Юридичні науки

УДК 341(4-672 ЄС) + (477)

Овчаренко Ярослава Олександрівна
магістрант факультету адвокатури
Національного юридичного університету імені Ярослава Мудрого

РЕГЛАМЕНТ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЄВРОПЕЙСЬКОГО СОЮЗУ (GDPR). ЗАСТОСУВАННЯ НА ТЕРИТОРІЇ УКРАЇНИ

Анотація. *Стаття присвячена початку застосування Регламенту 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) від 26.04.2016. Досліджено понятійний апарат Регламенту, положення про екстратериторіальність його дії, Регламент проаналізовано в контексті можливості його застосування щодо фізичних та юридичних осіб України, запропоновано основні шляхи адаптації українського законодавства про захист персональних даних до нових стандартів ЄС.*

Ключові слова: *регламент ЄС 2016/679, контролер, оператор (процесор), екстратериторіальність, незалежний контролюючий орган.*

Постановка проблеми. У сучасних умовах масштаби збирання та обробки персональних даних надзвичайно зросли. Органи державної влади та юридичні особи приватного права, завдяки стрімкому розвитку інформаційних технологій, мають можливість здійснювати збір та обробку персональних даних в необмеженій кількості.

Законодавством Європейського Союзу визначається, що захист фізичних осіб під час опрацювання персональних даних є фундаментальним правом.

Статтею 8(1) Хартії фундаментальних прав Європейського Союзу і статтею 16(1) Договору про функціонування Європейського Союзу встановлено, що кожна особа має право на захист своїх персональних даних [1-2].

В свою чергу, правові межі для захисту персональних даних у Європейському Союзі встановлювала Директива 95/46/ЄС Європейського парламенту і Ради від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних (далі – Директива) – документ, який не був обов'язковим, не носив імперативний характер, а встановлював певні орієнтири, які держави-члени мали закріплювати у своєму законодавстві тим способом, яким вони вважали за потрібне [3].

У зв'язку із явищем транскордонних потоків персональних даних, нагальною стала потреба не просто у правовому регулюванні захисту персональних даних, а й у дієвому механізмі жорсткого примусу.

Як наслідок, 26 квітня 2016 року прийнято 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) (далі – Регламент, GDPR).

25 травня 2018 року GDPR почав діяти, а його норми, на відмінну від положень Директиви, мають пряму дію [4].

Виникає питання: що це означає безпосередньо для України?

Насправді актуальність дослідження цього питання зумовлена не тільки процесом євроінтеграції та підписанням Україною Угоди про асоціацію між Україною та ЄС, а переважно тим, що відповідно до

Регламенту, передача персональних даних за межі Європейського Союзу буде дозволена лише за умови достатнього рівня захисту персональних даних, що забезпечується в країні, в яку здійснюється така передача.

Крім того, відповідно до п. 11 Плану заходів щодо імплементації Угоди про асоціацію між Україною та ЄС, що був затверджений 25 жовтня 2017 року, Україна має удосконалити своє законодавства про захист персональних даних з метою приведення його у відповідність з Регламентом до 25 травня 2018 року [5].

На сьогодні цього не відбулося, проте впевнено можна говорити, що для успішного проходження Україною шляхом євроінтеграції, імплементації положень GDPR в українське законодавство не уникнути.

Дослідження та публікації. Питання захисту персональних даних не залишилося недослідженим українськими науковцями, а саме Барановим О.А, Мельником К.С., Серьогіним С.А, Базановим О. Ю., Кохановською О. В., Оніщенко О. В., Пазюк А. В., Пилипчук В.Г., Брижко В. М.

Проте вказані дослідження були проведені до прийняття та набуття чинності Регламенту Європейського Союзу про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних.

Варто наголосити, що питання практичного застосування нових приписів Європейського Союзу у сфері захисту персональних даних, відповідно до GDPR залишаються дискусійними та знаходяться на початковому етапі пошуку шляхів їх вирішення.

У зв'язку із цим **метою даної статті** є дослідження окремих теоретичних та практичних проблем захисту персональних даних, пов'язаних із прийняттям GDPR, визначення ключових правових вимог, які стосуються безпосередньо України та встановлення базових аспектів, необхідних для адаптації українського законодавства до нового

законодавства Європейського Союзу у сфері механізму правового регулювання персональних даних.

