KATARZYNA MORAWSKA

SPRZECIW WOBEC PRZETWARZANIA DANYCH OSOBOWYCH JAKO WYRAZ PRAWA DO PRYWATNOŚCI

STRESZCZENIE

Ciągły rozwój technologii jest możliwy, dzięki przetwarzaniu coraz to większej ilości danych, które umożliwiają między innymi tworzenie precyzyjnych profili użytkowników danej usługi. W czasach, w których mniej lub bardziej świadomie decydujemy się na dzielenie się swoją prywatną sferą, prawo do prywatności wymaga szczególnej ochrony. Z prawem tym nieodłącznie związana jest potrzeba sprawowania faktycznej kontroli nad przekazywanymi danymi co wiąże się z kolei z koniecznością budowania świadomości na temat tego, w jakich celach oraz w jaki sposób dane osobowe mogą być przez administratorów przetwarzane.

Główna teza publikacji sprowadza się do stwierdzenia, że prawo do sprzeciwu wobec przetwarzania danych stanowi wyraz prawa do prywatności rozumianego jako prawo do kontrolowania procesów przetwarzania danych osobowych i sprawowania realnej kontroli nad tym, w jaki sposób dane osobowe mogą być przez administratorów danych wykorzystywane. Uprawnienia, w tym prawo do sprzeciwu, jak i pozostałe instytucje chroniące prywatność zgodnie z RODO nie będą jednak odpowiednio realizowane i stosowane, jeśli nie będą ściśle związane z mechanizmami ochronnymi – to novum, które wprowadza RODO, by zapewnić większą skuteczność praw i obowiązków ustanowionych w tym akcie prawnym.

SŁOWA KLUCZOWE

Przetwarzanie danych, ochrona danych, prawo do prywatności

WPROWADZENIE

Ciągły rozwój technologii jest możliwy, dzięki przetwarzaniu coraz to większej ilości danych, które umożliwiają między innymi tworzenie precyzyjnych profili użytkowników danej usługi – osób, których dotyczą dane osobowe. W czasach, w których mniej lub bardziej świadomie decydujemy się na dzielenie się swoją prywatną sferą, prawo do prywatności wymaga szczególnej ochrony. Z prawem tym nieodłącznie związana jest potrzeba sprawowania faktycznej kontroli nad przekazywanymi danymi co wiąże się z kolei z koniecznością budowania świadomości na temat tego, w jakich celach oraz w jaki sposób dane osobowe mogą być przez administratorów przetwarzane.

Konieczność zapewnienia skutecznej ochrony danych osobowych i odzyskania kontroli nad procesem przetwarzania danych przez osoby, których dane dotyczą jest podnoszona od wielu lat jako kluczowe wyzwanie dla zapewnienia prawa do prywatności[1]. Dyrektywa 95/46/WE[2], która stanowiła podstawę prawodawstw krajowych do 25 maja 2018r. nie odpowiadała na potrzeby współczesnego społeczeństwa i wyzwania stawiane przez współczesną technologie. Próbą dostosowania przepisów unijnych z obszaru ochrony danych osobowych do tych wyzwań jest ogólnoeuropejska reforma.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej jako „RODO")[3] nakłada szereg nowych obowiązków na administratorów danych osobowych celem zapewnienia skuteczniejszej ochrony i bezpieczeństwa danych przez nich przetwarzanych oraz przewiduje odpowiedzialność za naruszenie przepisów RODO (odpowiedzialność o charakterze karnym, administracyjnym i cywilnym).

