УДК 342.951:351.82

АНАЛІЗ ДЕЯКИХ КЕРІВНИЦТВ РОБОЧОЇ ГРУПИ 29 У КОНТЕКСТІ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ПРО ЗАХИСТ ДАНИХ

ANALYSIS OF SOME OF THE GUIDES OF WORKING PARTY 29 IN THE CONTEXT OF THE GENERAL DATA PROTECTION REGULATION

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

Стаття присвячується аналізу певних керівництв Робочої групи 29 у контексті Загального регламенту про захист даних та можливості застосування положень таких керівництв у рамках українського правового поля задля забезпечення можливості реального контролю суб'єктів персональних даних за обробкою таких даних, у тому числі – в автоматизованому режимі. Аналіз таких положень є важливим для розвитку регулювання персональних даних в Україні. Згодом такі положення можуть бути імплементовані в українське законодавство.
Ключові слова: великі дані, Робоча група 29, Загальний регламент про захист даних, персональні дані, захист даних, приватність.

Статья посвящена анализу определенных руководств Рабочей группы 29 в контексте Общего регламента о защите данных и возможности применения положений таких руководств в украинском правовом поле для обеспечения возможности реального контроля субъектов персональных данных за обработкой таких данных, в том числе – в автоматизированном режиме. Анализ таких положений является важным для развития регулирования персональных данных в Украине. Со временем такие положения могут быть имплементированы в украинское законодательство.
Ключевые слова: большие данные, Рабочая группа 29 Общий регламент о защите данных, персональные данные, защита данных, приватность.

The article is devoted to the analysis of certain guidelines of the Working Party 29 in the context of the General Data Protection Regulation and the possibility of applying the provisions of such guidelines within the Ukrainian legal field in order to make possible the real control of the subjects of personal data on processing of such data, including in automated mode. An analysis of such provisions is important for the development of regulation of personal data protection in Ukraine. Subsequently, such provisions may be implemented in Ukrainian legislation.
Key words: big data, the Working Party 29, General Data protection regulation, personal data, data protection, privacy.

Постановка проблеми: Враховуючи розвиток технологій щодо обробки інформації, обробка персональних даних, у тому числі, в автоматичному режимі, стала ризиком для суб'єктів персональних даних, адже у зв'язку зі швидкістю такої обробки та передачі таких даних, контролери (розпорядники) відповідних баз персональних даних можуть зловживати реалізацією прав та свобод суб'єктів даних.

Такий стан речей став однією з причин прийняття Загального регламенту про захист даних (далі – GDPR) [1] Європейським парламентом. Враховуючи складність та певну футуристичність нового регулювання у контексті регулювання відносин, пов'язаних з постійним розвитком технологій, консультаційним органом у рамках GDPR, а саме Робочою групою 29 було випущено ряд керівництв, що мають допомогти контролерам та обробникам у рамках GDPR [1] привести свою діяльність у відповідність до норм регламенту. Аналіз таких керівництв є необхідним як для кращої адаптації до нових вимог контролерів та обробників персональних даних, що підпадають під вимоги GDPR в Україні, так і для можливого подальшого розвитку українського законодавства у сфері регулювання персональних даних.

Аналіз останніх досліджень і публікацій. Українським ученим С.А. Серьогіним досліджувалась схожа тематика – «великі дані, як загроза приватному життю» [2]. Ученим аналізувався вплив великих даних на стан захисту персональних даних. Також варто виділити праці таких науковців, як В.М. Брижко [3], О.А. Баранов [4], К.С. Мельник [5] у контексті аналізу правового статусу інформації та стану захисту персональних даних у цілому.

Проте питання аналізу конкретних керівництв Робочої групи 29 у контексті можливої імплементації їх положень до українського законодавства є малодослідженим і потребує вивчення.

Формулювання цілей статті. Мета статті – розробка практичних рекомендацій щодо використання певних роз'яснень у рамках керівництв Робочої групи 29 контролерами та обробниками даних, а також щодо можливості імплементації таких роз'яснень в українське законодавство.

Виклад основного матеріалу. GDPR набрав чинності у травні 2018 року і прийшов на зміну попередньому регулюванню персональних даних в Європейському союзі, а саме – Директиві 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» (далі – Директива) [6].

