Wybrane obowiązki strażników dostępu w świetle Aktu o rynkach cyfrowych z perspektywy ochrony danych osobowych

r.pr. *Krzysztof Wyderka*[1]

W ostatnich latach usługi cyfrowe, a zwłaszcza platformy internetowe odgrywają coraz ważniejszą rolę w europejskiej i światowej gospodarce. Możliwości, które stwarzają usługi platformowe w połączeniu z potencjalnymi, nieuczciwymi praktykami przedsiębiorstw świadczących te usługi, mogą niekorzystnie wpływać na konkurencję oraz prawa podstawowe użytkowników końcowych. Dostrzegalny jest również problem kontrolowania ważnych ekosystemów w gospodarce cyfrowej przez kilka dużych platform, które określane są mianem strażników dostępu (*gatekeepers*). W odpowiedzi na te wyzwania organy Unii Europejskiej ustanawiają nowe ramy prawne mające stworzyć bezpieczniejszą przestrzeń cyfrową oraz sprawiedliwe warunki działania w celu wspierania innowacji, wzrostu gospodarczego i konkurencyjności. Mając na uwadze fakt, że dane, w tym zwłaszcza dane osobowe, są kluczowym aktywem dla gospodarki cyfrowej, nowe akty prawne wprowadzają również obowiązki związane z przetwarzaniem danych osobowych. Wśród przyjętych w ostatnim czasie regulacji istotne miejsce zajmuje Akt o rynkach cyfrowych (DMA). Celem artykułu jest zidentyfikowanie wynikających z przepisów DMA kluczowych obowiązków strażników dostępu związanych z przetwarzaniem danych osobowych, określenie wzajemnych relacji pomiędzy przepisami Aktu o rynkach cyfrowych a przepisami RODO i wyzwań z nich wynikających, a także podjęcie próby wyjaśnienia wątpliwości.

Uwagi wstępne

W dniu 12.10.2022 r. w Dzienniku Urzędowym Unii Europejskiej zostało opublikowane rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z 14.9.2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych)[2]. Akt ten ma przyczynić się do zapewnienia sprawiedliwej i konkurencyjnej gospodarki cyfrowej, jednego z trzech głównych filarów strategii cyfrowej UE[3]. Ten cel, stosownie do treści art. 1 DMA, jest realizowany poprzez „ustanowienie zharmonizowanych przepisów służących zapewnieniu wszystkim przedsiębiorstwom kontestowalnych i uczciwych rynków w sektorze cyfrowym w całej Unii, na których działają strażnicy dostępu, z korzyścią dla użytkowników biznesowych i użytkowników końcowych".

Jeszcze w trakcie trwania procesu legislacyjnego w doktrynie wskazywano, że „przynależność projektowanej regulacji do określonej dziedziny prawa nie jest oczywista"[4]. Przepisy DMA przede wszystkim uzupełniają obecnie obowiązujące unijne i krajowe reguły konkurencji oraz zwalczania nieuczciwej konkurencji[5]. Zważywszy jednak, że aktywem o strategicznym znaczeniu dla gospodarki cyfrowej, dającym często przewagę konkurencyjną, są dane, w tym zwłaszcza dane osobowe, w DMA zawarto również przepisy regulujące obowiązki strażników dostępu związane z przetwarzaniem danych osobowych. Akt o rynkach cyfrowych wprowadza w szczególności ograniczenia w zakresie łączenia i wykorzystywania przez strażników dostępu danych osobowych użytkowników końcowych, reguluje uprawnienia związane z przenoszeniem i dostępem do danych, a także zawiera przepisy odnoszące się do profilowania.

Wzajemne oddziaływanie prawa ochrony danych osobowych i prawa ochrony konkurencji jest od dłuższego czasu zauważalne w treści aktów prawnych, w orzecznictwie, a także w praktyce organów antymonopolowych oraz organów ochrony danych. Wystarczy zauważyć, że przetwarzanie przez przedsiębiorców danych osobowych w sposób niezgodny z przepisami o ochronie danych osobowych może stanowić okoliczność o istotnym znaczeniu dla ustalenia naruszenia prawa ochrony konkurencji czy prawa ochrony konsumentów[6]. Dostęp do danych osobowych, ich zbieranie, łączenie

[1] Autor jest członkiem Okręgowej Izby Radców Prawnych w Warszawie. ORCID: 0000-0002-8793-1902. Przedstawione w artykule opinie stanowią wyraz osobistych poglądów autora i nie powinny być utożsamiane ze stanowiskiem żadnej organizacji lub instytucji, z którą autor był lub jest powiązany.

[2] Dz.Urz. UE L Nr 265, s. 1; dalej jako: DMA lub Akt o rynkach cyfrowych.

[3] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final 2020/0374 (COD), s. 3.

[4] *M. Namysłowska*, Zwalczanie nieuczciwych praktyk handlowych między przedsiębiorcami w prawie Unii Europejskiej. W poszukiwaniu modelu ochrony, Warszawa 2022, s. 536.

[5] Zob. *U. Czarnomska-Bokowy*, Prawo konkurencji a projekt rozporządzenia w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym – kto przypilnuje strażników?, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2022, Nr 1, s. 13.

[6] Zob. *I. Małobęcka-Szwast*, Oddziaływanie prawa ochrony danych osobowych (RODO) na prawo ochrony konkurencji i konsumentów, [w:] Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020 (red. *G. Sibiga*), MoP 2020, Nr 23, s. 92.

i analizowanie mogą sprzyjać wzmacnianiu pozycji rynkowej oraz negatywnie wpływać na konkurencję na rynkach cyfrowych, zwłaszcza w sytuacji, gdy przedsiębiorcy wykorzystują dane osobowe w sposób wykraczający poza cele, w których dane pierwotnie zebrano[7].

