Юридичні науки

УДК 347.122:004 (4-6ЄС)

Зозуля Анна Олександрівна

студентка

Національного юридичного університету імені Ярослава Мудрого

ПРАВА СУБ'ЄКТА ДАНИХ ЗГІДНО З GENERAL DATA PROTECTION (GDPR)

Анотація. *У даній статті було визначено права суб'єкта даних згідно з Регламентом General Data Protection (далі - GDPR), що був прийнятий 26 квітня 2016 р. та вступив в силу 25 травня 2018 р. Авторкою було наголошено про екстериторіальну дію даного документа, що поширює свою дію не тільки на компанії, що знаходяться на території ЄС, а й на ті, що знаходяться поза межами Союзу. Авторкою було проаналізовано наведений документ та виокремлено види прав суб'єкта даних у відповідних секціях. Також авторка проаналізувала положення попереднього нормативно-правового акту, що діяв до GDPR, та виявила суттєві відмінності з чинним документом. Наприкінці авторкою було розглянуто питання застосування норм регламенту, що стосуються прав суб'єкта даних на території України та зроблено аналіз із нормами, що існують у вітчизняному законодавстві.*

Ключові слова: *персональні дані, захист персональних даних, GDPR, права суб'єкта даних, Європейський Союз.*

Постановка проблеми. В сучасному світі об'єм збирання та оброблення персональних даних постійно зростає, що обумовлено діджиталізацією багатьох процесів. Тому, все актуальніше стає питання створення спеціальних стандартів для захисту персональних даних

фізичних осіб. Між тим, існує необхідність впровадження європейських норм із захисту персональних даних в українське законодавство, оскільки Україна проголосила європейську ідентичність Українського народу і незворотність європейського та євроатлантичного курсу та прийняла відповідну угоду про асоціацію.

Питанням дослідження захисту захисту персональних даних та прав суб'єктів досліджували багато науковців як вітчизняних так і зарубіжних, серед них можна виділити: Брижко В.М., Овчаренко Я.О., Некіт К.Г, Бойко А.М., Сухорильський П., I. van Ooijen, Helena U. Vrabe.

Виклад основного матеріалу. 26 квітня 2016 року був прийнятий Регламент Європейського Союзу про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (General data protection regulation/Загальний регламент по захисту даних), а 25 травня 2018 року він набрав чинності. Цей документ дуже чітко визначив поняття персональних даних, їхнє опрацювання, а також лаконічно та зрозуміло навів права, якими володіє суб'єкт персональних даних.

З прийняттям GDPR втратила чинність Директива 95/46/ЕС, яка раніше була спрямована на захист персональних даних. Проте, вона не мала такого імперативного характеру як GDPR та початково була спрямована на гармонізацію фундаментальних прав і свобод людини у сфері захисту персональних даних. Однак, в ній також зазначалось про можливість забезпечення вільного обміну даними резидентами ЄС. Але стрімкий розвиток технологій та світової мережі зумовив необхідність прийняття більш детального документу, що створить необхідні вимоги до обробки і захисту персональних даних, ним став GDPR. Так, в статті 5 зазначеної Директиви 95/46/ЕС вказується, що держави-члени в рамках положень Директиви більш точно визначають умови, за яких обробка персональних даних є законною [1]. Отже, раніше зазначена директива

мала диспозитивний характер, а в новоприйнятому документі вже було чітко визначено умови для того, щоб опрацювання було законним, що стало єдиним стандартом.

Стосовно екстериторіальної дій даного документу, то положення GDPR можуть застосовуватись на території інших держав, зокрема й на території України. Це відбувається якщо: компанія є оператором персональних даних або обробляє персональні дані та знаходиться на території ЄС; компанія розташована за межами ЄС, але обробляє персональні дані громадян ЄС. Це також стосується випадків, коли компанія займається продажем товарів або послуг та здійснює моніторинг поведінки користувачів, що перебувають на території ЄС, а забезпеченням виконання вимог GDPR є штрафи, які можуть бути покладені на компанію, що їх порушила.