У рамках ст. 29 Директиви було створено робочу групу, а саме «Робочу групу із захисту фізичних осіб при обробці персональних даних» (далі за текстом – «Робоча група 29»). Така група має консультативний статус і незалежна у своїй діяльності і трансформується в Європейську раду з захисту персональних

даних (European data protection board) після набрання чинності GDPR у відповідності до ст. 68 GDPR. До такої трансформації Робоча група 29 видає керівництва щодо положень GDPR відповідно до ст. ст. 29 та 30 вказаного регламенту. Такі керівництва дозволяють компаніям, що мають статус контролера та обробника у рамках GDPR, краще підготуватись до GDPR та бути впевненими у дотриманні норм такого регламенту.

У рамках даної статті будуть проаналізовані наступні керівництва Робочої групи 29:

1. Керівництво щодо прозорості [7].
2. Керівництво щодо згоди на обробку персональних даних [8]
3. Керівництво щодо оцінки впливу на захист даних та визначення того, чи може обробка привести до високого ризику [9].
4. Керівництво щодо портативності даних [10].

Першим необхідно проаналізувати Керівництво щодо прозорості [7].

Говорячи про принцип прозорості у рамках обробки персональних даних, варто зазначити, що в Україні основним законом, що регулює захист персональних даних, є закон України «Про захист персональних даних» [11]. У ст. 6 указаного закону вказано, що «обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки» [11].

Таким чином, у рамках українського законодавства «прозорість» визначається як одна з умов обробки персональних даних, але деталізація умов «прозорості» відсутня у вказаному законі [12].

Виходячи зі ст. 12 GDPR, у рамках Керівництва щодо прозорості, виділяється наступні ключові стадії циклу обробки даних: (1) перед або у момент початку циклу обробки персональних даних, тобто тоді, коли персональні дані збираються від суб'єкта персональних даних або отримуються іншим шляхом, (2) впродовж всього процесу обробки, тобто у процесі комунікації з суб'єктами персональних даних щодо їхніх прав та (3) у специфічні моменти у рамках процесу обробки персональних даних, наприклад, коли трапляються порушення персональних даних або відбуваються матеріальні зміни до такої обробки [7].

Таким чином, принцип прозорості фактично пронизує весь процес роботи обробників з персональними даними і зобов'язує їх вести якісну та зрозумілу комунікацію з суб'єктами персональних даних у рамках всього циклу обробки персональних даних. Такий підхід до кваліфікації етапів у контексті аналізу відповідності вимозі щодо прозорості процесу обробки персональних даних може також бути використаний і українськими компаніями, які не підпадають під дію GDPR.

Виходячи з визначення прозорості у рамках GDPR та Керівництва щодо прозорості, можна виділити декілька ключових елементів прозорості, зокрема – повне і зрозуміле інформування суб'єктів персональних даних щодо всього процесу обробки персональних даних таких осіб у зрозумілому для них ключі та зрозумілою для них мовою таким чином, щоб такі суб'єкти даних розуміли, що відбувається з їх персональними даними, хто здійснює відповідні дії та які права вони мають у контексті такої обробки.

Роз'яснення щодо прозорості, які наявні у Керівництві щодо прозорості, можуть використовуватись обробниками персональних даних в Україні для забезпечення якнайкращої можливості суб'єктів персональних даних реалізовувати свої права.

Наступним керівництвом, яке необхідно проаналізувати, є Керівництво щодо згоди у рамках GDPR [8]. У рамках цього керівництва роз'яснюються умови отримання згоди від суб'єктів персональних даних у рамках GDPR.

У Керівництві щодо згоди у рамках GDPR наводяться елементи дійсної згоди. Зокрема, зазначається, що у відповідності до ч. 11 ст. 4 GDPR, «згода» суб'єкта даних означає будь-яке вільно надане, конкретне, поінформоване та однозначне зазначення бажань суб'єкта даних, яким він або вона, шляхом оформлення заяви чи проявом чітких ствердних дій, підтверджує згоду на опрацювання своїх персональних даних [1].