Nawet bez przeprowadzania pogłębionej analizy DMA możliwe jest stwierdzenie, że stosowanie tego rozporządzenia wpływa na operacje przetwarzania danych osobowych związane ze świadczeniem podstawowych usług platformowych. Treść niektórych przepisów oraz zastosowane konstrukcje, omówione w dalszej części artykułu, potwierdzają istnienie silnych związków między prawem ochrony danych osobowych a prawem ochrony konkurencji[8]. Doniosłe znaczenie w tym kontekście mają wzajemne relacje pomiędzy przepisami DMA a przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych)[9].

Zgodnie z motywem 12 DMA rozporządzenie to powinno mieć zastosowanie bez uszczerbku dla przepisów wynikających z innych aktów prawa UE regulujących niektóre aspekty świadczenia usług objętych DMA, w tym w szczególności przepisów RODO. Ponadto na podstawie art. 8 ust. 1 DMA, strażnicy dostępu są zobowiązani zapewnić, aby wdrożenie środków zapewniających przestrzeganie ich obowiązków ustanowionych w DMA było zgodne m.in. z przepisami RODO. Stosowanie jednak równocześnie przepisów obydwu rozporządzeń w niektórych wypadkach może okazać się problematyczne. Celowe jest zatem zbadanie obowiązków strażników dostępu związanych z przetwarzaniem danych osobowych oraz określenie wzajemnych relacji pomiędzy przepisami DMA a przepisami RODO, a także zidentyfikowanie wynikających z nich problemów interpretacyjnych i praktycznych oraz sformułowanie potencjalnych rozwiązań.

Strażnicy dostępu oraz podstawowe usługi platformowe

Kluczowe znaczenie dla ustalenia zakresu zastosowania przepisów DMA mają pojęcia strażnika dostępu oraz podstawowej usługi platformowej. W świetle definicji zawartej w art. 2 DMA strażnikiem dostępu jest „przedsiębiorstwo świadczące podstawowe usługi platformowe, które wskazano na podstawie art. 3". Jako strażnik dostępu może natomiast zostać wskazane przedsiębiorstwo, które łącznie spełnia trzy wymogi określone w art. 3 ust. 1 DMA. Przepisy DMA ustanawiają przy tym wzruszalne domniemania spełnienia przez przedsiębiorstwo poszczególnych wymogów warunkujących wskazanie go przez Komisję Europejską jako strażnika dostępu.

Pierwszym wymogiem jest wywieranie znaczącego wpływu na rynek wewnętrzny UE. Domniemywa się, że wymóg ten jest spełniony, jeżeli przedsiębiorstwo „uzyskało roczny obrót w Unii wynoszący co najmniej 7,5 mld euro w każdym z ostatnich trzech lat obrotowych lub jeżeli jego średnia kapitalizacja rynkowa lub równoważna rzeczywista wartość rynkowa wynosiła co najmniej 75 mld euro w ostatnim roku obrotowym oraz świadczy tę samą podstawową usługę platformową w co najmniej trzech państwach członkowskich". Drugie kryterium stanowi świadczenie podstawowej usługi platformowej będącej ważnym punktem dostępu, za pośrednictwem którego użytkownicy biznesowi docierają do użytkowników końcowych. Spełnienie tego wymogu domniemywa się, jeżeli przedsiębiorstwo „świadczy podstawową usługę platformową, z której w ostatnim roku obrotowym korzystało co najmniej 45 mln aktywnych miesięcznie użytkowników końcowych mających siedzibę lub miejsce pobytu w Unii oraz co najmniej 10 000 aktywnych rocznie użytkowników biznesowych z siedzibą w Unii". Trzeci wymóg polega na zajmowaniu przez przedsiębiorstwo ugruntowanej i trwałej pozycji w zakresie prowadzonej przez siebie działalności lub możliwości przewidzenia, że zajmie taką pozycję w niedalekiej przyszłości. Domniemywa się jego spełnienie, jeżeli progi dotyczące drugiego wymogu zostały osiągnięte w każdym z ostatnich trzech lat obrotowych.

Przedsiębiorstwo, które osiągnęło progi pozwalające uznać spełnienie wymogów kwalifikujących je jako strażnika dostępu, jest zobowiązane do bezzwłocznego powiadomienia o tym Komisji. Wraz z powiadomieniem przedsiębiorstwo może jednak przedstawić argumenty podważające domniemania. Istotne jest również, że Komisja może w dowolnym momencie, na wniosek lub z własnej inicjatywy, ponownie rozpatrzyć, zmienić lub uchylić decyzję o wskazaniu przedsiębiorstwa jako strażnika dostępu. Ponadto Komisja regularnie, co najmniej raz na trzy lata, dokonuje przeglądu w celu ustalenia, czy strażnicy dostępu spełniają wymogi określone w art. 3 ust. 1 DMA, a także sprawdza, przynajmniej co roku, czy nowe przedsiębiorstwa świadczące podstawowe usługi platformowe spełniają te wymogi. Obowiązkiem Komisji jest również publikowanie i aktualizowanie na bieżąco wykazu strażników dostępu oraz wykazu podstawowych usług platformowych.

[7] Zob. *L. Taylor*, *H. Mukiri-Smith*, *T. Petročnik*, *L. Savolainen*, *A. Martin*, (Re)making data markets: an exploration of the regulatory challenges, Law, Innovation and Technology 2022, vol. 14, iss. 2, s. 379.

[8] Zob. *J. Tielemans*, The EU's DMA and DSA: Why this should be of interest to privacy pros, https://iapp.org/news/a/developments-on-the-dma-and-dsa-why-this-should-be-of-interest-to-privacy-professionals/ (dostęp 5.5.2023 r.).

[9] Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

Akt o rynkach cyfrowych zawiera w art. 2 pkt 2 szeroki katalog podstawowych usług platformowych. Obejmuje on usługi pośrednictwa internetowego, wyszukiwarki internetowe, internetowe serwisy społecznościowe, usługi platformy udostępniania wideo, usługi łączności interpersonalnej niewykorzystujące numerów, systemy operacyjne, przeglądarki internetowe, wirtualnych asystentów, usługi przetwarzania w chmurze, a także internetowe usługi reklamowe, w tym sieci reklamowe, giełdy reklamowe i inne usługi pośrednictwa w zakresie reklam, świadczone przez przedsiębiorstwo, które świadczy dowolne podstawowe usługi platformowe.