Osoby, których dane dotyczą na mocy RODO otrzymały także szereg nowych uprawnień, dzięki którym możliwe jest skuteczniejsze dochodzenie praw im przysługujących. Na przykładzie prawa do sprzeciwu wobec przetwarzanych danych w publikacji zostanie

[1] Komunikat prasowy Komisji Europejskiej w sprawie lepszej ochrony danych z wykorzystaniem technologii na rzecz ochrony prywatności, Bruksela 2017, dostęp na 15.07.2019r.
[2] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. WE 1995 Nr L 281/31.
[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz. Urz. UE L 2016, Nr 119, s.1.

omówiony jeden z najważniejszych aspektów reformy ochrony danych, szczególnie istotny w ocenie autorki w kontekście analizy prawa do prywatności, to jest zagadnienie wzmocnienia praw osób, których dane dotyczą określonych w RODO.

Główna teza publikacji sprowadza się w związku z powyższym do stwierdzenia, że prawo do sprzeciwu wobec przetwarzania danych stanowi wyraz prawa do prywatności rozumianego jako prawo do kontrolowania procesów przetwarzania danych osobowych i sprawowania realnej kontroli nad tym, w jaki sposób dane osobowe mogą być przez administratorów danych wykorzystywane.

Uprawnienia, w tym prawo do sprzeciwu, jak i pozostałe instytucje chroniące prywatność zgodnie z RODO nie będą jednak odpowiednio realizowane i stosowane, jeśli nie będą ściśle związane z mechanizmami ochronnymi – to novum, które wprowadza RODO, by zapewnić większą skuteczność praw i obowiązków ustanowionych w tym akcie prawnym.

W związku z powyższym w publikacji analizie zostaną poddane także sankcje administracyjne, które organ nadzorczy może nałożyć na administratorów danych osobowych lub podmioty przetwarzające dane za nieprzestrzeganie przepisów dotyczących praw podmiotów danych.

PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ JAKO WYRAZ POSTULATU OCHRONY PRAWA DO PRYWATNOŚCI

Jednym z celów RODO jest, zgodnie z art. 1 ust. 2, konieczność realizacji podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych[4]. Postulat umacniania praw osób, których dane dotyczą wiąże się z koniecznością jednoczesnego umacniania skuteczności ich realizacji, który został między innymi zapewniony poprzez wprowadzenie wysokich kar administracyjnych, ale także poprzez wzmocnienie wagi informowania podmiotów danych o katalogu informacji, który administrator danych osobowych jest obowiązany przekazać.

Obowiązek ten określa art. 13 i 14 RODO, które to przepisy stanowią wyraz realizacji zasad rzetelnego i przejrzystego przetwarzania danych, które wymagają by osoba, której dane

[4] A. Grzelak, *Główne cele ogólnego rozporządzenia o ochronie danych*, [w:] red. M. Kawecki, T. Osiej, *Ogólne rozporządzenie o ochronie danych - Wybrane zagadnienia*, s. 18.

dotyczą była informowana o prowadzeniu operacji przetwarzania i o jej celach, a także o prawach przysługujących podmiotom danych (motyw 60 RODO). Administrator powinien podać osobie, której dane dotyczą inne niezbędne informacje, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Przykładowo administrator powinien poinformować osobę, której dane dotyczą o fakcie profilowania oraz o konsekwencjach takiego profilowania. Klauzula obowiązku informacyjnego może być odpowiednim miejscem na zrealizowanie postanowień art. 22 RODO.

W kontekście analizy prawa do sprzeciwu warto podkreślić, że podmiot danych ma uprawnienie do sprzeciwienia się wobec profilowania jego danych osobowych. Aby z tego uprawnienia skorzystać osoba, której dane dotyczą powinna na etapie zbierania danych, w ramach klauzuli obowiązku informacyjnego, zostać poinformowana o takiej formie przetwarzania danych osobowych. Podmiotom danych należy umożliwić realizacje prawa do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu (w tym profilowaniu) i która wywołuje wobec tych osób skutki prawne lub w podobny sposób istotnie na nich wpływa. Podkreśla się zatem, że art. 21 ust. 4 RODO nakłada na administratora obowiązek informowania osoby, której dane dotyczą o uprawnieniu do wniesienia sprzeciwu[5].