У Керівництві щодо згоди у рамках GDPR звертається увага на таку концепцію як «зернистість» у рамках конкретної згоди, яка отримується у суб'єкта персональних даних. Під зернистістю слід розуміти необхідність отримання згоди на всі види опрацювання даних за кожною з цілей [6]. Як приклад, в одній згоді, яка надається шляхом проставлення однієї відмітки, не слід вказувати на можливість використання персональних даних для передачі третім особам для маркетингових цілей і для можливості надання послуги як такої.

Необхідність отримання окремої згоди на кожну з цілей обробки даних є можливістю реального впливу суб'єкта даних на обробку своїх даних і може бути надалі імплементована в українське законодавство.

Наступним керівництвом, яке необхідно проаналізувати у рамках цієї роботи, є Керівництво щодо оцінки впливу на захист даних та визначення того, чи може обробка привести до високого ризику [9].

У рамках такого Керівництва розглядаються питання необхідності застосування контролером процедури оцінки впливу на захист даних процесів обробки даних, що здійснюються таким обробником, а також визначення, чи може така обробка привести до високого ризику для суб'єктів даних.

Процес проведення оцінки впливу обробки даних на захист персональних даних (Data protection impact assessment / DPIA) визначається у GDPR, а нюанси його проведення та конкретні випадки вказуються у Керівництві щодо оцінки впливу.

У рамках Керівництва щодо оцінки впливу вказується, що обов'язок контролера проводити оцінювання витікає з загального обов'язку контролера з управління ризиками під час обробки персональних даних [9].

Отже, у рамках GDPR вводиться новий механізм оцінки впливу обробки персональних даних на предмет можливого ризику для захисту їх персональних даних у рамках такої обробки. Встановлюються критерії, які зобов'язують контролера провести таке оцінювання у конкретних випадках. Такими випадками визначаються зокрема ситуації, у рамках яких виникає значний ризик для суб'єктів даних. Серед вказаних вище випадків варто виділити обробку персональних даних осіб, які є вразливими, а також обробку персональних даних з застосуванням новітніх технологій.

Положення щодо проведення оцінки впливу обробки персональних даних на захист таких персональних даних могли б бути і мають бути імплементовані в українське законодавство щодо захисту персональних даних. Враховуючи об'єми обробки персональних даних громадян України та осіб, що перебувають на території України великими компаніями, особливо тими, що працюють у сфері надання інформаційних послуг, проведення ними таких оцінювань є необхідним, адже дозволить краще захистити права та інтереси суб'єктів персональних даних завдяки зменшенню або нівелюванню ризиків для суб'єктів персональних даних, у тому числі шляхом впровадження новітніх технічних та організаційних засобів для забезпечення дотримання вимог законодавства.

Останнім керівництвом, що буде проаналізоване у рамках даної роботи, є Керівництво щодо портативності даних [10]. В українському законодавстві не передбачене право «на мобільність даних».

Таке право є певною новелою GDPR і його поява покликана дати більший контроль суб'єктам даних за використанням та переміщенням своїх персональних даних від одного контролера до іншого.

Враховуючи той факт, що компанії резиденти України, які виступають у статусі контролерів у рамках GDPR мають забезпечувати таке право, а також його новизну як для українського, так і для європейського права, необхідно детально проаналізувати умови реалізації такого права, а також відповідні положення нормативних актів та роз'яснень щодо такого права. У рамках GDPR право на мобільність даних передбачене ст. 20 Регламенту [1]. Робоча група 29 випустила спеціальне Керівництво щодо портативності даних від 27.10.2017 [10].

У Керівництві щодо мобільності даних вказується на те, що сама суть «мобільності» або «портативності» даних може дати поштовх для розвитку контрольованого та обмеженого розповсюдження персональних даних суб'єктів даних [10].

У Керівництві щодо мобільності даних [10] також вказується, що інформацією, що має бути переданою у рамках реалізації суб'єктом даних права на мобільність даних, не буде інформація, яка була анонімізована (з неї були повністю видалені всі та будь-які можливі ідентифікатори, що могли б відноситись до певного суб'єкта даних. З іншого боку, псевдонімізована (інформація, що може бути відновлена у випадку наявності певного ідентифікатора) інформація має бути надана суб'єкту даних [10].