Ograniczenia przetwarzania danych osobowych użytkowników końcowych

Akt o rynkach cyfrowych wprowadza ograniczenia w zakresie przetwarzania przez strażników dostępu danych osobowych użytkowników końcowych. Dotyczą one niektórych czynności oraz podstaw prawnych, na których może opierać się przetwarzanie. W art. 5 ust. 2 DMA ustanowiono katalog czynności przetwarzania, które co do zasady nie mogą być dokonywane przez strażnika dostępu, chyba że występuje jedna z określonych podstaw prawnych. W ten sposób ograniczono dopuszczalność przetwarzania przez strażników dostępu danych osobowych użytkowników końcowych w stosunku do zasad ogólnych wynikających z przepisów RODO.

Stosownie do treści art. 6 ust. 1 RODO przetwarzanie danych osobowych jest zgodne z prawem, gdy istnieje co najmniej jedna spośród sześciu wymienionych w tym przepisie podstaw prawnych. Tymczasem czynności przetwarzania określone w art. 5 ust. 2 DMA mogą opierać się jedynie na czterech podstawach prawnych. Stanowią je zgoda oraz przesłanki uregulowane art. 6 ust. 1 lit. c, d i e RODO, tj. niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze, niezbędność do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a także niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. W konsekwencji podstawą prawną realizacji czynności przetwarzania wymienionych w art. 5 ust. 2 DMA nie może być niezbędność do zawarcia umowy ani prawnie uzasadniony interes.

Wśród czterech czynności, których zgodnie z art. 5 ust. 2 DMA co do zasady nie może dokonywać strażnik dostępu, jako pierwszą wymieniono przetwarzanie do celów świadczenia internetowych usług reklamowych danych osobowych użytkowników końcowych, którzy korzystają ze świadczonych przez osoby trzecie usług wykorzystujących podstawowe usługi platformowe strażnika dostępu (art. 5 ust. 2 lit. a DMA). Rozwiązanie to ma w zamierzeniu unijnego prawodawcy niwelować potencjalną przewagę konkurencyjną uzyskiwaną przez strażników dostępu w związku z przetwarzaniem danych osobowych pochodzących od znacznie większej liczby użytkowników niż w wypadku innych przedsiębiorstw[10]. Przyjęta ostatecznie w toku prac legislacyjnych treść art. 5 ust. 2 lit. a DMA wzbudza jednak wątpliwości z perspektywy wyrażonej w RODO zasady ograniczenia celu przetwarzania[11]. Brzmienie tego przepisu, m.in. w angielskiej wersji językowej, może bowiem sugerować istnienie jednego, ogólnego celu przetwarzania danych polegającego na świadczeniu usług reklamowych[12]. Tymczasem funkcjonowanie reklamy internetowej w praktyce wiąże się z realizacją wielu czynności przetwarzania służących różnym celom. W konsekwencji istnieje potencjalnie możliwość podejmowania próby wykorzystania przez strażników dostępu treści art. 5 ust. 2 lit. a DMA jako argumentu uzasadniającego pozyskiwanie jednej, ogólnej zgody na przetwarzanie danych osobowych użytkownika końcowego w wielu różnych celach. Taka praktyka wzbudzałaby natomiast kontrowersje w kontekście wymogów dotyczących zgody wynikających z art. 7 RODO.

Zasadniczo, w świetle DMA nie jest ponadto dopuszczalne łączenie przez strażnika dostępu danych osobowych pochodzących z danej podstawowej usługi platformowej z danymi osobowymi pochodzącymi z innych podstawowych usług platformowych lub z dowolnych innych usług świadczonych przez strażnika dostępu lub z danymi osobowymi pochodzącymi z usług świadczonych przez osoby trzecie (art. 5 ust. 2 lit. b DMA). Akt o rynkach cyfrowych co do zasady zabrania również strażnikom dostępu logowania użytkowników końcowych do innych usług świadczonych przez strażnika dostępu, po to by łączyć dane osobowe (art. 5 ust. 2 lit. d DMA). Łączenie danych osobowych stanowi bowiem źródło uzyskiwania przez strażników dostępu przewagi konkurencyjnej[13]. Jednakże wprowadzenie zakazu w tym zakresie może niekorzystnie wpływać na bezpieczeństwo platform internetowych oraz realizację wynikającego z art. 32 ust. 1 RODO obowiązku wdrażania odpowiednich środków technicznych i organizacyjnych, zapewniających właściwy stopień bezpieczeństwa przetwarzania danych osobowych. Łączenie oraz porównywanie niektórych elementów danych służy bowiem wykrywaniu zagrożeń i zapobieganiu oszustwom lub innym,

[10] Akt o rynkach cyfrowych, motyw 36.

[11] Zob. *F. Pop*, The Digital Markets Act: more choice and improved data protection for users?, https://www.eipa.eu/blog/the-digital-markets-act-more-choice-and-improved-data-protection-for-users/ (dostęp 5.5.2023 r.).

[12] W angielskiej wersji językowej DMA użyto liczby pojedynczej („*purpose*") *„process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper*".

[13] Akt o rynkach cyfrowych, motyw 36.

niepożądanym działaniom[14]. Z reguły przetwarzanie danych osobowych w tym celu opiera się na prawnie uzasadnionym interesie (art. 6 ust. 1 lit. f RODO). Przepisy DMA wykluczają jednak możliwość powołania się na tę podstawę. W rezultacie, w praktyce konieczne może okazać się rozważenie przez strażników dostępu oparcia czynności łączenia danych osobowych na podstawie zgody, obowiązku prawnym, przesłance ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej albo interesie publicznym.