Основні питання, на які спрямовано дослідження:

1. Яким чином правила, встановлені Регламентом ЄС, розповсюджуються на фізичних та юридичних осіб України?
2. Які принципові нововведення містить Регламент, порівняно із державним регулюванням захисту персональних даних в Україні?
3. Які дії на законодавчому рівні варто здійснити для подальшої адаптації положень України про захист персональних даних до законодавства Європейського Союзу?

Виклад основного матеріалу. Проаналізувавши детально положення Регламенту, можна дійти висновку, що хоча Україна і не є державою-учасницею Європейського Союзу, але правила, закріплені GDPR, можуть стосуватися безпосередньо суб'єктів, що належать до її юрисдикції. Оскільки відповідно до ст. 3 Регламенту «Територіальна сфера дії», GDPR має екстратериторіальну дію, то його положення поширюються не лише на держав-членів ЄС, а й на фізичних та юридичних осіб України в конкретних, передбачених Регламентом, випадках:

«…2. Цей Регламент застосовують до опрацювання персональних даних суб'єктів даних, які перебувають у Союзі, *контролером* або *оператором*, який має осідок *поза межами Союзу* (не є резидентом держави-учасниці ЄС), якщо опрацювання даних пов'язано з: (a) постачанням товарів чи наданням послуг таким суб'єктам даних у Союзі, незалежно від того, чи вимагають оплату від таких суб'єктів даних; або (b) моніторингом поведінки суб'єктів даних, якщо така поведінка має місце у межах Союзу…» [4].

Отже, хто є контролером та/або оператором (процесором), відповідно до Регламенту?

Згідно із пунктами 7 та 8 ст. 4 Регламенту, «контролер» - фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних; «оператор» (процесор) - фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який опрацьовує персональні дані від імені контролера [4].

Таким чином із комплексного аналізу вищевказаних положень слідує, що крім самих держав-членів ЄС, дія Регламенту поширюється на «контролерів» та «операторів», які:

- мають співробітників в ЄС;
- проводять кампанії, здійснюють дослідження, моніторинг суб'єктів ринку ЄС (електронна комерція, маркетинг і т.д.);
- здійснюють будь-яку діяльність, спрямовану на ринок ЄС (постачають товари та надають послуги громадянам ЄС на платній та безоплатній основі);
- використовують персональні дані громадян ЄС для здійснення вищевказаної діяльності.

Оскільки в епоху Великих даних правовідносини виникають на перетині юрисдикцій, то персональні дані будь-якої особи, в тому числі громадянина України, можуть піддаватися обробці суб'єктами господарювання ЄС, США і т. д. в режимі реального часу і відповідно до правил цих країн. Аналогічно, фізичні та юридичні особи України, надаючи послуги з використанням мережі Інтернет суб'єктам персональних даних з держав-членів Європейського Союзу, можуть оброблювати персональні дані таких осіб.

Отже, фізичні та юридичні особи України підпадатимуть під регулювання GDPR, перебуваючи у статусі контролера або оператора, як це визначено в самому GDPR за умов, вказаних вище.

Далі слід дослідити ключові нововведення GDPR в контексті моделювання їх застосування до контролерів та операторів персональних даних – фізичних та юридичних осіб України.

Для повного євроінтеграційного процесу стандарт захисту персональних даних в Україні повинен відповідати стандартам ЄС.

На час дії Директиви 95/46/ЄС та перед підписанням Угоди про асоціацію України з ЄС було визнано, що механізм регулювання захисту персональних даних в Україні відповідає стандартам ЄС. Проте Регламент з одного боку містить подібні до Директиви за змістом положення, а з іншого – закріплює принципово нові.

В свою чергу у Звіті Про виконання Угоди про асоціацію між Україною та Європейським Союзом в 2016 році вказано, що відповідно до статті 15 Угоди, Сторони домовились співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів [6].

Так, Законом України «Про захист персональних даних» повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини. В структурі Секретаріату Уповноваженого Верховної Ради України з прав людини функціонує окремий підрозділ з питань захисту персональних даних, серед основних функцій якого – здійснення контролю за дотриманням прав людини у сфері захисту персональних даних, розгляд скарг громадян та вжиття заходів щодо поновлення їхніх прав у сфері захисту персональних даних, перевірка володільців персональних даних. Секретаріатом Уповноваженого Верховної Ради України з прав людини на постійній основі здійснюється моніторинг застосування законодавства з питань захисту персональних даних, за результатами якого вживаються необхідні заходи. Зокрема, на регулярній основі проводяться навчальні лекції для професійних та

цільових груп з питань практичного застосування положень законодавства у сфері захисту персональних даних. Крім того, створена робоча група, у рамках якої здійснюється напрацювання змін та доповнень до Закону України «Про захист персональних даних» з метою ліквідації законодавчих прогалин, які були виявлені при застосуванні на практиці цього Закону та гармонізації із законодавством України про доступ до публічної інформації [7].