Наступною категорією даних, яка має бути передана контролером даних у випадку відповідного запиту суб'єкта даних у рамках реалізації права на мобільність такого суб'єкта даних та яка виділяється в рамках керівництва щодо мобільності даних, є «дані, що передані таким суб'єктом даних».

Зокрема, у керівництві вказується, що такими даними є не лише «account information» (електронна скринька, ім'я тощо) а і будь-яка інформація, яка була передана суб'єктом даних у рамках використання певного сервісу. Зокрема, такою інформацією може бути – історія пошуку на певному вебсайті, поведінка та кліки у рамках певного ресурсу, серцевий ритм, який передається у рамках використання певного технічного засобу, тощо [10].

З іншого боку, інформація, яка є створеною контролером у рамках обробки таких даних, не є такою, що передана суб'єктом даних і може не передаватись у рамках такої категорії інформації. Таким чином, виходячи з положень Керівництва, «сира» інформація, що була передана суб'єктом даних, має бути передана новому контролеру у випадку відповідного запиту суб'єкта даних, а «збагачена» інформація, тобто така, яка являє собою певні висновки не має бути передана у випадку вказаного запиту [10].

Таким чином, станом на сьогодні, реалізація права на мобільність даних буде мати певні технічні перепони, але надання такого права суб'єктам даних це великий крок уперед у контексті реального захисту прав і свобод таких суб'єктів даних.

Висновки. Аналіз роз'яснень Робочої групи 29 щодо прозорості, оцінки впливу обробки даних, згоди та права на мобільність даних робить можливим розвиток подальших досліджень щодо можливості імплементації положень таких роз'яснень в українське законодавство, зокрема для забезпечення можливості реального впливу суб'єктів персональних даних на обробку таких даних компаніями контролерами (розпорядниками). Також певні практичні поради з керівництв можуть використовуватись компаніями резидентами України, які не підпадають під GDPR, для кращої роботи з персональними даними у контексті забезпечення та гарантування прав і свобод суб'єктів даних під час обробки персональних даних таких суб'єктів.

Перспективою подальших досліджень цього напрямку є детальне вивчення практичної реалізації положень вказаних керівництв компаніями, які підпадають під GDPR, та розробка рекомендацій щодо можливих змін в українське законодавство щодо захисту персональних даних на основі вивчення такого досвіду.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. General protection data regulation. URL: https://www.eugdpr.org/
2. Серёгин В.А. «BIG DATA»: Новая угроза для прайвеси в условиях информационного общества. Науковий вісник Ужгородського національного університету. Серія Право. 2015. № 35. Ч. 1 (Том 1). С. 93-97.
3. Брижко В.М. «Захист персональних даних: реалії та практика сучасності». Журнал «Інформація і право». 3(9)/2013. URL: http://ippi.org.ua/brizhko-vm-zakhist-personalnikh-danikh-realii-ta-praktika-suchasnosti
4. Баранов О.А. Напрями перспективних досліджень у галузі інформаційного права. Журнал «Інформація і право». 3(9)/2013. URL: http://ippi.org.ua/baranov-oa-napryami-perspektivnikh-doslidzhen-u-galuzi-informatsiinogo-prava-stor-15-31
5. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних. Інформаційна безпека людини, суспільства, держави. 2013. № 2. С. 97-103. URL: http://nbuv.gov.ua/UJRN/iblsd_2013_2_18
6. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46/ЄС Європейського Парламенту і Ради. URL: http://zakon2.rada.gov.ua/laws/show/994_242
7. Guidelines on Transparency under Regulation 2016/679. URL: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
8. Guidelines on consent under Regulation 2016/679. URL: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
9. Guidelines on Data Protection Impact Assessment (DPIA). URL: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
10. Guidelines on the right to Data portability (DPIA). URL: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233
11. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Верховна Рада України. Київ: Відомості верховної Ради України, 2010. №34. 481с.
12. Прозорість у рамках загального регулювання захисту даних (GDPR). Тарасюк А.В. Тези на «Міжнародній науково-практичній конференції «Правові та інституційні механізми забезпечення розвитку України в умовах європейської інтеграції» в Національному університеті «Одеська юридична академія» Південний регіональний центр Національної академії правових наук України 18 травня 2018 року.