Kolejną czynność, której co do zasady nie może dokonywać strażnik dostępu, stanowi wykorzystywanie danych osobowych pochodzących z danej podstawowej usługi platformowej w ramach innych usług świadczonych oddzielnie przez strażnika dostępu, w tym innych podstawowych usług platformowych, i odwrotnie – wykorzystywanie danych osobowych pochodzących z takich innych usług w ramach podstawowej usługi platformowej (art. 5 ust. 2 lit. c DMA). Ograniczenie to odnosi się do sytuacji, w której strażnik dostępu odgrywa podwójną rolę – przedsiębiorstwa świadczącego na rzecz swoich użytkowników biznesowych podstawową usługę platformową (np. internetowe usługi reklamowe) oraz przedsiębiorstwa konkurującego z tymi samymi użytkownikami biznesowymi w oferowaniu takich samych lub podobnych usług lub produktów na rzecz tych samych użytkowników końcowych[15]. Zakaz ustanowiony w tym przepisie ma na celu uniemożliwienie strażnikom dostępu czerpania korzyści z pełnienia podwójnej roli. Dodatkowo, na podstawie art. 6 ust. 2 DMA, konkurując z użytkownikami biznesowymi, strażnik dostępu nie może wykorzystywać niedostępnych publicznie danych wygenerowanych lub dostarczonych przez użytkowników biznesowych w ramach korzystania przez nich z podstawowych usług platformowych lub usług świadczonych wraz z podstawowymi usługami platformowymi lub wspierających takie usługi, w tym danych wygenerowanych lub dostarczonych przez klientów użytkowników biznesowych. Dane niedostępne publicznie obejmują przy tym wszelkie zagregowane i niezagregowane dane wygenerowane przez użytkowników biznesowych, w tym m.in. dane dotyczące kliknięć, zapytań, wyświetleń i dane głosowe.

Zgoda użytkownika końcowego na niektóre czynności strażnika dostępu

Kluczowy z perspektywy strażników dostępu wyjątek od zakazu realizowania czynności wymienionych w art. 5 ust. 2 DMA wiąże się z zapewnieniem użytkownikom końcowym możliwości dokonania konkretnego wyboru i wyrażenia zgody w rozumieniu przepisów RODO. Konieczne jest zatem spełnienie przez strażników dostępu wymogów wynikających z art. 4 pkt 11 oraz art. 7 RODO. Koncepcja wykorzystania zgody jako zasadniczej podstawy dokonywania niektórych czynności określonych w DMA spotkała się z krytyką przedstawicieli doktryny oraz podmiotów prezentujących swoje stanowisko w toku prac legislacyjnych. W szczególności podnoszono, że poddanie otwarcia rynku danych wymogowi wyrażenia zgody przez użytkowników końcowych utrudni realizację głównych celów DMA[16]. Ponadto wskazywano, że rozwiązanie to może sprzyjać zjawisku tzw. zmęczenia zgodą (*consent fatigue*) oraz łatwemu pozyskiwaniu przez strażników dostępu zgód użytkowników końcowych[17]. Dostrzegano również trudności o charakterze technicznym związane z wdrożeniem efektywnych procesów wycofania zgody na wielu platformach i w wielu przedsiębiorstwach. Ponadto z uwagi na wyraźną dysproporcję sił pomiędzy użytkownikiem końcowym a strażnikiem dostępu wyrażano wątpliwości dotyczące możliwości zapewnienia faktycznej dobrowolności zgody.

Wymienione ryzyka w pewnym stopniu mogą zostać ograniczone w związku z zawarciem przez unijnego prawodawcę w preambule DMA wskazań odnoszących się do procesu zarządzania zgodami użytkowników końcowych. Zwrócono w niej w szczególności uwagę na powinność proaktywnego przedstawiania przez strażnika dostępu użytkownikowi końcowemu „przyjaznego dla użytkownika rozwiązania umożliwiającego wyrażenie, zmianę lub cofnięcie zgody w sposób wyraźny, jasny i prosty”[18]. Strażnicy dostępu powinni dawać użytkownikom końcowym możliwość swobodnego decydowania o uczestnictwie w praktykach polegających na wykonywaniu czynności określonych w art. 5 ust. 2 DMA. Służyć temu ma oferowanie mniej spersonalizowanego, ale równoważnego rozwiązania, a także nieuzależnianie korzystania z podstawowej usługi platformowej lub niektórych jej funkcjonalności od uzyskania zgody użytkownika końcowego[19]. Ponadto w momencie wyrażania zgody użytkownik końcowy powinien zostać poinformowany o skutkach jej niewyrażenia, w tym o otrzymaniu mniej spersonalizowanej oferty, a także o tym, że „podstawowa usługa platformowa pozostanie niezmieniona i że żadne funkcjonalności nie zostaną usunięte”. Wyjątek dotyczy sytuacji braku możliwości wyrażenia zgody bezpośrednio w ramach podstawowej usługi

[14] Zob. *B. Bellamy, A. Simpson*, How the EU Digital Markets Act Affects GDPR, https://www.lawyer-monthly.com/2022/08/how-the-eu-digital-markets-act-affects-gdpr/ (dostęp 5.5.2023 r.).

[15] Akt o rynkach cyfrowych, motywy 46 i 47.

[16] Zob. Bridging the DMA and the GDPR – Comments by the Centre for Information Policy Leadership on the Data Protection Implications of the Draft Digital Markets Act, s. 12, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_data_protection_implications_of_the_draft_digital_markets_act__6_dec_2021_.pdf (dostęp 5.5.2023 r.).

[17] Zob. *R. Podszun*, Should Gatekeepers Be Allowed to Combine Data? – Ideas for Art. 5(a) of the Draft Digital Markets Act, GRUR International 2022, vol. 71, iss. 3, s. 199.

[18] Akt o rynkach cyfrowych, motyw 37.

[19] Akt o rynkach cyfrowych, motyw 36.

platformowej strażnika dostępu. Wówczas wymagane jest umożliwienie użytkownikom końcowym wyrażenia zgody za pośrednictwem korzystającej z podstawowej usługi platformowej usługi świadczonej przez osobę trzecią, „aby zezwolić strażnikowi dostępu na przetwarzanie danych osobowych do celów świadczenia internetowych usług reklamowych”[20].

