УДК 342.951:351.82

ТАРАСЮК А.В., аспірант Національного університету
біоресурсів і природокористування України

ВПЛИВ ЗАГАЛЬНОГО РЕГУЛЮВАННЯ ЗАХИСТУ ДАНИХ НА КОНТРОЛЕРІВ ТА ПРОЦЕСОРІВ ПЕРСОНАЛЬНИХ ДАНИХ – РЕЗИДЕНТІВ УКРАЇНИ

Анотація. *Стаття присвячується правовим аспектам та проблемам застосування загального регулювання захисту даних до контролерів та процесорів персональних даних – резидентів України, в контексті обробки останніми персональних даних в рамках законодавства Європейського Союзу.*

Ключові слова: *захист персональних даних, інформаційні відносини, інформаційне право*

Summary. *The article is dedicated to the legal aspects and problems of application of the general adjusting of data protection to the inspectors and processors of the personal information – residents of Ukraine, in the context of the personal data handling carried out by them within the framework of legislation of European Union.*

Keywords: *personal data protection, informative relations, informative right.*

Аннотация. *Статья посвящается правовым аспектам и проблемам применения общей регуляции защиты данных к контролерам и процессорам персональных данных – резидентов Украины, в контексте обработки последними персональных данных в рамках законодательства Европейского Союза.*

Ключевые слова: *защита персональных данных, информационные отношения, информационное право.*

Постановка проблеми. В умовах поширення застосування технологій Великих даних, персональні дані фактично стають сировиною для володільців баз даних і забезпечують можливість прийняття компаніями рішень, в основі яких лежить прогноз можливої поведінки конкурентів в рамках конкретних ресурсів в мережі Інтернет. Межа між законною обробкою таких даних та втручанням у приватне життя надзвичайно тонка.

Законодавства про захист персональних даних різняться в залежності від юрисдикції, але з прийняттям у 2016 році Європейським Парламентом і Радою Регламенту (ЄС) 2016/679 від 27.04.16 р. – “Загальне регулювання захисту даних” (General data protection regulation) (далі – GDPR) [1], вимоги до регулювання інформаційних відносин в сфері захисту персональних даних стають уніфікованими для всіх “контролерів” та “процесорів” персональних даних (далі – контролер та процесор відповідно), якщо вказані суб’єкти мають зв’язки з державами-членами Європейського Союзу.

Регламент GDPR вступає в силу в травні 2018 року і відповідне регулювання застосовуватиметься і до контролерів та процесорів – резидентів України. Оскільки зміни є значущими і положення вказаного Регламенту значно відрізняються від норм, які застосовувались до цього, а також від норм вітчизняного законодавства, що регулює умови обробки персональних даних, для українських контролерів та процесорів є проблемним розуміння нових правил та, відповідно, впровадження відповідних правових процедур у свою діяльність. Одним з завдань вітчизняної правової науки є вирішення питання можливості такої адаптації та розробки відповідної дорожньої карти для дотримання вказаними суб’єктами норм GDPR, що будуть застосовані до регулювання їх діяльності.

Результати аналізу наукових публікацій. Визначення та вирішення проблем правових основ у створенні нормативно-правової системи та механізмів захисту персональних даних в Україні, а також – загальної систематизації суспільних відносин в сфері інформаційного права було детально розглянута у роботах Брижко В.М., зокрема у [2; 3]. Значній вклад в удосконалення нормативно-правового регулювання інформаційних відносин в сфері захисту персональних даних було здійснено Барановим О.А., зокрема у [5; 6], Пилипчуком В.Г. [4; 5], Мельником К.С. [5; 7; 8] та іншими українськими вченими. Серед них можливо виділити праці таких, як Кохановська М.Ю. [9], Боєр В.М. та Павельева О.Г. [10], які займалися проблемами цивільно-правових відносин в інформаційній сфері. Іншими українськими вченими, зокрема, такими як Серьогін С.А., досліджувалась тематика – Великі дані, як загроза приватному життю [11].

