки.** 25 травня 2018 року вступив в силу Регламент ЄС № 2016/679 щодо захисту персональних даних. У рамках визначення підходу щодо імплементації зазначеного Регламенту в українське законодавство та за ініціативи Уповноваженої Верховної Ради України з прав людини створено робочу групу, якою напрацьовано пропозиції до змін у національне законодавство. Наразі триває процес вироблення концептуальної позиції щодо часових рамок та обсягу імплементації зазначеного Регламенту [4]. Таким чином, зростання масштабів збирання та обміну персональними даними, їх використання у повсякденному житті повинно гарантувати фізичним та юридичним особам усі необхідні та можливі умови захисту таких даних. В цьому контексті позитивним є перейняття досвіду, запровадженого Регламентом ЄС щодо захисту персональних даних та закріплення відповідних положень у законодавство України.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Регламент Європейського Парламенту та Ради ЄС щодо захисту персональних даних усіх осіб в межах Європейського Союзу та Європейської економічної зони [Електронний ресурс]. – Режим доступу : [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.119.01.0001.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG).
2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних // Офіційний вісник України від 14.01.201. – № 1. – ст. 1994.
3. Загальна декларація прав людини і громадянина 1948 р. // Урядовий кур'єр від 10.12.2018. – № 232.
4. <https://www.kmu.gov.ua/storage/app/media>.
5. Хартія Європейського Союзу про основні права // Хартія Європейського Союзу про основні права // Европейский Союз: основополагающие акты в редакции Лиссабонского договора с комментариями. – Москва : ИНФРА, 2010. – С. 554–570.

*Стаття надійшла до редколегії 10.12.2018*

*Прийнята до друку 20.12.2018*

## PERSONAL DATA PROTECTION IN EU LAW

**Iryna Yavorska, Myhailo Mykievich**

*Ivan Franko National University in Lviv,  
1, Universytetska Str., Lviv, Ukraine, 79000, tel. (032)239-41-99,  
e-mail: irynayavorska@hotmail.com, mmmedulaw@gmail.com*

General information on the protection of personal data within the EU, the General Data Protection Regulation (GDPR 2016/679) on the protection of personal data of all persons within the European Union and the European Economic Area covering a wide range of issues related to personal data protection.

The article outlines the area of application of the GDPR 2016/679 on personal data protection and defines the cases of when it is not applied.

Taking into account the fact that children belong to a separate category of personal data owners, the article stresses the importance of protection of their personal data by this EU regulation. It is emphasized that children might be less aware of the risks, guarantees and consequences of violation of personal data protections, as well as of their rights in terms of personal data protection. The article also focuses on the principles of the personal data protection as defined in the EU regulation, such as the transparency principle or the «right to be forgotten», as well as explains the order of collecting and processing personal data. Procedure of getting permission for the personal data processing is of utmost importance in this regard, and due attention should be paid to the form of consent for the personal data processing.

**Key words:** personal data; protection of personal data; personal data registration; identification of a person.