МІЖНАРОДНЕ ПРАВО

АСІРЯН С. Р.,
кандидат юридичних наук,
асистент кафедри права
Європейського Союзу
(Національний юридичний університет імені Ярослава Мудрого)

АЛЕКСАНЯН К. А.,
студентка IV курсу
(Інститут прокуратури та кримінальної юстиції Національного юридичного університету імені Ярослава Мудрого)

УДК 347.91/.95
DOI https://doi.org/10.32842/2078-3736/2021.6.43

GDPR ЯК СТАНДАРТ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

У статті проаналізовано особливості Регламенту з захисту персональних даних в Європейському Союзі. Зазначено, що цей Регламент є найсуворішим законом про конфіденційність та безпеку персональних даних фізичних осіб у світі. Незважаючи на те, що він був розроблений і прийнятий в Європейському Союзі, Регламент із захисту персональних даних накладає зобов'язання на організації в будь-якому місці, якщо вони націлені або збирають дані, пов'язані з особами в ЄС. Метою цього Регламенту є функціонування єдиного закону про безпеку даних для всіх держав-членів ЄС, щоб кожній державі-члену не доводилось ухвалювати власні закони про захист даних, а такі нормативно-правові акти були узгоджені в усьому Європейському Союзі. Зокрема, було наведено обов'язкові та рекомендовані GDPR-заходи, які має впроваджувати контролер даних. Крім того, охарактеризовано GDPR-Compliance, а саме політику внутрішнього та зовнішнього документообігу контролера даних, який працює із персональними даними фізичних осіб. Також розкрито умови ухвалення Регламенту з захисту персональних даних, а також попередній нормативно-правовий акт, що захищав персональні дані в ЄС до Регламенту, яким є Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб під час обробки персональних даних і про вільне переміщення таких даних», ухвалена 24 жовтня 1995 р. Крім того, зроблено порівняльний аналіз із іншими нормативно-правовими актами, які діють в інших країнах, зокрема з California Consumer Privacy Act (CCPA), який поширюється на територію штату Каліфорнія в США, Personal Information Protection and Electronic Documents Act (PIPEDA), який діє в Канаді, та Brazilian General Data Protection Law (LGPD), що діє, відповідно, у Бразилії. Розкрито відмінності та схожість цих документів, охарактеризовано територіальну і матеріальну дію, суб'єктів.

Ключові слова: *персональні дані, захист персональних даних, Європейський Союз, GDPR, контролер.*

Asiryan S. R., Aleksanyan K. A. GDPR as a standard for personal data protection in in the European Union

At the beginning of the article, the author analyzed the features of the General Data Protection Reglament (hereinafter – GDPR) in the European Union. It was noted that the GDPR is the toughest privacy and security law of private data of individuals in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The purpose of the GDPR is to impose a uniform data security law on all EU members so that each member state no longer needs to write its own data protection laws and laws are consistent across the entire EU. In particular, mandatory and recommended GDPR measures to be implemented by the data controller were provided. Besides, the author noted the GDPR Compliance, namely the policy of internal and external document management of the data controller who works with personal data. Further, the conditions for the adoption of this Regulation were mentioned. The author mentioned the previous legal act that protected personal data in the EU before the GDPR. It was Directive 95/46/ EU of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 24 October 1995.In addition, a comparative analysis was made with other data protection laws in other countries. They are the California Consumer Privacy Act (CCPA), which applies to the state of California in the United States, Personal Information Protection and Electronic Documents Act (PIPEDA), which operates in Canada, and the Brazilian General Data Protection Law (LGPD), which operates in Brazil, respectively. It was noted about the differences and similarities of these documents, about their territorial and material effect, and the subjects.

Key words: *personal data, personal data protection, European Union, GDPR, controller.*

Вступ. Регламент із захисту персональних даних (далі – Регламент) є найсуворішим законом про конфіденційність та безпеку персональних даних фізичних осіб у світі. Він встановлює низку прав, якими наділений суб'єкт персональних даних. Документ розрізняє контролера та процесора даних. Так, контролером виступає фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних. Процесором (оператором) є фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який опрацьовує персональні дані від імені контролера [1]. Крім того, у Регламенті чітко визначено поняття «персональні дані», такими даними може бути будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати. Крім того, встановлений також порядок опрацювання спеціальних (чутливих) категорій персональних даних. Загальним правилом визначена заборона на опрацювання таких категорій інформації, проте окреслено винятки, наприклад у разі надання згоди на опрацювання таких персональних даних для однієї чи декількох визначених цілей від самого суб'єкта даних або якщо це є необхідним для досягнення цілей суспільного інтересу, цілей наукового чи історичного дослідження або статистичних цілей. Документом передбачено варіювання видів відповідальності: від штрафів у розмірі до 20 млн євро або 4% від щорічного світового обігу компанії (контролера або обробника) до кримінальної відповідальності (залежно від національного законодавства) [2, с. 103].