Проте, питання практичного застосування нових приписів Європейського Союзу для сфери захисту персональних даних стосовно Регламенту GDPR залишаються дискусійними та знаходяться на початковому етапі пошуку шляхів їх вирішення.

Метою статті є визначення ключових правових вимог, які стосуються українських контролерів та процесорів в контексті Регламенту GDPR та створення базової дорожньої карти для адаптації відповідних суб’єктів під нові вимоги законодавства Європейського Союзу.

Виклад основного матеріалу. Регулювання питання законності обробки персональних даних варіюється в залежності від юрисдикцій. Основним законом, який регулює це питання на території України, є Закон України “Про захист персональних даних” [12]. Цей Закон регулює правові відносини, 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. В епоху інформатизації та великих даних, правовідносини виникають на перетині юрисдикцій і персональні дані певної особи, громадянина України, можуть оброблюватись компаніями з США або країн західної Європи в режимі реального часу і відповідно до законів цих країн.

Так само, компанії-резиденти України, надаючи послуги з використанням мережі Інтернет суб’єктам персональних даних з держав-члены Європейського Союзу, можуть оброблювати персональні дані таких осіб на умовах відповідної згоди від вказаних суб’єктів та імперативних норм відповідного правопорядку. Концептуальним є питання вибору вказаного правопорядку. Зазвичай, компанії, які оброблюють персональні дані та надають відповідні шаблони згод на обробку таких даних, визначають право країни, результатом якої вони є, як таке, що застосовується, у тому числі, до питання обробки персональних даних.

Мотивація вибору правопорядку проста – на веб-портал компанії можуть зайти фізичні особи з будь-якої точки світу і на стадії, поки такі особи не сповістили інформацію про себе шляхом заповнення відповідних форм, для компанії не є зрозумілим, резидентами якої країни є такі користувачі. Більш того, технічними засобами не завжди можливо встановити, на території якої країни перебуває фізична особа-користувач, який може не завжди вводити точні дані або не вводити їх взагалі. Таким чином, на сьогодні склалася практика, коли саме володільці персональних даних (контролери) визначають умови згоди на обробку персональних даних, а користувачі погоджуються з такими умовами, або не використовують певний сервіс взагалі. Одним з ключових аспектів в розрізі даної проблематики буде визначення місця надання конкретної послуги – його зазвичай визначає компанія, яка такі послуги надає, у

відповідній публічній оферті. При цьому, така дефініція має відбуватись з урахуванням імперативних норм держави, резидентом якої є компанія і від цього і залежить можливість вибору конкретного правопорядку і відповідних норм.

З іншого боку, деякі країни встановлюють спеціальні захисні норми, які мають бути враховані при обробці персональних даних громадян таких країн та націленості певної послуги саме на ринок відповідної країни. Як приклад, вимоги статті частини 5 статті 18 Закону Російської Федерації “Про персональні дані”, відповідно до положень якої, на оператора персональних даних, під час їх збирання, покладається вимога забезпечити запис, систематизацію, накопичення, зберігання, уточнення (оновлення, зміну), виїмку персональних даних громадян Російської Федерації з використанням баз даних, що знаходяться на території РФ [13]. В контексті застосування вказаних вимог до операторів персональних даних – вони будуть застосовуватись лише до суб’єктів, чиї веб-сайти, в рамках яких відбувається обробка персональних даних користувачів, направлені на територію РФ, та які не підпадають під виключення, що встановлені законом. Як ключові індикатори “направленості” визначаються – пропонування товарів та послуг російською мовою, можливість придбання та прямого отримання товару чи послуги на території РФ та можливість сплати в російських рублях [14].

Таким чином, деякі країни, прагнучі додатково захистити персональні дані осіб, що перебувають на їх території та/або своїх громадян, встановлюють імперативні норми, які розповсюджуються і на іноземних суб’єктів, чия діяльність націлена на відповідний ринок.

Як вже зазначалося раніше, в квітні 2016 року було прийнято Регламент (ЄС) 2016/679 “Про захист фізичних осіб при обробці персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС” (GDPR) [1]. Регламент вступає в силу 24 травня 2018 року та визначає нові умови обробки персональних даних у Європейському Союзі.