Ponadto jeżeli administrator gromadzi dane osobowe bezpośrednio od osoby, której dane dotyczą należy taką osobę poinformować, czy ma ona obowiązek przekazać dane osobowe oraz o konsekwencjach ich niepodania. Z kolei jeżeli dane pozyskane są z innego źródła niż podmiot danych, administrator jest zobowiązany przekazać informacje o kategorii otrzymanych danych (np. dane kontaktowe, dane identyfikacyjne) oraz o źródle pochodzenia danych (np. pracodawca tej osoby, osoba polecająca ją do pracy, podmiot z grupy kapitałowej, na którego rzecz podmiot danych wyraził zgodę).

Motyw 61 wskazuje na moment, w którym obowiązek informacyjny powinien zostać spełniony zarówno w przypadku gdy dane są zbierane bezpośrednio (art. 13 RODO), jak i pośrednio (art. 14 RODO). Informacje o przetwarzaniu danych osobowych osoby, której dane dotyczą, należy przekazać tej osobie w momencie zbierania danych, a jeżeli danych nie uzyskuje się od osoby, której dane dotyczą, lecz z innego źródła w rozsądnym terminie, najpóźniej w ciągu miesiąca. Jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą, klauzula powinna być przekazana najpóźniej przy pierwszej takiej

[5] P. Fajgielski, *Komentarz do art. 14 ogólnego rozporządzenia o ochronie danych*, [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, s. 147.

komunikacji z osobą, której dane dotyczą, a jeżeli planuje się ujawnić dane osobowe innemu odbiorcy, obowiązek informacyjny powinien być zrealizowany najpóźniej przy ich pierwszym ujawnieniu.

Wyrazem realizacji postulatu prawa do prywatności jest w kontekście analizy art. 12, 13 oraz 14 RODO nie tylko budowanie świadomości podmiotów danych o przysługujących ich uprawnieniach, ale także zapewnienie aby żądania podmiotów danych były respektowane zgodnie z trybem określonym w art. 12 RODO. Artykuł ten stanowi o przejrzystym informowaniu i komunikacji z osobami, których dane dotyczą. Przepis ten odnosi się zatem do generalnej zasady polegającej na tym, że obowiązek informacyjny powinien być napisany przejrzystym i prostym językiem, a także wskazuje na tryb, w jakim administrator danych powinien odpowiadać na żądania osób, których dane dotyczą. Zasadą jest odpowiadanie na żądania w przeciągu miesiąca. Termin ten można jednak przedłużyć do łącznie trzech miesięcy[6]. W przypadku gdy administrator nie odpowie na żądanie, lub odmówi jego realizacji, podmiot danych może złożyć na administratora skargę do organu nadzorczego lub wprost zwrócić się z wnioskiem o nakazanie spełnienia żądania[7].

Gwarantem stosowania RODO jest nie tylko dobra wola administratorów danych osobowych, czy podmiotów przetwarzających dane w ich imieniu, ale jest nim przede wszystkim zagrożenie nałożeniem dotkliwych kar administracyjnych przez krajowe organy nadzorcze. Zgodnie z art. 83 RODO „każdy organ nadzorczy zapewnia, by stosowane (…) kary pieniężne (…) były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające". Za naruszenie przepisów dotyczących realizacji obowiązku informacyjnego oraz praw podmiotów danych, przysługuje zgodnie z art. 83 ust. 5 kara, która może wynieść do 20 000 000 EUR, a w przypadku przedsiębiorstwa w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego[8]. Są to bowiem obowiązki, które nie stanowią novum, gdyż funkcjonowały w poprzednim stanie prawnym, stąd zagrożenie karą jest wyższe. Z kolei za naruszenie obowiązków administratora i podmiotu przetwarzającego, które wprowadza RODO, a o których mowa np. w art. 8, 11, 25 –39 oraz 42 i 43, czy obowiązków podmiotu certyfikującego, organ może nałożyć karę, która może wynieść do 10

[6] P. Litwiński, *Komentarz do art. 12*, [w:] *red.* P. Litwiński, M. Kawecki, P. Barta, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*,, pkt 7.
[7] P. Fajgielski, *Komentarz do art. 12 ogólnego rozporządzenia o ochronie danych*, [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, s. 99.
[8] J. Łuczak, *Artykuł 83 Ogólne warunki nakładania administracyjnych kar pieniężnych* [w:] red. D. Lubasz, E. Bielak-Jomaa, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, s.1054-1065.

