УДК 343.45

DOI <https://doi.org/10.32844/2618-1258.2019.4-1.17>

ГУКОВА А.Р.

GDPR: ЗАСТОСУВАННЯ СТАНДАРТІВ В УКРАЇНІ

У статті розглянуто забезпечення реалізації права на приватність особи у мережі Інтернет. Статтю присвячено актуальному питанню в сучасному періоді цифрової трансформації – збору та використанню персональних даних. Відповідно до цього, автор розглядає нормативно-правовий акт, ухвалений у 2016 р. Європейським парламентом, – General Data Protection Regulation. Регламент встановлює норми, пов'язані із захистом фізичних осіб щодо обробки персональних даних, і норми, що стосуються вільного переміщення персональних даних. Ознайомлення з GDPR є цікавим через те, що його дія поширюється на будь-які компанії, до цільової аудиторії яких входять громадяни країн-учасниць Європейського Союзу.

У статті проаналізовано стандарти General Data Protection Regulation, доцільність впровадження стандартів GDPR на українському ринку, розглянуто процес адаптації українських компаній щодо обробки персональних даних відповідно до GDPR, вивчено обсяг категорії «персональні дані». Автор розглядає основні принципи, методи GDPR та виокремлює компоненти для трансформації українського бізнесу відповідно до європейських стандартів.

У статті розглянуто приклади та шляхи накладання штрафів за європейським нормативно-правовим актом на українські компанії. Також розглядається функція DPA (Data Protection Authority) на території ЄС. Виокремлено аспекти, за умови наявності яких українські компанії зможуть позиціонувати себе як адаптованими до GDPR. Автор зауважує, що порушенням обробки персональних даних є недотримання правил збирання, опрацювання та зберігання конфіденційної інформації, тому детально розкриває кожен цей процес.

У статті зроблено висновок про неготовність українського ринку до цифрових трансформацій щодо обробки та зберігання персональних даних і необхідність покрокової гармонізації законодавства України відповідно до стандартів GDPR задля забезпечення можливості українському бізнесу надавати послуги, орієнтовані на європейський ринок. Автор називає досі неврегульованим питання щодо обробки інформації, яка збирається через cookies, та звертає увагу на запропонований Європейським парламентом Регламент “ePrivacy Regulation”.

Ключові слова: *персональні дані, стандарти GDPR, конфіденційна інформація, обробка персональних даних, інформаційні технології.*

The article deals with ensuring the exercise of the right to privacy of a person on the Internet. The article deals with the pressing issue in the modern era of digital transformation – the collection and use of personal data. Accordingly, the author is considering a legislative act adopted in 2016 by the European Parliament, the General Data Protection Regulation. The Regulation establishes rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data. Introduction to GDPR is interesting because it extends to any company that is targeted at nationals of EU Member States.

The article analyzes the General Data Protection Regulation standards, the feasibility of implementing GDPR standards in the Ukrainian market, examines the process of adaptation of Ukrainian companies to processing personal data in accordance with GDPR, examines the scope of the category of personal data. The author examines the basic principles, methods of GDPR and identifies components for the transformation of Ukrainian business in accordance with European standards.

The article deals with examples and ways of imposing fines under the European regulatory act on Ukrainian companies. The function of DPA (Data Protection Authority) on the territory of the EU is considered too. The author highlights aspects, due to Ukrainian companies will be able to position themselves as GDPR-compliant. The author notes that a violation of the processing of personal data is a failure to comply with the rules for the collection, processing and storage of confidential information, so it details each process.

The article concludes that the Ukrainian market is unprepared for digital transformations regarding the processing and storage of personal data and the need for step-by-step harmonization of Ukrainian legislation to GDPR standards to enable Ukrainian businesses to provide services focused on the European market. The author calls the issues regarding the processing of information collected through cookies still unsettled and calls attention to the ePrivacy Regulation proposed by the European Parliament.

Key words: *personal data, GDPR standards, confidential information, processing of personal data, information technologies.*

Вступ. У вирі цифрової трансформації, з розвитком інформаційних технологій і діджиталізацією життєвих процесів до переліку об'єктів цивільних правовідносин увійшли персональні дані. Інформація про особу стала валютою соціальних мереж, основним активом більшості компаній та основою найпопулярнішого інструмента маркетингу – таргетингу.

Соціальні мережі, мобільні додатки, поштові сервіси, вебсайти збирають інформацію про своїх користувачів через cookies, після чого ці дані аналізують і систематизують за певними конкретними цільовими групами з метою подальшого продажу цих даних компаніям у комерційних цілях. Відповідно, за безкоштовне користування онлайн-послугами особа самостійно надає згоду на аналіз інформації про себе, обробка якої забезпечує якісну конверсію.

Дедалі частіше постає питання про реалізацію принципу недоторканності приватного життя, зокрема захисту персональних даних у мережі Інтернет.