Ефективний захист персональних даних на території ЄС вимагає зміцнення і встановлення в деталях прав суб'єктів даних і обов'язків тих, хто обробляє і визначає обробку персональних даних, конкретність повноважень для моніторингу виконання правил із захисту персональних даних, а також еквівалентних санкцій за їх порушення в державах-членах ЄС [2, с.47].

Регламент направлений на встановлення норм щодо захисту фізичних осіб у зв'язку з опрацюванням персональних даних і норм про їх вільний рух. Так, питанню правам суб'єкта даних присвячено 3 Главу GDPR, що розподілено на п'ять секцій. У статті 12 зазначається, що контролер (ним є фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних) повинен вжити необхідних заходів для надання будь-якої інформації, вказаної в статтях 13 і 14 та в будь-якому

повідомленні згідно зі статтями 15–22 і 34 щодо опрацювання, суб'єкту даних у стислій, прозорій, доступній для розуміння та легко доступній формі, з використанням чітких і простих формулювань, зокрема, для будь-якої інформації, яку спеціально призначено для дитини [3]. Отже, Регламентом прямо встановлено обов'язок контролера сприяти наданню необхідної інформації суб'єкту даних.

У секції "Інформація та доступ до персональних даних" зазначено про право на доступ. Так, суб'єкт персональних даних має право на отримання підтвердження факту опрацювання його персональних даних та інформацію, яка стосується: категорії відповідних персональних даних; одержувачів чи категорії одержувача, якому персональні дані були або будуть розкриті, зокрема, одержувачі в третіх країнах або міжнародні організації. Регламентом встановлено широкий спектр інформації, яку суб'єкт може і має отримати задля того, щоб дізнатись які саме фактичні дані стануть відомими.

У наступній секції "Виправлення та стирання" передбачено відповідне право на виправлення. Так, суб'єкт даних повинен мати право на виправлення його або її неточних персональних даних, яке повинен здійснити контролер без будь-якої необґрунтованої затримки. Крім, цього він/вона має право на заповнення персональних даних, яких раніше не було внесено, якщо надасть відповідну заявку.

Надзвичайно важливим є наступне право - право на стирання (право бути забутим), оскільки по-суті забезпечує технічну можливість видалення інформації, що на законних підставах перебувають у контролера. Згідно з цим правом, для суб'єкта даних передбачено право на стирання своїх персональних даних, без будь-якої безпідставної затримки, також контролер повинен бути зобов'язаним стерти персональні дані без будь-якої необґрунтованої затримки у разі виникнення однієї наведених у Регламенті підстав. Між іншим, право суб'єкта персональних даних

вимагати у контролера даних видалення цих даних закріплене у багатьох міжнародних договорах, рішеннях міжнародних організацій та актах національного законодавства держав, проте формулювання далеко не усіх цих документів дають підстави стверджувати щодо визнання ними права на забуття [4, с.93]. У Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року йдеться, що суб'єкт даних може вимагати виправлення або знищення даних, якщо їх обробляли всупереч положенням внутрішнього законодавства, що впроваджують принципи, зазначені у Конвенції [5]. Подібно до цього, у Законі України «Про захист персональних даних» зазначено, що суб'єкт персональних даних має право «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» [6]. Через свою нематеріальність особисті дані в принципі мають таку характеристику, що їх можна множити майже необмежено. Право на видалення даних, і особливо обов'язок контролера даних повідомляти інші сторони про відповідальність за видалення даних, збільшує індивідуальний контроль за обсягом і потоком цих даних [7, с.103].

Більш того, суб'єкт даних має право на обмеження опрацювання контролером даних у разі настання таких обставин: точність персональних даних оскаржує суб'єкт даних, протягом періоду часу, що надає контролеру можливість перевірити точність персональних даних; опрацювання є незаконним та суб'єкт даних виступає проти стирання персональних даних і натомість надсилає запит на обмеження їх використання.