000 000 EUR, a w przypadku przedsiębiorstwa odpowiednio, w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Mając na uwadze funkcję, jaką ma spełniać kara tj. przede wszystkim funkcję odstraszającą, organ przy nakładaniu kary bierze się pod uwagę to, aby kara była proporcjonalna do stwierdzonych naruszeń i skuteczna.

Zgodnie z art. 83 ust. 2 RODO organ przy miarkowaniu kary analizuje charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody. Ocenia się także kategorie danych osobowych, których dotyczyło naruszenie tj. czy naruszenie dotyczyło danych szczególnie chronionych, o których mowa w art. 9 RODO, czy tzw. danych zwykłych. Ponadto organ ocenia charakter naruszenia tj. czy naruszenie było umyślne czy nieumyślne oraz wszelkie stosowane wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego. Organ może wziąć pod uwagę także działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez podmiot danych. Ocenia także stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32 RODO (tj. ochrona danych w fazie projektowania oraz domyślna ochrona danych z art. 25 oraz bezpieczeństwo przetwarzania określone w art. 32 RODO). Istotnym jest także, że organ nadzorczy bierze pod uwagę stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków. Poza stopniem współpracy ważne również jest, w jaki sposób organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie. Ocenia się także czy wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 RODO (tj. uprawnienia naprawcze organów nadzorczych takie jak: wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania, udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów RODO przez operacje przetwarzania, nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, czy nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych lub wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania).

Katalog czynników jakie organ nadzorczy może wziąć pod uwagę przy nakładaniu kary jest otwarty. Jako ostanie ustawodawca unijny wskazał na „wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty".

Z powyższego wynika, że postulat realizacji praw osób, których dane dotyczą został zagwarantowany przez unijnego prawodawcę przede wszystkim poprzez określenie sposobu, w jaki administrator powinien o prawach przysługujących podmiotom danych poinformować (realizacja obowiązku informacyjnego), a po drugie poprzez zapewnienie odpowiednich sankcji za nieprzestrzeganie przepisów.

Przykładem obrazującym podejście krajowego organu nadzorczego do tego postulatu jest wydana przez Prezesa Urzędu Ochrony Danych Osobowych decyzja nakładająca pierwszą pieniężną karę administracyjną[9] opartą o przepisy RODO, właśnie za niedopełnienie obowiązku informacyjnego. W decyzji ZSPR.421.3.2018 organ stwierdził m.in., że naruszenie ma poważny charakter, gdyż dotyczyło podstawowych praw i wolności osób, których dane Spółka przetwarzała (przetwarza). Działanie Spółki naruszało również podstawową w odniesieniu do przetwarzania danych osobowych zasadę rzetelności i przejrzystości (art. 5 ust. 1 lit a RODO). Naruszenie przez Spółkę obowiązku podania podstawowych informacji o przetwarzaniu oraz pouczenia o przysługujących podmiotom danych prawach z tym związanych (wskazanych w art. 15-21 RODO), organ uznał za pociągające za sobą m.in. ryzyko odebrania możliwości podmiotom danych skorzystania z tych praw[10].