Міжнародна спільнота вчасно реагує на виклики сьогодення та пропонує рішення у вигляді нормативно-правових актів щодо захисту конфіденційної інформації про особу. Наприклад, у 2016 р. Парламентом Європейського Союзу був ухвалений Загальний регламент захисту даних, і вступив у силу він 26 травня 2018 р. Регламент встановлює норми, пов'язані із захистом фізичних осіб щодо обробки персональних даних, і норми, що стосуються вільного переміщення персональних даних. Важливо зазначити, що норми Регламенту поширюються не лише на європейські компанії, а на всі, що зареєстровані поза межами Європейського Союзу, але здійснюють послуги, орієнтовані на європейський ринок. До компаній, що перебувають під впливом сили норми, належать також гравці українського ринку, діяльність яких пов'язана з наданням послуг особам, які є громадянами країн-учасниць Європейського Союзу. Отже, вивчення змісту General Data Protection Regulation та розгляд процесу впровадження стандартів GDPR на українському ринку є вкрай актуальним і важливим.

Постановка завдання. Завданням роботи є аналіз змісту Загального регламенту захисту даних (англ. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679), аналіз питання про доцільність впровадження стандартів GDPR на українському ринку, формування процесу адаптації українських компаній щодо процесу обробки персональних даних відповідно до стандартів GDPR.

Результати дослідження. Положення Загального регламенту захисту даних визначає «персональні дані» як будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати. У свою чергу, 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 місцезнаходження, онлайн-ідентифікатор, або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи [10, с. 36].

Положення Загального регламенту захисту даних спираються на те, що кожному користувачеві послуг має за замовчуванням гарантуватися максимальна приватність. У Регламенті затверджено спеціальні принципи щодо обробки персональних даних, які покликані забезпечувати реалізацію фундаментальних прав особи, зокрема право на приватність.

Серед таких можна виділити принцип цільового обмеження, згідно з яким збирання даних дозволяється лише для конкретних цілей і забороняється їхнє опрацювання в такий спосіб,

що суперечить цим цілям. Принцип надає право на подальше опрацювання з метою досягнення цілей суспільних інтересів, наукового чи історичного дослідження або статистичних цілей.

Цікавим є принцип обмеження зберігання, за яким дані можуть бути збережені лише на той термін, протягом якого будуть оброблятися дані, після досягнення мети опрацювання дані мають бути видалені. Окрім вищезгаданих принципів, на рівні із загальними принципами права регламентуються принципи мінімізації даних (опрацювання того обсягу даних, який необхідний для досягнення цілей), точності (систематичне оновлення даних задля унеможливлення викривлення інформації), цілісності і конфіденційності (забезпечення належної безпеки персональних даних) та підзвітності (реалізація принципу покладена на контролера, який несе відповідальність за будь-які операції з персональними даними) [10, с. 42].

Важливим є питання меж законності обробки даних. Щодо цього законодавець затверджує певні обставини, які виступають підставами, щоби вважати опрацювання даних законним. По-перше, обробляти дозволено на підставі наданої згоди суб'єкта на опрацювання своїх даних для спеціальної мети, також у разі виконання контракту для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи, виконання завдання в суспільних інтересах. Регламент встановлює, що заява має бути отримана в письмовій формі, бути зрозумілою та доступною, містити прості та чіткі формулювання. Суб'єкт даних повинен мати право відкликати свою згоду будь-якої миті. До того ж під час отримання персональних даних контролер має надати такі суб'єкту інформацію: контактні дані контролера, цілі опрацювання, користувачів та отримувачів персональних даних.

GDPR виокремлює двох суб'єктів – контролера та обробника. Завданням контролера є визначення цілей і методів обробки даних; у свою чергу, обробник лише здійснює розпорядження контролера. Отже, відповідальність у разі порушення вимог GDPR несе контролер, хоча це не виключає вимоги до обробника запровадити стандарти GDPR.

Якщо розглянути типову модель для українського ринку, то зазвичай європейська компанія виступає контролером, а українська ІТ-компанія виконує замовлення на аутсорсі, тому є обробником. У такому випадку європейський замовник обов'язково має укласти письмовий договір на обробку персональних даних. У разі застосування штрафу через порушення GDPR замовник може звернутися до суду в порядку регресу на підставі укладеного договору та вимагати від компанії-обробника відшкодування частини збитків.

Через ці обставини європейські компанії під час вибору підрядника звертають увагу на імплементацію стандартів GDPR задля унеможливлення виникнення факту порушення законодавства. Отже, GDPR не лише стандартизує та унормовує ринок із надання послуг, що пов'язані з обробкою персональних даних, спонукає компанії на території України трансформуватися, але й змушує компанії ЄС уважно шукати контрагентів.