Pewne wątpliwości wzbudza treść art. 5 ust. 2 akapit drugi DMA, a zwłaszcza zawarte w nim sformułowanie dotyczące „wyrażenia zgody do celu akapitu pierwszego”[21]. Akapit pierwszy obejmuje bowiem cztery różne czynności mogące służyć realizacji wielu celów przetwarzania danych osobowych. Dlatego też w trakcie prac legislacyjnych podnoszono, że proponowana treść art. 5 ust. 2 akapit drugi DMA tworzy lukę prawną i stawia strażników dostępu w korzystnej sytuacji, umożliwiając im pozyskiwanie jednej, ogólnej zgody obejmującej wiele czynności oraz celów przetwarzania[22]. W tym samym przepisie wyraźnie ustanowiono jednak wymóg „zapewnienia możliwości dokonania konkretnego wyboru”. Umożliwienie wyrażenia zgody wyłącznie na wszystkie czynności określone w art. 5 ust. 2 DMA byłoby zatem niewystarczające. Zważywszy, że zgoda wyrażana przez użytkownika końcowego powinna spełniać wymogi wynikające z przepisów RODO, strażnik dostępu powinien umożliwić wyrażenie zgody na poszczególne czynności przetwarzania realizowane w określonych celach. Biorąc pod uwagę możliwości techniczne, którymi dysponują podmioty posiadające status strażników dostępu, uzasadnione jest również oczekiwanie zapewnienia odpowiedniej dostępności oraz jasnego i prostego języka.

Preambuła Aktu o rynkach cyfrowych zawiera również wskazania odnoszące się do cofnięcia zgody. Przede wszystkim powinno być ono równie proste co jej wyrażenie. Ponadto „strażnicy dostępu nie powinni projektować, organizować lub obsługiwać swoich interfejsów internetowych w sposób, który w drodze wprowadzenia w błąd, manipulacji lub w inny sposób istotnie zakłóca lub ogranicza zdolność użytkowników końcowych do swobodnego wyrażenia zgody”. Akt o rynkach cyfrowych ustanawia także ograniczenia w zakresie występowania przez strażników dostępu z wnioskiem o wyrażenie zgody. W świetle art. 5 ust. 2 akapit drugi DMA, jeżeli użytkownik końcowy odmówił wyrażenia zgody lub cofnął taką zgodę, strażnik dostępu nie może występować z ponownym wnioskiem o wyrażenie zgody do tego samego celu częściej niż raz w ciągu roku.

Szczegółowe wskazania dotyczące zarządzania zgodami użytkowników końcowych zawarte w preambule DMA nie gwarantują realizacji celów Aktu o rynkach cyfrowych, ale mogą mieć istotny wpływ na stosowanie przepisów rozporządzenia. Jeszcze większe znaczenie dla zapewnienia kontestowalności rynków cyfrowych oraz ochrony danych osobowych użytkowników będzie mieć jednak praktyka organów nadzorczych.

Zapewnienie możliwości przenoszenia danych

Jednym z instrumentów sprzyjających synergii pomiędzy prawem ochrony danych osobowych a prawem konkurencji jest uprawnienie do przenoszenia danych[23]. Dotychczas istniejące mechanizmy w tym zakresie były jednak niejednokrotnie oceniane w literaturze jako niewystarczające, aby przyczynić się do przeciwdziałania monopolizacji rynków cyfrowych przez duże platformy internetowe[24]. W Akcie o rynkach cyfrowych ustanowiono obowiązek zapewnienia przez strażnika dostępu możliwości przenoszenia danych dostarczonych przez użytkownika końcowego lub wygenerowanych przez użytkownika końcowego w ramach korzystania z podstawowej usługi platformowej. Stosownie do treści art. 6 ust. 9 DMA obowiązek ten obejmuje zapewnienie nieodpłatnych narzędzi ułatwiających przenoszenie danych oraz stałego dostępu do danych w czasie rzeczywistym. Uprawnienie do przenoszenia danych może być realizowane przez użytkownika końcowego oraz upoważnione przez niego osoby trzecie. W preambule DMA wskazano, że obowiązek zapewnienia skutecznego przenoszenia danych wynikający z przepisów tego rozporządzenia stanowi uzupełnienie prawa do przenoszenia danych osobowych uregulowanego w RODO[25]. Z uwagi na pewne elementy wspólne i powiązania pomiędzy obiema konstrukcjami ich analiza ma istotne znaczenie praktyczne.

Szczególnie wyraźna różnica pomiędzy porównywanymi instytucjami dotyczy zakresu ich zastosowania. W odróżnieniu od prawa do przenoszenia danych osobowych uregulowanego w art. 20 RODO obowiązek zapewnienia możliwości przenoszenia danych wynikający z art. 6 ust. 9 DMA obejmuje dane dostarczone przez użytkownika końcowego lub wygenerowane w toku działalności użytkownika końcowego w ramach korzystania z podstawowej usługi platformowej, a zatem nie tylko dane osobowe. Ponadto prawo osoby, której dane dotyczą, zostało w art. 20 ust. 1 RODO ograniczone do danych, które osoba ta „dostarczyła administratorowi”. Stosownie do treści wytycznych Grupy Roboczej Art. 29 sfor-

[20] Akt o rynkach cyfrowych, motyw 37.

[21] W angielskiej wersji językowej DMA: „*consent given for the purposes of the first subparagraph*”.

[22] Zob. EPC & DCN statement on the DMA, https://www.epceurope.eu/post/epc-dcn-statement-on-the-dma, https://www.epceurope.eu/post/epc-dcn-statement-on-the-dma (dostęp 5.5.2023 r.).

[23] Zob. *W. Kerber, L. Specht -Riemenschneider*, Synergies between Data Protection Law and Competition Law, s. 43, https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf (dostęp 5.5.2023 r.).