1) Спочатку варто провести аналогію ***суб'єктів***, зазначених у законодавстві України та, відповідно у Регламенті ЄС. Основним законом, який регулює питання персональних даних на території України, є Закон України «Про захист персональних даних». Цей Закон регулює правовідносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Поняття «контролер» та «оператор», як вони визначені в GDPR можна аналогічно співставити з поняттями «володілець персональних даних» та «розпорядник персональних даних», як вони визначені в Законі України «Про захист персональних даних». Зокрема, для «контролера» і «володільця персональних даних» ключовим є встановлення мети та засобів (способів) обробки персональних даних, а для «оператора» та «розпорядника персональних даних» ключовим є те, що вони є суб'єктами, яким надано право обробляти персональні дані від імені «контролера» та «володільця персональних даних» відповідно.

2) Наступним кроком буде дослідження ***механізму***, який пропонує застосовувати GDPR, для того аби положення не просто були закріплені на папері, а й ефективно діяли.

У всіх державах – членах ЄС та країнах, пов'язаних економічними відносинами з ними, мають бути створені спеціальні державні інститути для контролю за дотриманням прав у сфері захисту персональних даних.

Відповідно до Глави 6 Регламенту, кожна держава-учасник повинна створити *незалежний контролюючий орган* (*Supervisory authority*) для розгляду скарг, застосування санкцій, співробітництва з іншими контролюючими органами щодо захисту персональних даних [4].

В свою чергу організаційно-правове та методологічне забезпечення мають здійснювати національні *Уповноважені органи контролю захисту персональних даних*, мають бути незалежними, підпорядкованими закону та підзвітними парламенту.

Натомість саме ці Уповноважені органи повинні призначати уже вищезгаданих контролерів.

Кожен контролер (оператор) на підприємствах та в організаціях з чисельністю працівників понад 250 осіб повинен вести облік діяльності з обробки персональних даних.

Крім того на підприємствах, в організаціях тощо або їх об'єднаннях усіх форм власності має бути призначений *спеціаліст із захисту даних*.

У тому випадку, коли контролер або оператор є суб'єктом, який передбачений п. 2 ст. 3 Регламенту, а саме знаходиться поза межами ЄС, то в такому разі він повинен призначити в письмовій формі представника в Союзі.

Для прикладу, в Європейському Союзі функціонують Європейський Омбудсмен – призначається та звітує перед Європейським Парламентом, та Європейський інспектор із захисту даних – призначається та звітує перед Європейським Парламентом і Радою ЄС [8].

Якщо прослідковувати цей процес на рівні держав-членів Європейського союзу, то можна навести наступні приклади.

Ірландія, Ісландія, Іспанія – Комісія Парламенту та Омбудсмен із захисту даних. Підзвітний парламенту;

Угорщина – Комісар із захисту інформації. Очолює інститут з питань захисту персональних даних. Призначається рішенням Парламенту;

Франція – Національна комісія з інформатики. Обирається Парламентом. Комісар із захисту персональних даних. Очолює Французьке агентство з питань захисту персональних даних. Призначається рішенням Прем'єр-міністра;

Швеція – Інспекційна рада та Омбудсмен із захисту даних. Підзвітний парламенту [9].

3) Для того, аби положення діяли та застосовувалися на практиці, потрібно передбачити жорсткий примус та санкції за порушення положень про захист персональних даних. Варто наголосити, що однією із головних відмінностей GDPR від попереднього регулювання є запровадження значних штрафів. Найменша сума штрафу, відповідно до ст. 83 Регламенту, складає 20 млн євро або 4% від валового доходу контролера та/або оператора. Та варто звернути увагу, що у випадку виявлення порушення, застосуванню підлягає вища сума штрафу [4]. Для порівняння: відповідно до законодавства України, у сфері захисту персональних даних максимальна сума штрафу складає 34 тис. грн (ч. 5 ст. 188^{39} КУпАП).