Наступним є право на мобільність даних, що являє собою здатність таких даних щодо перенесення між різними володільцями. Так, суб'єкт даних повинен мати право на отримання його або її персональних даних,

які він надав контролеру, в структурованому, загальноприйнятому форматі, що легко читається машиною, та мати право на передавання таких даних іншому контролеру без перешкод від контролера, якому було надано персональні дані у випадках, визначених Регламентом [3]. Як правило, під такими даними розуміють досить широкий спектр інформації, а саме дані, які є безпосередньо завантажені чи опубліковані суб'єктом, тобто контакти чи особиста інформація, фотографії чи повідомлення в блозі чи на форумах.

Основна ідея цього права полягає в тому, що людина може безперешкодно передавати свої персональні дані та інші матеріали від однієї інформаційної служби, наприклад, з Facebook до Google. Зараз ці види індустрії схильні до монополізації, через результат інновацій, ефекту Мережі, що ставить під загрозу індивідуальний контроль над особистими даними - у особи просто немає вибору. Вважається, що мобільність може дозволити людям максимізувати переваги великого масиву даних та отримати вигоду від вартості, створеної в результаті використання їх особистих даних. Наприклад, це дозволить обробляти дані для власних цілей або обмінюватися даними з третіми сторонами в обмін на свої послуги [7, с. 102].

У секції право на заперечення та автоматизоване індивідуальне вироблення й ухвалення рішень визначено про право на заперечення. Воно полягає в тому, що суб'єкт даних повинен мати право заперечувати, на підставах, що пов'язані з його або її конкретною ситуацією, в будь-який час, проти опрацювання його або її персональних даних, у тому числі, проти профайлінгу, що ґрунтується на тих положеннях, визначених Регламентом. В свою чергу контролер не повинен більше опрацьовувати персональні дані за винятком доведення ним наявності істотних законних підстав для опрацювання, що переважають над інтересами, правами та

свободами суб'єкта даних або для формування, здійснення або захисту правових претензій.

У секції обмеження приділено увагу випадкам коли, наведені права можуть обмежуватись. Однак, особливістю є те, що якщо таке обмеження зберігає сутність фундаментальних прав і свобод і є необхідним та пропорційним заходом у демократичному суспільстві для забезпечення національної безпеки чи оборони або інших важливих цілей загального суспільного інтересу Союзу або держави-члена, зокрема важливого економічного чи фінансового інтересу Союзу або держави-члена, в тому числі, питань валютної, бюджетної і податкової політики, охорони суспільного здоров'я та соціального забезпечення.

Аналізуючи наведені права суб'єкта даних у GDPR пропонується їх повне закріплення у Законі України "Про захист персональних даних" окремою статтею чи декількома статтями, тим самим задля того, щоб з одного боку розширити права суб'єкта персональних даних з метою їх індивідуального контролю, з іншого - з метою гармонізації національного законодавства до законодавства ЄС. Також необхідним є на законодавчому рівні закріпити незалежних наглядових органів, а також процедуру призначення співробітника з питань захисту даних.

Висновки. GDPR э дуже важливим та прогресивним документом, який наголошує на важливості посилення індивідуального контролю персональних даних. В еру мінімізації анонімності GDPR встановлює засоби збереження її, для забезпечення кожної особи. Права, які закріплені за суб'єктом даних покращують та розширюють гарантії належної та законної обробки даних та їхнім використанням контролером, з подальшою можливістю видалити такі дані. Отже, беззаперечним є визначення ефективності GDPR у посиленні індивідуального контролю та розширення прав суб'єкта даних.

Література

1. 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 р. // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення 15.12.2020)
2. Брижко В. М. Сучасні основи захисту персональних даних в європейських правових актах // Інформація і право. 2016. №3(18). С. 45–57.
3. 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) URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf (дата звернення 15.12.2020)
4. Сухорольський 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. Львів. 2016. С. 90–101. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/34412/1/sukhorolskyi16.pdf
5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 від 28.01.1981 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення 15.12.2020)
6. Закон України "Про захист персональних даних" від 01.06.2010// База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show

/2297-17#Text(дата звернення 15.12.2020)

7. Van Ooijen, I. & Vrabec, H. U. Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. J. Consum. Policy 2019. №42. PP.91-107.