Розглядаючи питання про гармонізацію законодавства України відповідно до GDPR, слід зазначити, що на Уповноваженого Верховної Ради України з прав людини було покладено обов'язок розроблення законодавства відповідно до нових вимог. Серед нагальних питань постає визначення термінів та умов перехідного періоду. В ЄС цей період тривав 2 роки, за цей час компанії встигли перейти на вдосконалене програмне забезпечення та запровадити нові системи безпеки. Через намір встановити менший строк перехідного періоду є ризик того, що середній бізнес стане занепадати через накладання штрафів.

До того ж у межах Європейського Союзу за додержання стандартів GDPR відповідає Data Protection Authority (DPA), в українських реаліях пропонується покласти такі обов'язки на офіс Уповноваженого Верховної Ради України з прав людини, але інституційно це складно реалізувати через брак кадрів і відсутність матеріально-технічної бази. Науковці вважають, що доцільним буде створення окремого органу з виключною компетенцією та новим штатом спеціалістів.

Розмір покарання, передбачений нормами GDPR, за порушення стандартів є значним, що, у свою чергу, гарантує користувачам надійний захист їхніх персональних даних, з іншого боку, стимулює компанії здійснювати діяльність відповідно до встановлених правил. В українських реаліях із великими штрафами компаніям буде складно адаптуватись до нових вимог, з іншого боку, низькі штрафи перетворюють закон на формальний, адже ніким не буде виконуватись.

Дискусійним питанням є процес стягнення штрафів з українських компаній. Є декілька шляхів. Перший – це укладання спеціальних законів щодо визнання компетенції Data Protection Authority на території України, відповідно до якого DPA здійснюватиме нагляд за дотриманням стандартів і накладатиме штрафи на правопорушників. Другий полягає в процедурі звернення DPA до національних судів задля санкціонування рішень.

Крім того, слід пам'ятати, що Регламент був створений не з метою штрафування, а з метою захисту персональних даних. Відсутність в Україні будь-яких стандартів процесу обробки персональних даних знижує привабливість для інвесторів та іноземних компаній, що, у свою чергу, Отже, постає питання про механізм адаптації методів роботи українських компаній до стандартів GDPR, які орієнтовані на європейський ринок.

По-перше, компанія має проаналізувати перелік тих персональних даних, які нею обробляються, і з'ясувати доцільність впровадження стандартів. Слід узяти до уваги, що до персональних даних належать не лише паспортні дані, індивідуальний податковий номер, але й інформація щодо політичних, ідеологічних поглядів особи, її етнічної належності та генетичних або біологічних відомостей. Отже, запровадження технологій GDPR може стосуватися компаній різних сфер діяльності, зокрема і громадських організацій. Є тенденція на обробку даних громадськими організаціями задля здійснення статистичної діяльності та узагальнення поглядів населення в економічній, політичній і соціальній сферах, формування портрету сучасної особистості. Після обробки дані використовуються для розроблення програм розвитку тієї чи іншої сфери, для розроблення та реалізації політичних компаній.

Регламент поширюється зазвичай на компанії, які надають послуги через вебресурси: сайти, лендинги, сторінки в соціальних мережах. За умовами Регламенту платформи повинні мати декілька версій, обов'язково на одній з мов Європейського Союзу.

Слід зазначити, що порушенням вимог щодо обробки персональних даних вважається порушення безпеки, що призвело до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних. До речі, у разі, якщо правопорушення вчинено фізичною особою підприємцем, до такої особи в разі незначного порушення застосовуються догана. Зважаючи на це, компанія має встановити програмне забезпечення, яке забезпечить надійний захист даних, що обробляються через той чи інший вебресурс, та унеможливить витік інформації.

Обов'язково на вебресурсі має бути налагоджена процедура отримання згоди на обробку конфіденційної інформації. Наприклад, наявність «впливаючого вікна», в якому буде міститися інформація про мету, методи та термін обробки інформації, контактні дані контролера та ознайомлення з можливістю в будь-який час відхилити свою згоду. Отже, особа попередньо отримає повну інформацію щодо цільового призначення використання її даних, що надасть особі право контролю процесу роботи з її даними.

Додатково можна призначити DPA – спеціаліста з питань захисту даних, який володіє експертними знаннями у сфері права та практиці захисту персональних даних. Цей співробітник може виконувати декілька функцій: контролювати дотримання вимог GDPR і сприяти розвитку корпоративної культури щодо обробки персональних даних у компанії.

Доцільним є ведення систематичного звіту щодо осіб, які мають доступ до даних, обсягу та змісту даних, часу обробки та періоду збереження, що зробить процес роботи з даними прозорим і простим.

Додатково спеціалісти радять пройти сертифікацію в інституціях ЄС, ухвалити кодекс поведінки в компанії та політики конфіденційності.