PRAWO DO SPRZECIWU WOBEC PRZETWARZANYCH DANYCH

Prawo do sprzeciwu wobec przetwarzania danych zostało określone w art. 21 RODO. Z przepisu wynikają określone przesłanki uprawniające osobę, której dane dotyczą do skorzystania z tego prawa oraz konsekwencje jego wniesienia. Przepis ten wskazuje także na obowiązki administratora danych w zakresie prawidłowego przekazania informacji osobom, których dane dotyczą co do sposobu skorzystania z tego uprawnienia.

[9] Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożyła pierwszą karę w wysokości ponad 943 tys. zł., źródło: https://uodo.gov.pl/pl/138/786, dostęp na 15.07.2019r.
[10] Decyzja Prezesa Urzędu Ochrony Danych Osobowych ZSPR.421.3.2018, źródło: https://uodo.gov.pl/pl/324/787, dostęp na 15.07.2019r.

Sprzeciwić się wobec przetwarzanych danych można było już na gruncie poprzedniego reżimu prawnego, jednak w RODO wprowadzono znaczne zmiany, w szczególności w zakresie reguł korzystania z uprawnienia wskazanego w art. 21. Przede wszystkim prawo do sprzeciwu znajduje zastosowanie w zależności od tego, na jakiej podstawie przetwarzane są dane osobowe. Z uprawnienia tego można skorzystać więc, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi oraz, gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią. Zatem z prawa do sprzeciwu nie można skorzystać, gdy dane są przetwarzane na podstawie zgody, umowy, czy w związku z obowiązkiem prawnym, a także gdy dane są niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą [11].

Z powyższej analizy wynika, że prawo do sprzeciwu powstało w związku z potrzebą zapewnienia równorzędnej ochrony osób, których dane przetwarzane są w oparciu o podstawę prawną, która nie wymaga z ich strony aktywnego działania takiego jak np. wyrażenie oświadczenia woli – wyrażenie zgody w postaci odznaczenia check box'a.

W obrębie tego uprawnienia istnieją pewne różnice co do dodatkowych wymogów, które musi wykazać podmiot danych. Rozróżnienie wynika z okoliczności, w jakich dane te są przetwarzane, co wiąże się w pewnych przypadkach z koniecznością wykazania dodatkowo przez podmiot danych, że sprzeciw jest umotywowany szczególną sytuacją tej osoby. Z taką sytuacją będziemy mieli do czynienia, gdy dane są przetwarzane na podstawie wspomnianej już podstawy prawnej, określonej w art. 6 ust. 1 lit. e i f tj. gdy przetwarzanie danych osobowych odbywa się w związku z realizacją zadań publicznych, sprawowaniem władzy publicznej oraz na podstawie prawnie uzasadnionego interesu administratora. W obszarze nowych technologii najczęściej będziemy mieli do czynienia z prawnie uzasadnionym interesem, a przykładem procesów przetwarzania, które mogą być oparte na tej postawie prawnej to: wysyłka newslettera, działania podejmowane w ramach marketingu własnego administratora, czy prowadzenie kontaktu z konsumentem w związku z wykonywaniem usługi w ramach obowiązującej strony umowy. Poza środowiskiem internetowym procesami opartymi na tej przesłance może być monitoring CCTV, prowadzenie oceny rocznej pracowników

[11] P. Fajgielski, *Komentarz do art. 21 ogólnego rozporządzenia o ochronie danych*, [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, s. 144.

i współpracowników, wykorzystanie wizerunku pracownika w związku z wyrażoną przez niego zgodą na rozpowszechnienie wizerunku.

Administratorowi w wyniku zgłoszenia umotywowanego sprzeciwu nie wolno przetwarzać tych danych osobowych, chyba że wykaże on istnienie prawnie uzasadnionych podstaw do dalszego przetwarzania. Podstawy te powinny mieć charakter nadrzędny wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Należy przy tym podkreślić, że zgodnie z motywem 69 za wykazanie, że ważne prawnie uzasadnione interesy administratora mają nadrzędny charakter wobec interesów lub podstawowych praw i wolności osoby, której dane dotyczą, powinien odpowiadać administrator.