Виникає питання: якщо фізичні та юридичні особи України можуть підпадати під екстериторіальну дію Регламенту, то чи можна притягти такого порушника до відповідальності та накласти санкції, передбачені Регламентом?

Звичайно, що в Україні чіткого механізму застосування штрафів відповідно до законодавства ЄС немає. І поки що є не повністю зрозумілим, яким чином до вищевказаної відповідальності можна притягти порушників-фізичних та юридичних осіб України.

Порушення контролерами/операторами України положень GDPR може призвести до наступних варіантів розвитку подій:

1) якщо при відкритті рахунку для ведення комерційної діяльності в банку ЄС в базі даних буде наявна інформація про порушення фізичною чи юридичною особою України норм GDPR, то скоріше всього, рахунок їм не відкриють;
2) наглядовий орган заборонить суб'єкту права ЄС продовжувати потік або передачу даних в Україну, тобто це фактично розірвання договірних відносин;
3) в свою чергу, ті контролери/оператори України, які відповідатимуть положенням Регламенту, будуть більш конкурентоспроможним на ринку, та їм більше довірятимуть користувачі та контрагенти з ЄС.

Отже, Регламент викладений таким чином, щоб не тільки здійснити примус до порушників, а й створити такі умови, щоб суб'єкт на території ЄС ретельно обирав контрагентів з обробки персональних даних поза територією ЄС.

Наступним кроком після аналізу нових правил Регламенту щодо захисту персональних даних є дослідження проблеми адаптації українського законодавства до безпосередньо GDPR та встановлення базових кроків для наближення українських положень до європейських.

Враховуючи активність використання сучасних інформаційних технологій, загрозу несанкціонованої автоматизованої обробки персональних даних, на основі проаналізованого вище можна стверджувати, що Україна повинна впроваджувати нові Європейські положення щодо персональних даних та застосовувати нову модель їх захисту. Нехай поки що не як держава-учасник ЄС, а як держава, фізичні та юридичні особи якої здійснюють свою діяльність на ринку ЄС та мають безпосередній контакт із персональними даними громадян Європейського

Союзу (відповідно до п. 2 ст. 3 Регламенту). В будь-якому випадку на шляху до послідовної євроінтеграції такої адаптації не уникнути.

До базових та першочергових кроків адаптації можна виділити наступні:

1) затвердження та розробка Верховною Радою України, відповідно до Регламенту та стандартів ЄС, ефективної державної політики щодо захисту персональних даних та здійснення парламентського контролю у цій сфері;
2) запровадження та закріплення інституту Уповноваженого з питань захисту персональних даних, який повинен бути підзвітним Верховній Раді України, основними функціями якого будуть забезпечення нагляду і контролю та удосконалення нормативно-правової бази з питань захисту персональних даних, а також взаємодія з уповноваженими органами ЄС та країн – членів ЄС з питань захисту даних;
3) покладання на центральні органи виконавчої влади функцій, направлені на захист персональних даних, створення спеціальних підрозділів, які могли б діяти у складі Міністерства юстиції, наприклад;
4) оскільки в Україні функціонує Адміністрація Державної служби спеціального зв'язку та захисту інформації України, то на неї слід покласти функції організації забезпечення технічного захисту персональних даних в Україні;
5) віднесення до компетенції Державного бюро розслідувань України проведення розслідування правопорушень, які стосуються захисту персональних даних;
6) щодо судової влади, то можливо взяти до уваги досвід Великобританії, де діє суд із захисту даних, також можливим видається створення окремих судових палат у складі апеляційних

судів або створення спеціалізованого суду з питань захисту інформації (даних), де можна розглядати питання не тільки захисту персональних даних, а й порушень щодо приватності життя, обігу публічної інформації, діяльності ЗМІ і т. д . [10];

7) запровадження в органах, установах, закладах, підприємствах та організаціях посад фахівців з питань захисту персональних даних або покладання цих функцій на окремих працівників цих організацій, як того вимагає ст. 37 Регламенту [4].

Отже, варто наголосити на тому, що 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) є принципово новим положенням законодавства Європейського союзу щодо захисту персональних даних. На відмінну від попереднього директивного та рекомендованого регулювання цієї сфери, GDPR встановлює чіткі та жорсткі правила, запроваджує дієвий механізм, який дозволить практично застосовувати принципи і норми щодо захисту фізичних осіб у зв'язку з опрацюванням їхніх персональних даних, незалежно від їхнього громадянства або місця проживання, дотримання їхніх фундаментальних прав і свобод, зокрема їхнього права на захист персональних даних.