Регламент GDPR має екстериторіальну дію, що означає, що його положення застосовуються не лише до компаній-резидентів ЄС, але і до контролерів та процесорів, які оброблюють персональні дані в Євросоюзі, навіть, якщо вони є резидентами інших країн, за умов, які прямо передбачені положеннями GDPR, зокрема, якщо обробка персональних даних пов’язана з пропонуванням товарів або послуг (навіть безкоштовно) суб’єктам персональних даних в ЄС або моніторингу поведінки таких суб’єктів. При цьому наявні окремі спеціальні вимоги як до контролерів, так і до процесорів [1]. Таким чином, компанії-резиденти України підпадатимуть під регулювання GDPR, перебуваючи у статусі контролера або процесора, як це визначено в самому GDPR за умов, що вказані вище.

В рамках GDPR значно розширене саме поняття “персональні дані” в контексті можливих ідентифікаторів та інформації, яка може бути віднесена до персональних даних, а суб’єкти персональних даних отримали більше реальних важелів впливу на контролерів та процесорів в контексті реалізації своїх прав, перелік яких також значно розширений. У зв’язку з цим виникає необхідність проаналізувати ключові нововведення GDPR в контексті моделювання їх застосування до контролерів та процесорів персональних даних – резидентів України.

В статті 4 GDPR визначені ключові поняття, зокрема: персональні дані означають будь-яку інформацію, що стосується ідентифікованої чи такої, що ідентифікується фізичної особи (“суб’єкта даних”), а фізичною особою, яка ідентифікується, визначається особа, яка може бути ідентифікована безпосередньо чи опосередковано, зокрема шляхом посилання на такий ідентифікатор, як ім’я, ідентифікаційний номер, дані про місцезнаходження, он-лайн – ідентифікатор або один чи більше факторів,

характерних для фізичної, фізіологічної, генетичної, психічної, економічної, культурної, або соціальної ідентичності цієї фізичної особи [1]. Поняття “контролер” та “процесор”, як вони визначені в GDPR можна за аналогією порівняти 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 “процесора” та “розпорядника персональних даних” ключовим є те, що вони є суб’єктами, яким надано право обробляти персональні дані від імені “процесора” та “володільця персональних даних” відповідно.

В рамках GDPR вводиться також багато нових термінів, які використовуються в регулюванні персональних даних. Одним з таких термінів, який, можливо, в майбутньому, буде доданий і до українського законодавства в сфері персональних даних є поняття “профілювання”.

Зокрема, профілювання означає будь-яку автоматичну обробку персональних даних, що полягає у використанні персональних даних для оцінки певних особистих аспектів, пов’язаних з фізичною особою, зокрема для аналізу та прогнозування аспектів, що стосуються результатів діяльності фізичної особи на роботі, економічної ситуації, здоров’я, особистих уподобань, інтересів, надійності, поведінки, місцезнаходження або переміщень [1].

При застосуванні технологій Великих Даних персональні дані певною мірою можна вважати матеріалом, який після автоматичної обробки перетворюється на інсайти – інформацію, що дозволяє автоматизоване прийняття рішень на основі первинної інформації. Це можуть бути пропозиції реклами певних товарів або послуг, в яких особа може бути зацікавлена виходячи з даних аналізу. Стаття 22 GDPR передбачає право суб’єкта персональних даних заборонити контролеру приймати щодо такого суб’єкта рішення, що засновані виключно на автоматичній обробці, включаючи профілювання, якщо такі рішення мають юридичні наслідки. Як можливий приклад такого автоматичного рішення – рішення фінансової установи про видачу чи не видачу кредиту особі в режимі он-лайн, виходячи з даних анкети, що була нею заповнена або інші види послуг, в рамках яких відбувається так званий “скоринг” або оцінка клієнта як потенційного контрагента за допомогою автоматичних систем. Ще одним прикладом може бути сфера онлайн – рекрутингу (підбору персоналу), в рамках якої можуть мати місце автоматичні рішення про можливість пропонування роботи чи відхилення кандидатури певного суб’єкта персональних даних.