Незважаючи на те, що Регламент був розроблений і прийнятий в ЄС, він накладає зобов'язання на організації в будь-якому місці, якщо вони націлені або збирають дані, пов'язані з фізичними особами в Європейському Союзі. Метою цього документа є функціонування єдиного закону про безпеку даних для всіх держав-членів ЄС, щоб кожній державі-члену не доводилось ухвалювати власні закони про захист персональних даних, а такі

нормативно-правові акти були узгоджені в усьому ЄС. Регламент був прийнятий 26 квітня 2016 р. і почав діяти 25 травня 2018 р.

Постановка завдання. Прийняття ЄС Регламенту з захисту персональних даних, відомого як GDPR, стало поштовхом для інших країн змінити та удосконалити власне законодавство про захист персональних даних фізичних осіб. Важливим є визначення головних особливостей зазначеного Регламенту, його ролі під час формування політики збереження даних приватних осіб контролером і порівняння його з аналогічними законами у провідних країнах, що також формують світову практику захисту персональних даних та є взірцем для прийняття таких законів в інших країнах.

Результати дослідження. Регламент встановлює обов'язкові та рекомендовані GDPR-заходи, які має впроваджувати контролер даних. Так, до обов'язкових заходів відносять: підготовку оцінювання впливу на захист даних, консультації з органами контролю і нагляду за дотриманням правил у сфері захисту персональних даних, обов'язкове призначення особи, відповідальної за захист персональних даних у компанії (DPO). До необов'язкових, проте рекомендованих заходів належить: складання механізму дій реагування на випадки порушення захисту персональних даних, проведення навчань і тренінгів для персоналу, який залучений до обробки даних клієнтів і користувачів. Крім цього, необхідно також виокремити так званий «GDPR Compliance» – це узгодження політики внутрішнього та зовнішнього документообігу в компанії згідно з вимогами Регламенту. До документів внутрішнього документообігу відносять документи, запровадження яких вимагається від контролера і процесора персональних даних, але не потребує демонстрації суб'єктам персональних даних. Зовнішні документи – ті, які передбачені Регламентом і стосуються суб'єктів персональних даних. До них належать Політика приватності, Cookies Політика, Форма згоди, внутрішня політика щодо відповідей на запити користувачів.

Варто також зазначити, що оскільки цей документ є регламентом, то він є обов'язковим для всіх держав-членів ЄС, його норми є нормами прямої дії. Попереднім документом була Директива 95/46/ЄС Європейського парламенту і Ради «Про захист фізичних осіб під час обробки персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 р. Її особливість полягала в тому, що директива була необов'язковою, не мала імперативного характеру, а встановлювала певні орієнтири, які держави-члени мали закріплювати у своєму законодавстві в такий спосіб, як вважали за потрібне [3].

Крім цього, слід зауважити, що законодавство ЄС у сфері захисту персональних даних можна пов'язувати з 1995 р., адже саме у той час почалось узгодження законодавства країн-членів ЄС із Директивою 95/46/ЄС, Конвенцією 108 та Договором про Європейський Союз (ДЄС), Договором про функціонування Європейського Союзу (ДфЄС), якщо не зважати на Загальну Декларацію прав людини. Варто зазначити, що ЄС завжди намагається використовувати дані та необхідність захисту персональних даних, зокрема, Хартія основних прав ЄС закріплювала як норми у захисті персональних даних, так і принципи захисту та гарантії контролю за захистом персональних даних. А реформи 2012 р. у контексті захисту персональних даних, які майже повністю змінили Директиву, лише підтверджують занепокоєння ЄС щодо ефективності захисту персональних даних країн-членів [4, с. 98].