[24] Zob. *I. Graef, J. Prüfer*, Governance of data sharing: A law & economics proposal, Research Policy 2021, vol. 50, iss. 9, s. 12.

[25] Akt o rynkach cyfrowych, motyw 59.

mułowanie to oznacza, że uprawnienie osoby, której dane dotyczą, ma zastosowanie do danych osobowych „aktywnie i świadomie" przekazanych przez tę osobę, a także do danych osobowych, „które wynikają z obserwacji działań użytkowników, takich jak surowe dane przetwarzane przez inteligentny licznik lub inne rodzaje podłączonych obiektów, dzienniki aktywności, historia korzystania ze strony internetowej lub działań związanych z wyszukiwaniem"[26]. Zakres prawa do przenoszenia danych osobowych nie obejmuje jednak danych wywnioskowanych i pochodnych, tworzonych przez administratora na podstawie danych przekazanych przez osobę, której dane dotyczą[27]. Takie ograniczenie nie występuje natomiast w wypadku obowiązku strażnika dostępu określonego w art. 6 ust. 9 DMA. Pewien wpływ na zakres danych objętych zakresem analizowanych instytucji ma również podstawa prawna przetwarzania danych. Prawo do przenoszenia danych zgodnie z art. 20 ust. 1 RODO znajduje zastosowanie wyłącznie, gdy przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy. Tymczasem obowiązek zapewnienia możliwości przenoszenia danych wynikający z przepisów DMA istnieje również w wypadku przetwarzania danych osobowych na innej podstawie prawnej.

Kolejne różnice dotyczą szczegółowych warunków realizacji obydwu uprawnień. W Akcie o rynkach cyfrowych wyraźnie wskazano, że możliwość przenoszenia danych powinna być zapewniona przez strażnika dostępu nieodpłatnie. Natomiast zgodnie z art. 12 ust. 5 RODO na zasadzie wyjątku, „jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań".

W preambułach obydwu rozporządzeń zawarto ponadto wskazania odnoszące się do warunków technicznych realizacji uprawnień związanych z przenoszeniem danych. Również w tym zakresie dostrzegalne są różnice. W wypadku prawa do przenoszenia danych osobowych osoba, której dane dotyczą, powinna mieć możliwość otrzymania danych osobowych „w ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego i interoperacyjnym formacie oraz przesyłania ich innemu administratorowi"[28]. Ponadto w preambule RODO postuluje się zachęcanie administratorów danych do opracowywania interoperacyjnych formatów, które umożliwiają przenoszenie danych[29]. Grupa Robocza Art. 29 wskazuje przy tym jako dobrą praktykę rozwijanie przez administratorów środków, które przyczynią się do odpowiadania na wnioski o przeniesienie danych takich jak narzędzia do pobierania danych oraz interfejsy programowania aplikacyjnego[30]. Znacznie dalej idące wymagania techniczne sformułowano natomiast w preambule DMA odnośnie do obowiązku zapewnienia możliwości przenoszenia danych. Dane powinny być otrzymywane w formacie umożliwiającym natychmiastowe uzyskanie do nich dostępu przez użytkownika końcowego lub osobę trzecią, do której są przenoszone[31]. Przede wszystkim jednak od strażników dostępu oczekiwane jest zapewnienie możliwości „ciągłego i przebiegającego w czasie rzeczywistym swobodnego przenoszenia danych", które jest realizowane „za pomocą odpowiednich i wysokiej jakości środków technicznych, takich jak interfejsy programowania aplikacyjnego"[32].

Z uwagi na liczne różnice dotyczące zwłaszcza zakresu zastosowania oraz warunków realizacji obydwu analizowanych uprawnień trudno jest podzielić stanowisko, że obowiązek zapewnienia możliwości przenoszenia danych stanowi jedynie uzupełnienie prawa do przenoszenia danych ustanowionego w RODO. W rzeczywistości uprawnienie przysługujące użytkownikowi końcowemu na podstawie art. 6 ust. 9 DMA jest znacznie bardziej rozbudowane w stosunku do prawa wynikającego z art. 20 RODO. Wyzwaniem może być w praktyce prawidłowa interpretacja intencji użytkownika końcowego występującego z żądaniem oraz właściwe jego zakwalifikowanie przez strażnika dostępu. Potencjalne rozwiązanie tego problemu mogłoby polegać w szczególności na wdrażaniu przez strażników dostępu rozwiązań technicznych umożliwiających informowanie w przejrzysty sposób użytkownika końcowego o obydwu uprawnieniach oraz dokonywanie świadomego wyboru prawa, z którego użytkownik chce skorzystać.

Zapewnienie dostępu do danych

Kolejny obowiązek strażników dostępu, który może mieć istotne znaczenie dla zapewnienia kontestowalności rynków cyfrowych, a jednocześnie uwidacznia rolę danych, w tym danych osobowych, został ustanowiony w art. 6 ust. 10 DMA. Przepis ten reguluje zapewnienie użytkownikom biznesowym i osobom trzecim przez nich upoważnionym dostępu do danych i możliwości korzystania z nich. Obowiązek zapewnienia dostępu obejmuje dane dostarczane lub generowane w ramach korzystania przez użytkowników biznesowych oraz przez użytkowników końcowych korzystających z produktów dostarczanych lub usług świadczonych przez użytkowników biznesowych z podstawowych usług platformowych lub usług świadczonych wraz z podstawowymi usługami platformowy-

[26] Article 29 Working Party, Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01, s. 10.
[27] *Ibidem.*
[28] RODO, motyw 68.
[29] *Ibidem.*
[30] Article 29 Working Party, Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01, s. 3.
[31] Akt o rynkach cyfrowych, motyw 59.
[32] *Ibidem.*

mi lub wspierających takie usługi. Stosownie do treści art. 6 ust. 10 DMA dostęp ten powinien być „skuteczny, wysokiej jakości i stały", a ponadto zapewniony w czasie rzeczywistym oraz ma obejmować dane zagregowane i niezagregowane, w tym dane osobowe. Jednakże w wypadku danych osobowych strażnik dostępu jest zobowiązany zapewnić dostęp i możliwość korzystania z nich wyłącznie, gdy są one „bezpośrednio powiązane z faktem korzystania przez użytkowników końcowych z produktów lub usług" oferowanych przez użytkownika biznesowego za pośrednictwem podstawowej usługi platformowej. Ponadto warunkiem udostępniania danych osobowych jest wyrażenie na to zgody przez użytkowników końcowych.