Niemniej, jak podkreśla P. Fajgielski, już w poprzednim reżimie funkcjonował pogląd, zgodnie z którym w sytuacji, gdy przetwarzanie danych oparte jest na więcej niż jednej przesłance dopuszczalności (np. te same dane wykorzystywane są do realizacji umowy, a dodatkowo w celach marketingowych), wniesienie sprzeciwu może nie skutkować usunięciem danych (ponieważ prowadziłoby to do braku możliwości wykonania umowy), ale tylko zaprzestaniem wykorzystywania ich do celów marketingowych[12]. Zatem osoba, której dane dotyczą po wniesieniu sprzeciwu wobec otrzymywania materiałów marketingowych, materiałów tych otrzymywać już nie powinna, natomiast jeśli strony wiąże przykładowo umowa o świadczenie usług, dane osobowe mogą być w dalszym ciągu przetwarzane przez administratora i wykorzystywane wyłącznie w tym zakresie.

W pewnych okolicznościach poza zgłoszeniem sprzeciwu podmiot danych musi wykazać się szczególną sytuacją. Warto więc w tym miejscu przybliżyć, czym może być ta szczególna sytuacja podmiotu danych. Wskazuje się, że szczególna sytuacja może być związana z ujawnieniem przez przetwarzanie danych związanych ze sferą prywatną, czy rodzinną[13]. Ponadto za sytuację szczególną należy uznać stan faktyczny, który nie miał miejsca w chwili zbierania danych osobowych (jeżeli mamy do czynienia z bezpośrednim zbieraniem danych), lub który istniał w chwili zbierania danych, lecz nie był wiadomy administratorowi danych (pośrednie zbieranie danych). Przy ocenie szczególnej sytuacji osoby, której dane dotyczą, należy wziąć pod uwagę, że sytuacja ta powinna wpływać na przetwarzanie danych

[12] P. Fajgielski, *Komentarz do art. 14 ogólnego rozporządzenia o ochronie danych*, [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, s. 146.
[13] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, s. 531.

osobowych w ten sposób, że dochodzi do zachwiania równowagi interesów tej osoby oraz administratora danych[14].

Na szczególną sytuację nie muszą powoływać się osoby, które zgłaszają sprzeciw wobec przetwarzania danych w celach marketingowych, a dokładnie w związku z marketingiem bezpośrednim. Zgodnie z art. 21 ust. 2 RODO „jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim". Z wniesieniem sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego nie wiąże się, tak jak było to wskazane powyżej, możliwość wykazania przez administratora, że dane te są mu potrzebne np. do ochrony przy roszczeniach.

Prawo do sprzeciwu znajduje szczególne zastosowanie w związku z korzystaniem z usług społeczeństwa informacyjnego. Usługi te nie zostały w RODO zdefiniowane, gdyż przepis rozporządzenia odsyła w tym zakresie do Dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego[15]. Usługa społeczeństwa informacyjnego oznacza zatem każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług[16]. Zgodnie z art. 21 ust. 5, RODO wymaga stworzenia możliwości skorzystania z prawa do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne. Wymóg ten, zgodnie ze stanowiskiem doktryny można interpretować jako konieczność zapewnienia przez administratora przetwarzającego dane w serwisie internetowym możliwości skorzystania z uprawnienia do sprzeciwu jako funkcjonalności dostępnej w tym serwisie[17].

[14] P. Litwiński, *Komentarz do art. 21*, [w:] *red.* P. Litwiński, M. Kawecki, P. Barta, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*.pkt 4.

[15] Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z 9.09.2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego, Dz. Urz. UE L 241, s. 1.

[16] P. Makowski, D. Lubasz, *Artykuł 4 pkt 25 Usługa społeczeństwa informacyjnego*, [w:] red. D. Lubasz, E. Bielak-Jomaa, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*., s. 311.