У зв'язку із підписанням Угоди про асоціацію між Україною та ЄС, активним процесом євроінтеграції та адаптації українського законодавства до законодавства ЄС, а головне, відповідно до самого положення Регламенту, зокрема ст. 3, Україна підпадає під дію GDPR у конкретних випадках.

Таким чином фізичні та юридичні особи України, що орієнтуються на ринок держав-членів Європейського Союзу, повинні детально проаналізувати, чи підпадають вони під дію положень Регламенту і якщо так – адаптувати свою політику та процес діяльності щодо обробки та

збору персональних даних відповідно до GDPR. І якщо на сьогодні важко встановити та дослідити, яким саме чином вони (фізичні та юридичні особи України) можуть притягуватися до відповідальності, передбаченої Регламентом, то це не означає, що варто ігнорувати його положення, оскільки в будь-якому випадку негативні наслідки настануть. Навіть якщо це буде не штраф, передбачений ст. 83 Регламенту, то, як варіант, наслідком стане неможливість відкрити банківський рахунок в ЄС, послаблення позицій на ринку ЄС, розірвання вартісних контрактів із суб'єктами ЄС (оскільки останні після 25 травня 2018 року вже обирають собі контрагентів, які не мають порушень у сфері захисту персональних даних).

Якщо говорити про проблему законодавчого врегулювання, то враховуючи принципову новизну багатьох положень та норм GDPR порівняно з регулюванням захисту персональних даних відповідно до українського законодавства про захист персональних даних, то у цьому випадку слід внести суттєві зміни до механізму регулювання та захисту персональних даних в Україні. Зокрема, але не виключно, варто посилити парламентський контроль у цій сфері, привести понятійний апарат українського законодавства у відповідність із законодавством Європейського Союзу, запровадити та врегулювати інститут Уповноваженого з питань захисту персональних даних, створити спеціальні підрозділи у складі центральних органів виконавчої влади із повноваженнями щодо захисту персональних даних, створити незалежний контролюючий орган, запровадити жорсткі санкції за порушення захисту персональних даних та інші заходи.

Література

1. Хартія фундаментальних прав Європейського Союзу від 07.12.2000 / База даних «Законодавство України». URL: http://zakon.rada.gov.ua/go/994_524.
2. Договір про функціонування Європейського Союзу від 07.02.1992, 25.03.1957 / База даних «Законодавство України». URL: http://zakon.rada.gov.ua/go/994_b06.
3. Директива 95/46/ЄС Європейського парламенту і Ради від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних / База даних «Законодавство України». URL: http://zakon.rada.gov.ua/go/994_242.
4. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679.
5. План заходів щодо імплементації Угоди про асоціацію між Україною та ЄС. URL: https://www.kmu.gov.ua/ua/npas/pro-vikonannya-ugodi-pro-asociaciyu-mizh-ukrayinoyu-z-odniyeyi-storoni-ta-yevropejskim-soyuzom-yevropejskim-spivtovaristvom-z-atomnoyi-energiyi-i-yihnimi-derzhavami-chlenami-z-inshoyi-storoni.
6. Звіт «Про виконання Угоди про асоціацію між Україною та Європейським Союзом в 2016». URL: https://www.kmu.gov.ua/diyalnist/yevropejska-integraciya/vikonannya-ugodi-pro-asociaciyu/zviti-pro-vikonannya-ugodi-pro-asociaciyu.

7. Про захист персональних даних: Законом України від 01.06.2010 № 2297-VI/ Верховна Рада України. URL: http://zakon.rada.gov.ua/go/2297-17.
8. Сучасні основи захисту персональних даних в європейських правових актах / В.М. Брижко // Інформація і право. – № 3(18)/2016. – С. 45.
9. Посібник з європейського права у сфері захисту персональних даних. URL:https://www.echr.coe.int/Documents/Handbook_data_protection_UKR.pdf.
10. Гуз А. М. Навчальний посібник «Історія захисту інформації в Україні та провідних країнах світу». URL: http://narodna-osvita.com.ua/2453-navchalniy-posbnik-storya-zahistu-nformacyi-v-ukrayin-ta-provdnih-krayinah-svtu-guz-a-m-skachati-chitati-onlayn.html.