Podobnie jak w wypadku zapewnienia możliwości przenoszenia danych, również w odniesieniu do obowiązku zapewnienia dostępu do danych, unijny prawodawca zawarł w preambule DMA wskazania dotyczące warunków realizacji tego obowiązku. Przede wszystkim nie jest dopuszczalne stosowanie przez strażnika dostępu jakichkolwiek ograniczeń, w tym w szczególności umownych, w celu uniemożliwienia użytkownikom biznesowym dostępu do danych[33]. Ponadto strażnik dostępu powinien umożliwiać użytkownikom biznesowym uzyskanie zgody użytkowników końcowych na udzielenie dostępu, jeśli jest ona wymagana. Zapewnienie stałego dostępu do danych w czasie rzeczywistym powinno być realizowane za pomocą odpowiednich środków technicznych, takich jak np. interfejsy programowania aplikacyjnego oraz zintegrowane narzędzia dla „drobnych użytkowników biznesowych"[34].

Regulacja zawarta w art. 6 ust. 10 DMA wzbudza liczne wątpliwości w kontekście ochrony danych osobowych. Ograniczenie zakresu zastosowania obowiązku zapewnienia dostępu do danych „bezpośrednio powiązanych z faktem korzystania przez użytkowników końcowych z produktów lub usług" koresponduje z uregulowaną w art. 5 ust. 1 lit. c RODO zasadą minimalizacji danych. Jednakże poważnym wyzwaniem może być w praktyce określenie, które dane są „bezpośrednio powiązane". Ponadto, wobec braku precyzyjnej regulacji w części normatywnej DMA oraz ewentualnych wskazań w jego preambule, kwestię dyskusyjną może stanowić interpretacja sformułowania „dane dostarczane lub generowane w ramach korzystania". Zwłaszcza zakres drugiej kategorii wydaje się niejasny. Nie jest bowiem oczywiste, czy zakres obowiązku udostępnienia danych obejmuje poza danymi przekazanymi przez użytkownika również np. dane wynikające z obserwacji działań użytkowników, dane wywnioskowane i pochodne, tworzone na podstawie danych przekazanych przez użytkownika końcowego[35]. Z perspektywy strażników dostępu konkurujących z użytkownikami biznesowymi niewątpliwie korzystne jest ograniczenie do minimum zbioru danych podlegających udostępnieniu. Z uwagi na sprzeczne interesy określenie zakresu danych objętych obowiązkiem udostępnienia może zatem stanowić w praktyce przedmiot sporu pomiędzy strażnikami dostępu oraz użytkownikami biznesowymi.

Potencjalnym źródłem napięć w relacjach pomiędzy strażnikami dostępu a użytkownikami biznesowymi może być również ustalenie treści i sposobu wyrażenia przez użytkowników końcowych zgody na udostępnienie danych. Trudności w tym zakresie wynikają m.in. z faktu, że udostępnienie danych na podstawie art. 6 ust. 10 DMA może obejmować różne zbiory danych i cele przetwarzania, w których dane wykorzystują użytkownicy biznesowi. Natomiast w świetle wymogów wynikających z przepisów RODO użytkownicy końcowi powinni zostać poinformowani o „tożsamości administratora oraz zamierzonych celach przetwarzania danych osobowych", a ponadto oświadczenie o wyrażeniu zgody powinno mieć „zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem"[36]. W tym kontekście dużym wyzwaniem może okazać się w praktyce wdrażanie przez strażników dostępu odpowiednich rozwiązań technicznych, umożliwiających użytkownikom biznesowym uzyskiwanie zgód spełniających wymogi ustanowione w RODO.

W art. 6 ust. 11 DMA uregulowano ponadto obowiązek zapewnienia „przedsiębiorstwu będącemu dostawcą wyszukiwarek internetowych, które jest osobą trzecią" dostępu do „danych dotyczących plasowania, zapytań, kliknięć i wyświetleń związanych z nieodpłatnym i płatnym wyszukiwaniem, wygenerowanych przez użytkowników końcowych przy wykorzystaniu jego wyszukiwarek internetowych". Ustanowiono przy tym wymóg poddania anonimizacji wszelkich danych wyszukiwania będących danymi osobowymi. Realizacja skutecznej anonimizacji danych stanowi poważny problem praktyczny, a udostępnianie danych wyszukiwania może wiązać się z ryzykiem ponownej identyfikacji osoby, której dane dotyczą. Na to ryzyko zwrócił uwagę w toku prac legislacyjnych m.in. EIOD[37], rekomendując uwzględnienie w motywach DMA wskazania, zgodnie z którymi strażnik dostępu powinien być w stanie wykazać, że zanonimizowane dane dotyczące zapytań, kliknięć i wyświetleń zostały odpowiednio przetestowane pod kątem ewentualnych zagrożeń związanych z ponowną identyfikacją[38].

W preambule DMA określono ogólne warunki dotyczące dokonywania anonimizacji danych osobowych. W szczególności wskazano, że odpowiednia anomimizacja polega na

[33] Akt o rynkach cyfrowych, motyw 60.
[34] *Ibidem*.
[35] Zob. Bridging the DMA and the GDPR..., s. 9.
[36] RODO, motyw 42.
[37] Europejski Inspektor Ochrony Danych.
[38] Zob. EDPS, Opinion 2/2021 on the Proposal for a Digital Markets Act, s. 12.

nieodwracalnej zmianie danych osobowych w taki sposób, że „informacje nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, lub gdy dane osobowe zostały zanonimizowane w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można ich zidentyfikować”[39]. Ponadto zawarto wskazanie, w świetle którego strażnik dostępu powinien zapewnić ochronę „przed zagrożeniami związanymi z deanonimizacją, za pomocą odpowiednich środków, takich jak anonimizacja takich danych osobowych, bez znacznego obniżania jakości lub przydatności danych”[40]. Treść preambuły DMA może w pewnym stopniu przeciwdziałać praktyce nadmiernego ograniczania zakresu i modyfikacji danych wyszukiwania podlegających udostępnieniu, jednak sposób realizacji anonimizacji danych może być przedmiotem sporu pomiędzy strażnikami dostępu, a dostawcami wyszukiwarek.