[17] P. Fajgielski, *Komentarz do art. 14 ogólnego rozporządzenia o ochronie danych*, [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, s. 147.

Celem podsumowania warto podkreślić różnice między sprzeciwem a wycofaniem zgody. O ile skutki wniesienia obu żądań co do zasady będą bardzo do siebie zbliżone, o tyle w przypadku sprzeciwu administrator danych może w szczególnych przypadkach nadal przetwarzać dane osobowe. Jest to możliwe w przypadku, gdy sprzeciw nie dotyczy działań marketingowych oraz gdy administrator jest w stanie wykazać, że jego ważne prawnie uzasadnione interesy mają nadrzędny charakter wobec interesów lub podstawowych praw i wolności osoby, której dane dotyczą. Natomiast w sytuacji, gdy zgoda jest dla administratora jedyną podstawą uprawniającą go do przetwarzania danych, to jej wycofanie oznacza, że administrator nie ma już możliwości przetwarzania danych w tym celu[18].

PODSUMOWANIE

Prawo do prywatności jest prawem, które w obszarze ochrony danych osobowych jest szczególnie związane z prawem do zachowania pewnych, osobistych informacji o sobie wyłącznie dla siebie, oraz do nieingerowania w sferę prywatną danej osoby poprzez zachowanie kontroli nad tym jakie informacje, w tym informacje marketingowe będą ten prywatny czas zajmować. Ponadto w związku z tym, że aktywność człowieka przeniosła się do świata cyfrowego znacznie wzrosło ryzyko braku kontroli nad tym co dzieje się z danymi osobowymi przetwarzanymi przez administratorów danych osobowych, czy podmioty przetwarzające. Aby zminimalizować to ryzyko RODO wprowadziło szereg narzędzi umożliwiających osobom fizycznym sprawowanie nadzoru nad przetwarzanymi danymi. Skorelowanie uprawnień z wysokimi sankcjami, których zasady ich nałożenia przypominają te z prawa konkurencji i ochrony konsumentów, stanowi rodzaj gwarancji dla realizacji praw osób, których dane dotyczą. Dodatkowo poprzez wzmocnienie katalogu informacji, które administrator jest zobowiązany przekazać na mocy art. 13 i 14 RODO, rośnie świadomość podmiotów danych w zakresie przysługujących im uprawnień, podstaw prawnych przetwarzania danych, czy celów w jakim dane są przetwarzane. Warto w miejscu wskazać, że w związku z tym, że po 25 maja 2018r. klauzule obowiązku informacyjnego zawierają więcej informacji na temat przetwarzania danych, oraz dzięki kampanii informacyjnej, która towarzyszyła rozpoczęciu stosowania RODO, liczba skarg, która wpłynęła do Urzędu Ochrony

[18]P. Litwiński, *Komentarz do art. 21,* [w:] *red.* P. Litwiński, M. Kawecki, P. Barta*, Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz.,* pkt 11.

Danych Osobowych od tej daty wynosi ok. 2 400. W porównaniu z poprzednim, 2017 rokiem, w którym liczna skarg wyniosła blisko 3 000, można wywnioskować znaczny ich wzrost, a co za idzie większa świadomość podmiotów danych[19].

Prawo do sprzeciwu wobec przetwarzanych danych wydaje się uprawnieniem, która wypełnia pewnego rodzaju lukę w sytuacji, gdy dane podmiotu danych są przetwarzane na podstawie, która nie wymaga aktywnej działalności ze strony osoby fizycznej. W związku z powyższym prawo to umożliwia w skuteczny i szybki sposób przejąć przez osobę, której dane dotyczą kontrolę nad przetwarzanymi danymi. Szczególnie praktyczne rozwiązanie znajdzie w przypadku, gdy dane administrator wykorzystuje w celach marketingu bezpośredniego.