Регламент ЄС слугує своєрідним стандартом, законом, що є взірцем захисту персональних даних. Тому багато країн, переймаючи досвід ЄС, створюють власні відповідні закони, що покликані захищати дані фізичних осіб. Зокрема, іншими актами, що так чи інакше схожі на Регламент, є: CCPA, PIPEDA та LGBD. Зробимо їх порівняння:

– ***Регламент ЄС*** встановлює норми щодо захисту фізичних осіб у зв'язку з опрацюванням персональних даних і норми про вільний рух персональних даних. Він поширюється на опрацювання персональних даних повністю чи частково із застосуванням автоматизованих засобів та доопрацювання персональних даних із застосуванням неавтоматизованих засобів, які формують частину картотеки або призначені для внесення до картотеки [1]. Регламент передбачає вимоги до конкретних ситуацій обробки, включаючи обробку для журналістських цілей та академічного, художнього чи літературного вираження. Щодо терито-

ріальної дії, то варто зазначити, що Регламент застосовують для опрацювання персональних даних у контексті діяльності осідку контролера або оператора в Європейському Союзі, незалежно від того, відбувається опрацювання в межах ЄС чи ні. Крім того, зазначений Регламент поширюється на обробку персональних даних суб'єктів даних, які перебувають в Європейському Союзі, контролером або обробником, не зареєстрованим в ЄС, якщо діяльність з обробки пов'язана з:

1) пропонуванням товарів або послуг, незалежно від того, чи потрібна оплата суб'єкту даних, таким суб'єктам даних в ЄС;

2) моніторингом їхньої поведінки у межах ЄС [1].

– ***CCPA*** набув чинності 1 січня 2020 р. Різниця між GDPR і CCPA полягає в тому, що в CCPA включаються дані, які не стосуються окремої фізичної особи, але класифікуються як дані користувача (споживача). CCPA визначає захист даних споживачів, які є фізичними особами і повинні бути резидентами штату Каліфорнія, тоді як GDPR стосується суб'єктів даних, які є фізичними особами, і не визначає вимоги щодо проживання чи громадянства ЄС. Згідно з CCPA захищається особиста інформація, яка ідентифікується, стосується, описується чи може бути пов'язана з певним споживачем прямо чи опосередковано [5]. CCPA застосовується до компаній, які ведуть бізнес у Каліфорнії та:

1) мають річний валовий дохід понад 25 млн доларів;

2) або купують чи продають, отримують чи передають з комерційною метою особисту інформацію понад 50 тис. жителів Каліфорнії;

3) або одержують 50% чи більше річного доходу від продажу особистої інформації.

CCPA захищає персональні дані жителів Каліфорнії незалежно від того, де вони перебувають зараз. Отже, можна зазначити, що CCPA так само має екстериторіальний характер.

– ***LGPD*** набув чинності 18 вересня 2020 р. LGPD так само, як Регламент ЄС, чітко захищає персональні дані фізичних осіб. Ст. 5 LGPD роз'яснює, що суб'єктом даних є фізична особа, якої стосуються персональні дані, що виступають об'єктом обробки [6]. LGPD поширюється на будь-яку операцію обробки, котра визначається як операція, що виконується з персональними даними, зокрема збір, отримання, класифікація, використання, доступ, відтворення, передача, поширення, обробка, подання, зберігання, видалення, оцінка або контроль інформації, модифікації, зв'язку, передачі, поширення або вилучення, тоді як GDPR застосовується до обробки персональних даних автоматизованими або неавтоматизованими засобами, які формують частину картотеки або призначені для внесення до картотеки. Персональні дані – це інформація стосовно визначеної або ідентифікованої фізичної особи. Щодо територіальної дії, то LGPD:

1) поширюється на операції з обробки даних, що здійснюються в Бразилії;

2) застосовується незалежно від місцезнаходження організації або даних, що обробляються, якщо такі дані належать особам, які перебувають у Бразилії, або якщо персональні дані, що обробляються, були зібрані в Бразилії. Дані, зібрані в Бразилії, визначаються як дані, що належать суб'єкту даних, котрий перебував у Бразилії на момент збору;

3) застосовується незалежно від розташування організації або місця розташування даних, що обробляються, якщо метою діяльності суб'єкта з обробки є пропонування або надання товарів чи послуг особам, які перебувають у Бразилії.