Informowanie o praktykach w zakresie profilowania

Akt o rynkach cyfrowych wprowadza również nowe obowiązki strażników dostępu związane z profilowaniem konsumentów. Stanowią one kolejny element złożonego systemu norm prawnych odnoszących się do transparentności algorytmicznego przetwarzania danych osobowych[41]. Poza przepisami DMA w wypadku stosowania przez strażników dostępu profilowania konieczne może okazać się również uwzględnienie m.in. obowiązków określonych w art. 13, 15 i 22 RODO, a także obowiązków dostawców usług pośrednich w zakresie przejrzystości wynikających z przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19.10.2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)[42].

Na podstawie art. 15 ust. 1 DMA strażnik dostępu powinien w terminie sześciu miesięcy od dnia wskazania przedsiębiorstwa jako strażnika dostępu przedłożyć Komisji Europejskiej „poddany niezależnemu audytowi opis technik profilowania konsumentów, z których korzysta w odniesieniu do lub w ramach świadczonych przez siebie podstawowych usług platformowych wymienionych w decyzji o wskazaniu”. Opis ten Komisja przekazuje następnie EROD[43]. Ponadto stosownie do treści art. 15 ust. 3 DMA obowiązkiem strażnika dostępu jest publiczne udostępnienie podsumowania opisu poddanego audytowi, a także aktualizowanie opisu i podsumowania co najmniej raz w roku. Istotne znaczenie dla zawartości udostępnianego publicznie podsumowania może mieć wynikające z przepisów Aktu o rynkach cyfrowych uprawnienie strażnika dostępu „do uwzględnienia konieczności zachowania swoich tajemnic handlowych”.

Regulacja zawarta w art. 15 DMA ma na celu zapewnienie przejrzystości oraz wywieranie presji na strażników dostępu, skłaniającej ich do ograniczenia stosowania „głębokiego profilowania konsumentów”[44]. W preambule tego rozporządzenia zawarto wskazania dotyczące treści opisu założeń profilowania. Powinien on obejmować informację o przetwarzaniu danych osobowych, o celu sporządzania i wykorzystywania profilu, czasie profilowania, wpływie na usługi świadczone przez strażnika dostępu, krokach podejmowanych w celu zapewnienia użytkownikom końcowym wiedzy na temat wykorzystania profilowania, a także krokach podejmowanych w celu uzyskania ich zgody lub w celu zapewnienia im możliwości odmowy lub cofnięcia zgody[45].

Podsumowanie

Akt o rynkach cyfrowych ustanawia liczne obowiązki strażników dostępu związane z przetwarzaniem danych osobowych. Ich realizacja może w praktyce okazać się poważnym wyzwaniem i wzbudzać kontrowersje. Wynika to z faktu, że stosowanie niektórych przepisów DMA prawdopodobnie będzie napotykać problemy interpretacyjne oraz trudności o charakterze technicznym. Mogą one występować zwłaszcza w kontekście próby realizacji obowiązków strażników dostępu wynikających z DMA bez uszczerbku dla przepisów RODO. Ponadto z uwagi na nieprecyzyjność regulacji przynajmniej do momentu opublikowania wytycznych lub stanowisk organów nadzorczych, a także ewentualnych rozstrzygnięć w postępowaniu przed Trybunałem Sprawiedliwości interpretacja przepisów DMA może być przedmiotem licznych sporów pomiędzy strażnikami dostępu a użytkownikami biznesowymi i użytkownikami końcowymi.

[39] Akt o rynkach cyfrowych, motyw 61.
[40] *Ibidem*.
[41] Zob. *M. Eifert, A. Metzger, H. Schweitzer, G. Wagner*, Taming the giants: The DMA/DSA package, Common Market Law Review 2021, vol. 58, iss. 4, s. 1016.
[42] Dz.Urz. UE L Nr 277, s. 1 – tzw. Akt o usługach cyfrowych.
[43] Europejska Rada Ochrony Danych.
[44] Akt o rynkach cyfrowych, motyw 72.
[45] *Ibidem*.

Słowa kluczowe: dane osobowe, Akt o rynkach cyfrowych, strażnicy dostępu, podstawowa usługa platformowa, przenoszenie danych, profilowanie.

Selected obligations of gatekeepers in the light of the Digital Markets Act from a perspective of personal data protection

In recent years, digital services and in particular online platforms have played an increasingly important role in the European and global economy. Opportunities created by platform services, combined with potential ill practices of enterprises providing these services, can adversely affect competition and the fundamental rights of end users. There is also a perceivable problem of control of important ecosystems in the digital economy by few large platforms, which are referred to as gatekeepers. In response to these challenges, European Union bodies are setting up a new legal framework to create a more secure digital space and a fair play field to foster innovation, economic growth and competitiveness. Bearing in mind the fact that data, and in particular personal data, is a key asset for the digital economy, new legislation also establishes obligations related to the processing of personal data. Among the recently adopted regulations, the Digital Markets Act (DMA) plays an important role. The purpose of this article is to identify the key obligations of gatekeepers relating to the processing of personal data arising from the provisions of DMA, to identify the interplay between the provisions of the Digital Markets Act and the provisions of the GDPR and the challenges arising from it, and to attempt to clarify doubts.

Keywords: personal data, Digital Markets Act, gatekeepers, core platform service, data portability, profiling.