Niemniej w związku z tym, że RODO zawiera liczne klauzule generalne, istnieje zagrożenie interpretacji przepisów na korzyść administratorów i podmiotów przetwarzających. Celem ograniczenia powyższego mogą być wytyczne i wszelkiego rodzaju wskazówki, wydawane przez organy nadzorcze, czy Europejską Radę Ochrony Danych, na podstawie art. 57 ust. 1.

***

OBJECTION TO PROCESSING PERSONAL DATA AS AN EXPRESSION OF THE RIGHT TO PRIVACY

Steady technological development stems from ever larger body of data being processed; as a result profiles of service users – data subject may be created. In times when we more or less consciously decide to share our private sphere, the right to privacy must be specially protected. This right is inextricably linked with the need to exercise effective control over the transferred data, and hence awareness must be built on the purposes and method of personal data's possible processing by the controllers.

The publication argues that the right to object to data processing expresses the right to privacy viewed as the right to control the processes of personal data processing and to exercise real control over how data controllers may use personal data. However, neither the rights, including

[19]E. Bielak- Jomaa, *Prezes UODO: Mamy ogromną liczbę skarg,* źródło: https://www.cyberdefence24.pl/nato/anuluj-zapisz-zmiany-prezes-uodo-mamy-ogromna-liczbe-skarg, dostęp 15.07.2019r.

the right to object, nor other institutions protecting privacy under GDPR will be properly exercised and applied unless they strictly link the protection mechanisms - this is a novelty implemented by GDPR to make the regulatory rights and obligations more effective.

The publication will also consider the administrative sanctions that the supervisory authority may impose on personal data controllers or processors for non-compliance with the rules on data subjects' rights.

BIBLIOGRAFIA

Barta, J., Fajgielski, P., Markiewicz, R. *Ochrona danych osobowych. Komentarz*, Warszawa 2015.

CyberDefence24, *Prezes UODO: Mamy ogromną liczbę skarg,* źródło: https://www.cyberdefence24.pl/nato/anuluj-zapisz-zmiany-prezes-uodo-mamy-ogromna-liczbe-skarg, dostęp 15.07.2019.

Decyzja Prezesa Urzędu Ochrony Danych Osobowych ZSPR.421.3.2018, źródło: https://uodo.gov.pl/pl/324/787, dostęp na 15.07.2019r.

Fajgielski, P. *Komentarz do art. 12 ogólnego rozporządzenia o ochronie danych*, [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018.

Fajgielski, P. *Komentarz do art. 14 ogólnego rozporządzenia o ochronie danych*, [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018.

Fajgielski, P. *Komentarz do art. 21 ogólnego rozporządzenia o ochronie danych*, [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018.

Grzelak, A., *Główne cele ogólnego rozporządzenia o ochronie danych*, [w:] red. M. Kawecki T. Osiej, *Ogólne rozporządzenie o ochronie danych - Wybrane zagadnienia*, Warszawa 2017.

Komunikat Komisji, *Komisja proponuje wprowadzenie wysokiego poziomu ochrony prywatności i danych osobowych w łączności elektronicznej i aktualizuje przepisy ochrony danych w instytucjach UE,* Bruksela 2017.

Litwiński P., *Komentarz do art. 12*, [w:] *red.* P. Litwiński, M. Kawecki, P. Barta,, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2017.

Litwiński P., *Komentarz do art. 21*, [w:] *red.* P. Litwiński, M. Kawecki, P. Barta, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz.,* Warszawa 2017.

Łuczak, J. *Artykuł 83 Ogólne warunki nakładania administracyjnych kar pieniężnych* [w:] red. Lubasz D., Bielak-Jomaa, E., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2017.

Makowski, P., Lubasz D., *Artykuł 4 pkt 25 Usługa społeczeństwa informacyjnego*, [w:] red. Lubasz D., Bielak-Jomaa E, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2017.

UODO, *Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożyła pierwszą karę w wysokości ponad 943 tys. zł.*, źródło**:** https://uodo.gov.pl/pl/138/786, dostęp na 15.07.2019r.