В GDPR визначено ряд прав для суб’єкта персональних даних, зокрема: право на зрозумілу та доступну інформацію, право бути забутим, право на мобільність даних, право заборони використання автоматизованих рішень, заснованих на профілюванні щодо себе, право отримувати інформацію про порушення правил безпеки зберігання даних.

Одним з найбільш цікавих з правової точки зору є право суб’єкта персональних даних “бути забутим”, яке передбачене статтею 17 GDPR. Однією з підстав реалізації цього права суб’єктом персональних даних може бути відкликання ним згоди на обробку персональних даних.

Право на мобільність даних, що передбачене статтею 20 GDPR надає право суб’єкту персональних даних вимагати у контролера свої персональні дані, які були йому надані таким суб’єктом у зручному, структурованому та такому, що може бути зчитаний комп’ютером, вигляді.

Одним з важливих аспектів GDPR, який необхідно враховувати контролерам-резидентам України, є необхідність збереження підтвердження факту надання згоди від

суб’єкта персональних даних та можливості демонстрації факту такої згоди за запитом. В рамках GDPR згода повинна бути однозначною та бути виражена чіткою заявою або дією. Цікавим є те, що в рамках GDPR прямо заборонена можливість отримувати згоду шляхом представлення для користувача вже заповнених полів з відповідними пташечками. Стаття 7 GDPR встановлює особливі вимоги до згоди. Зокрема, у випадку, якщо згода надається разом з іншою інформацією або завіренням, сам бланк згоди має бути таким, що є вільно відділений від іншої частини документу. Також, відповідно до норм вищевказаної статті, суб’єкт персональних даних має бути повідомлений про своє право відкликати свою згоду у будь-який момент і це буде зробити легко [1].

Стаття 8 Закону України “Про захист персональних даних” [10] також передбачає право суб’єкта персональних даних відкликати свою згоду на обробку персональних даних. На практиці реалізація цього права ускладняються тим, що персональні дані особи могли бути передані іншим володільцям персональних даних в рамках досить широких та розмитих умов згоди, на яку погодився суб’єкт персональних даних, фактично не маючи іншого виходу, адже прийняття відповідних умов згоди було єдино можливим варіантом для отримання відповідної послуги таким суб’єктом. При цьому суб’єкт персональних даних може навіть не знати, кому були передані його персональні дані, адже в умовах згоди було сказано “іншим третім особам, на розсуд володільця персональних даних для реалізації цілей надання цієї згоди”. При цьому, самі цілі згоди часто прописуються максимально широко та в незрозумілому ключі і в результаті – відкликання своєї згоди для суб’єкта персональних даних стає максимально складним.

Прийняття GDPR покликане уникнути таких ситуацій для суб’єктів персональних даних з Євросоюзу, адже встановлює чіткі вимоги не лише до формату згоди, а і до побудови процесів управління вже отриманими згодами. Зокрема, ICO (Information Commissioner’s Office), в своїх рекомендаціях щодо управління згодами, що будуть отримані в рамках GDPR, зазначає наступне (невиключний перелік):

- запит на отримання згоди варто робити виразним, стислим, відокремленим від інших умов і простим для розуміння;
- варто включити назву організації та будь-яких контролерів-третіх сторін, які будуть спиратися на згоду, пояснити, навіщо потрібна інформація, які дії будуть проводитись з інформацію, і наявність у суб’єкта персональних даних права на відкликання згоди;
- згода має бути надана в активній формі (без авто-заповнених полів анкет чи за замовчуванням);
- за можливості варто надавати можливість детального вибору умов згоди для різних цілей різних видів обробки;
- варто зберігати підтвердження факту надання згоди – суб’єкт, який надав згоду, час надання, спосіб та що було повідомлено суб’єкту перед наданням такої згоди;
- варто робити простою можливість відкликати надану згоду та розглянути можливість використання інструменту вибору преференцій;
- варто тримати отримані згоди під контролем та оновлювати їх у випадку змін, а також зробити це частиною власних бізнес-процесів [15].