Висновки. У роботі проаналізовано основні положення General Data Protection Regulation, доцільність і необхідність упровадження цих стандартів українськими компаніями та розглянуто процес їхньої адаптації до вимог GDPR, на основі чого можна зробити такі висновки.

Процес діджиталізації відкриває для права безліч нових сфер, які потребують урегулювання суспільних відносин, що виникають у мережі Інтернет, серед них – інститут захисту персональних даних. Регламент встановлює принципи обробки та збереження персональних даних, на опрацювання яких особа свідомо надає згоду. Неврегульованим залишається питання про обробку інформації, яка збирається через cookies, які дають змогу аналізувати політичні погляди особи, її етнічну належність і таке інше, що, у свою чергу, теж належить до персональних даних, але з цього приводу Європейським парламентом розроблений і запропонований до ухвалення Регламент “ePrivacy Regulation”.

Оскільки на законодавчому рівні закріплено курс України на євроінтеграцію, то законодавство України має бути гармонізовано у сфері захисту персональних даних. Очевидним є, що український бізнес не готовий до швидкого переходу на нові стандарти обслуговування через вебресурси. Для запровадження нових технологій знадобиться більше 2-х років, щоби створити контролюючий орган, підготувати кадри, перевести компанії на відповідне програмне забезпечення, що, у свою чергу, тягне великі фінансові розтрати компаній. Незважаючи на це, на мою

думку, покрокове впровадження стандартів GDPR є необхідним для українського ринку, адже процес діджиталізації з часом набиратиме обертів, що ставитиме нові виклики для бізнесу. Щоби залишатися конкурентними та виходити на іноземний ринок, український бізнес має відповідати запитам сучасності.

Список використаних джерел:

1. Бем М., Городинський І., Саттон Г., Родіоненко О. Захист персональних даних: Правове регулювання та практичні аспекти : науково-практичний посібник. Київ : К.І.С., 2015. 220 с.
2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р. URL: http://zakon3.rada.gov.ua/laws/show/994_326.
3. Закон України «Про інформацію» від 2 жовтня 1992 р. N 2657-XIII URL: <http://zakon5.rada.gov.ua/laws/show/2657-12>.
4. Закон України «Про захист персональних даних» від 30 січня 2018 р. 2297-VI URL: <https://zakon.rada.gov.ua/laws/show/2297-17>.
5. Пилипчук В., Брижка В., Баранов О., Мельник К. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / за ред. В. Брижка, В. Пилипчука. Київ : ТОВ «Видавничий дім «АртЕк», 2017. 226 с.
6. Проблеми захисту персональних даних у контексті сучасної комунікації. URL: http://www.visnyk-econom.uzhnu.uz.ua/archive/19_1_2018ua/25.pdf.
7. Рогова О. Захист персональних даних у законодавстві Європейського Союзу. URL: <http://www.kbuapa.kharkov.ua/e-book/tpdu/2011-3/doc/5/05.pdf>.
8. Тищенко К. GDPR – нові виклики для обробників персональних даних. *Юридична газета online*. URL: <http://jur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/gdpr-novi-vikliki-dlya-obrobnykiv-personalnih-danih-v-ukrayini.html>.
9. Уповноважений Верховної Ради з прав людини. Офіційний сайт URL: <http://www.ombudsman.gov.ua/ua/page/zpd>.
10. General Data Protection Regulation. URL: <https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf>.

УДК 347.9

DOI <https://doi.org/10.32844/2618-1258.2019.4-1.18>

ДЕЙНЕКО О.В., ДЯЧЕНКО С.В.

ІМПЕРАТИВНО-ДИСПОЗИТИВНИЙ МЕТОД ЦИВІЛЬНОГО ПРОЦЕСУ ЯК ФОРМА РЕАЛІЗАЦІЇ ПРИНЦИПУ ДИСПОЗИТИВНОСТІ

У статті розглянуто імперативно-диспозитивний метод як форму реалізації принципу диспозитивності в цивільному процесі України. Методи цивільно-процесуального права є особливою категорією, яка не досить досліджена сьогодні. Адже саме цивільно-процесуальне право є унікальним правом, у якому зосереджені як імперативний, так і диспозитивний методи правового регулювання. Так, цивільно-процесуальне право – це насамперед приватне право, у якому учасники захищають свої особисті права й інтереси. Приватним галузям права притаманний саме диспозитивний метод, адже учасники самі вирішують, як їм вчиняти певні дії. Водночас цивільно-процесуальне право є також публічною галуззю права, оскільки одним із його суб'єктів є суд, який є органом державної влади, тому при цьому

© ДЕЙНЕКО О.В. – студентка IV курсу (Навчально-науковий інститут права Університету державної фіскальної служби України)

© ДЯЧЕНКО С.В. – кандидат юридичних наук, доцент, доцент кафедри цивільного права та процесу (Університет державної фіскальної служби України)