Попри це, у LGPD прямо не вказано, чи поширюється закон на фізичних осіб, незалежно від їх громадянства або місця проживання. Однак вважається, що захист персональних даних поширюється на будь-яку особу, незалежно від громадянства або місця проживання суб'єкта даних. Крім того, ст. 3 встановлює, що LGPD буде застосовуватись, якщо персональні дані, що обробляються, належать особі, яка перебувала в Бразилії на момент їх збору [6]. Тому так само можна говорити про екстериторіальний характер зазначеного закону.

– ***PIPEDA*** був прийнятий парламентом у 2000 р. і впроваджувався поетапно до повного набуття чинності 1 січня 2004 р. Цей закон застосовується в усіх провінціях Канади, за винятком випадків, коли провінція ухвалила подібне законодавство про захист даних

(наприклад, Квебек). PIPEDA захищає особисту інформацію фізичних осіб. Особливістю PIPEDA є те, що цей документ не захищає особисту інформацію померлих осіб. На відміну від Регламенту ЄС він не розрізняє контролерів даних і процесорів даних та поширюється на всі організації, які збирають, використовують або розголошують особисту інформацію під час комерційної діяльності. Водночас PIPEDA поширюється лише на організації, які здійснюють комерційну діяльність, або на особисту інформацію про співробітника чи претендента на роботу в організації, що збирає, використовує або розкриває персональні дані, у зв'язку з функціонуванням федеральної служби, підприємства або бізнесу [7]. Матеріальна сфера стосується особистої інформації фізичної особи, яку організація збирає, використовує або розкриває під час комерційної діяльності. Однак сам документ не містить визначення обробки персональних даних, як GDPR. Щодо територіальної дії, то варто зазначити, що:

1) закон поширюється на організації в Канаді;

2) PIPEDA поширюється на організації, розташовані за межами Канади, якщо відповідна діяльність організації має реальний і суттєвий зв'язок із Канадою;

3) закон не поширюється на організації, які збирають, використовують або розголошують особисту інформацію в канадській провінції, що прийняла законодавство про захист персональних даних, котре федеральний уряд Канади вважає схожим на PIPEDA.

Таким чином, можна знову відзначити екстериторіальний характер закону, проте щодо його поширення за межами Канади потрібно виходити із встановлених законом факторів, які будуть визначати реальний і суттєвий зв'язок із Канадою. Отже, проаналізовані документи дають підстави вважати, що захист персональних даних здійснюється щодо фізичних осіб, щодо організацій як усередині країни (штату), так і поза нею. Особливістю є визначення суб'єкта персональних даних, у деяких документах зазначено, що ним має бути тільки резидент, інші стосуються всіх фізичних осіб, незалежно від того є особа резидентом чи ні.

Висновки. Отже, варто зазначити, що прийняття ЄС нового Регламенту стало поштовхом для зміни національного законодавства у сфері персональних даних в інших країнах. Наразі GDPR виступає певним стандартом, який враховується іншими державами, що імплементують його норми у своє законодавство. Україна також має гармонізувати власне законодавство до Регламенту ЄС, безпосередньо це стосується Закону України «Про персональні дані».

Список використаних джерел:

1. Загальний регламент про захист даних (GDPR) від 27 квітня 2016 р. URL: https://gdpr-text.com/uk/ (дата звернення: 07.11.2021 р.).

2. Гронь О.В., Погореленко А.К. Проблеми захисту персональних даних у контексті сучасної комунікації. *Науковий вісник Ужгородського національного університету. Серія «Міжнародні економічні відносини та світове господарство».* 2018. Вип. 19. Ч. 1. С. 102–109.

3. Директива 95/46/ЄС Європейського парламенту і Ради «Про захист фізичних осіб під час обробки персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 р. URL: http://zakon.rada.gov.ua/go/994_242 (дата звернення: 07.11.2021 р.).

4. Бойко А.М. Законодавство Європейського Союзу у сфері захисту персональних даних. *Юридичний науковий електронний журнал.* 2019. № 4. С. 96–99.

5. California Consumer Privacy Act (CCPA) URL: https://cdp.cooley.com/ccpa-2018/ (last accessed: 07.11.2021).

6. Brazilian General Data Protection Law (LGPD) URL: https://lgpd-brazil.info/ (last accessed: 07.11.2021).

7. Personal Information Protection and Electronic Documents Act. URL: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html (last accessed: 07.11.2021).