Таким чином, згоди стають певним матеріально вираженим об’єктом, що в більшості випадків буде існувати в електронному режимі. Кожна відповідна згода, як об’єкт, буде свідчити про факт надання права певному контролеру використовувати персональні дані на умовах, що визначені в такій згоді. Управління масивом таких згод є

завданням контролера, який оброблює відповідні персональні дані і, відповідно, є відповідальним за додержання всіх принципів обробки таких даних, як це визначено в статті 5 GDPR.

Ключовим для українських контролерів в рамках GDPR є умови трансферу персональних даних суб’єктів з Євросоюзу в інші країни. Такий трансфер можливий на умовах, що визначені в GDPR, і однією з відповідних підстав є явна згода суб’єкта персональних даних на запропонований трансфер після того, як він був поінформований про відповідні ризики та відсутність умов, що визначені в статті 49 GDPR. Таким чином, для передачі персональних даних в Україну, суб’єкт персональних даних повинен буде прямо погодитись на такий трансфер і відповідна компанія має зберігати таку його згоду.

GDPR визначає як загальні правила, що застосовуються до будь-якої обробки персональних даних, так і спеціальні правила, що застосовуються до обробки спеціальних категорій персональних даних, таких як дані про стан здоров’я, що відбуваються в контексті наукових досліджень, включаючи клінічні та трансляційні дослідження [16]. В GDPR мають місце розділи, присвячені особливим категоріям персональних даних, щодо обробки яких встановлюються додаткові вимоги.

Ще одним важливим нюансом для контролерів та процесорів – резидентів України, які підпадають під регулювання GDPR (згідно частини 2 статті 3 GDPR) буде необхідність призначення представника на території Європейського Союзу, як це визначено в п. 27 GDPR.

Стаття 28 визначає основні вимоги до процесорів, під які підпадають і компанії процесори – резиденти України, якщо персональні дані, які вони оброблюють від імені контролера, були отримані з Європейського Союзу.

Діяльність процесорів у тому числі визначається відповідним договором з контролером. В обов’язках процесора має бути зазначено тривалість, природу та мету обробки, типи даних, що оброблюються та права і обов’язки контролера [17].

Таким чином, компанії-резиденти України мають бути готові до нових реалій захисту персональних даних згідно нових приписів законодавства Європейського Союзу.

Висновки.

Українським компаніям, що орієнтуються на ринок держав-членів Європейського Союзу, необхідно проаналізувати, чи підпадають вони під регулювання положень Регламенту GDPR і якщо так – прийняти міри для дотримання відповідних вимог.

Ключовими індикаторами для визначення, чи підпадає організація під таке регулювання, є наступні:

а) контролер чи процесор засновані в державах-членах Європейського Союзу;

б) факт пропонування товарів чи послуг на ринок Європейського Союзу або моніторинг за поведінки суб’єктів персональних даних в Європейському Союзі на умовах, визначених в Регламенті GDPR.

Враховуючи неймовірну новизну багатьох положень та концепцій GDPR порівняно з регулюванням захисту персональних даних українським законодавством, компаніям-резидентам України, діяльність яких підпадає під регулювання GDPR необхідно якомога раніше починати підготовку до адаптування своїх бізнес-процесів під нові вимоги а також розпочинати розробку відповідних політик, форматів згод на обробку персональних даних та інших документів.

Основною особливістю для українських компаній в рамках виконання умов GDPR є також необхідність;

а) призначення свого представника для комунікації з відповідними уповноваженими органами Європейського Союзу;

б) наявність явної та недвозначної згоди від суб’єкта персональних даних на передачу своїх персональних даних на територію України, якщо такими є плановані бізнес-процеси.

Питання впливу GDPR на контролерів та процесорів резидентів України є новим та малодослідженим. Наступні наукові дослідження у цьому напрямку зможуть допомогти у розробці певної дорожньої карти, яка зможе зробити процес адаптації вказаних компаній до нових вимог європейського законодавства з захисту персональних даних зрозумілим та однозначним.

Використана література

1. 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). – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from= EN

2. Брижко В.М. Організаційно-правові питання захисту персональних даних : дис. на здобуття наук. ступеня. канд. юрид. наук : спец. 12.00.07 – теорія управління ; адміністративне право і процес ; фінансове право ; інформаційне право / В.М. Брижко. – (НДЦПІ АПрН України, НАДПС України). – К.- Ірпінь, 2004, – 251 с.

3. Брижко В.М. Основи систематизації інформаційного законодавства : теоретичні та правові засади : монографія / В.М. Брижко. – К. : ТОВ “ПанТот”, 2012 р. – 304 с.

4. Pylypchuk, Volodymyr; Bryzhko, Valery, 2016. PRIVACY AND HUMAN SECURITY IN THE PROTECTION OF PERSONAL DATA (Приватність та безпека людини у сфері захисту персональних даних) // Social and Human Sciences. Polish-Ukrainian scientific journal, 04 (12). – Available at : http://sp-sciences.io.ua/s2596466/pylypchuk_volodymyr_bryzhko_valery_2016_privacy_and_human_security_in_the_protection_of_personal_data_social_and_human_sciences._polish-ukrainian_scientific_journal_04_12_ (accessed 08 January 2017).

5. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / [В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник] ; за ред. В.М. Брижка, В.Г. Пилипчука. – К. : ТОВ “Видавничий дім “АртЕк”, 2017. – 226 с.

6. Баранов О.А. Напрями перспективних досліджень у галузі інформаційного права // Інформація і право. – 2(17)/2016. – Режим доступу : http://ippi.org.ua/baranov-oa-napryami-perspektivnikh-doslidzhen-u-galuzi-informatsiinogo-prava-stor-15-31

7. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних // Інформаційна безпека людини, суспільства, держави. – 2013. – № 2. – С. 97-103. – Режим доступу : http://nbuv.gov.ua/UJRN/iblsd_2013_2_18

8. Мельник К.С. Правові та організаційні основи захисту персональних даних в Європейському Союзі та в Україні : дис. на здобуття наук. ступеня. канд. юрид. наук : спец. 12.00.07 – теорія управління ; адміністративне право і процес ; фінансове право ; інформаційне право / К.С. Мельник. – (НДЦПІ АПрН України). – К., 2015, – 269 с.

9. Кохановська О.В. Інформація як об’єкт правовідносин. – Режим доступу : http://papers.univ.kiev.ua/1/jurydychni_nauky/articles/kokhanovska-o-information-as-an-object-of-legal-relations_18016.pdf

10. Боер В.М. Информационное право / В.М. Боер, О.Г. Павельева. – Ч. 1. – СПб. : ГУАП, 2006. – 116 с.

11. Серёгин В.А. BIG DATA : новая угроза для прайвеси в условиях информационного общества // Науковий вісник Ужгородського національного університету. – (Серія Право). – 2015. – № 35. – Ч. 1. – Т. 1. – С. 93-97.

12. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-17

13. О персональных данных : Закон Російської Федерації від 27.07.06 г. № 152-ФЗ : ред. от 29.07.17 г. – Режим доступу : http://www.consultant.ru/document/cons_doc_LAW_61801

14. О обработке и сохранении персональных данных : разъяснение Минкомсвязи России от 01.09.15 г. – Режим доступу : http://minsvyaz.ru/ru/personaldata

15. Рекомендації Информационного Комиссара (ICO). – Режим доступу : https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-bases-for-processing/co nsent

16. Gauthier Chassang,. The impact of the EU general data protection regulation on scientific research. – Режим доступу : http://ecancer.org/journal/11/full/709-the-impact-of-the-eu-general-data-protection-regulation-on-scientific-research.php

17. Debbie Heywood : Obligations on data processors under the GDPR. – Режим доступу : https://united-kingdom.taylorwessing.com/globaldatahub/article-obligations-on-data-processors-under-gdpr.html

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~