

Elżbieta Gudowska-Natanek¹

Uniwersytet Jagielloński

ORCID ID: 0000-0001-8590-548X

PRAWO DO SPRZECIWU – SZCZEGÓLNE UPRAWNIENIE DECYZYJNE PODMIOTU DANYCH OSOBOWYCH

ABSTRACT

The right to object – a special decision-making right of the personal data subject

The article deals with the issue of a special decision-making right of the subject of personal data, which is the right to object to the processing of personal data by the data subject. The purpose of the study is not only to show the essence of this right, including the analysis of the conditions entitling the data subject to use the objection, administrator's conduct, effects of making an effective request, as well as legal measures applicable in the event of rejection of the objection, but also to draw attention to the existing normative inaccuracies reflected in Regulation 2016/679. After reading the study, the readers will notice that the protection of the rights of the subject of personal data, without the help of a professional attorney, may not bring the expected results. The second emphasized aim of the study is of fundamental importance because ambiguous, hard-to-interpret, confusing, and highly formalized law is never helpful to the individual. Perhaps pointing out problems of a legal nature, which constitute specific postulates *de lege ferenda*, will cause a rational lawmaker to decide to introduce appropriate changes to the regulations.

¹ Radca prawny, członek OIRP w Krakowie, doktor nauk prawnych, wykładowca na Uniwersytecie Jagiellońskim, specjalistka w zakresie prawa konstytucyjnego. Adres do kontaktu: elzbieta.gudowska-natanek@uj.edu.pl.

Keywords: right to object, rights of data subjects, personal data protection, processing of personal data, regulation 2016/679, GDPR

Słowa kluczowe: prawo do sprzeciwu; prawa osób, których dane dotyczą; ochrona danych osobowych, przetwarzanie danych osobowych, rozporządzenie 2016/679, RODO

1. Wprowadzenie

Ochrona osoby, której dane dotyczą, jest nadrzędnym celem przepisów zawartych w rozporządzeniu 2016/679² sprowadzającym się nie tylko do zabezpieczenia przed ujemnymi skutkami niezgodnego z prawem przetwarzania danych, ale *in genere* przed naruszającym prawo przetwarzaniem danych osobowych³. Zmaterializowanie tej ochrony następuje między innymi w ramach realizacji przysługującego osobie prawa podmiotowego zorganizowanego w szeregu uprawnień zazwyczaj określanych jako uprawnienia informacyjne, korekcyjne, decyzyjne oraz uprawnienia do korzystania ze środków ochrony prawnej i uzyskania odszkodowania. Wśród nich ważne miejsce zajmuje prawo do sprzeciwu wobec przetwarzania danych osobowych będące szczególnym uprawnieniem decyzyjnym podmiotu danych osobowych, ujętym odpowiednio w art. 21 rozporządzenia 2016/679⁴.

Prawo do sprzeciwu polega na zakwestionowaniu przetwarzania danych przez osobę, której dane dotyczą, z tą jednak uwagą, że następstwa owej kontestacji mogą być różne, zależą bowiem od ziszczenia się pewnych warunków wynikających ze szczegółowych przepisów rozporządzenia 2016/679⁵. O przysługującym uprawnieniu podmiot danych osobowych powinien się dowiedzieć od administratora danych, ponieważ to na nim spoczywa obowiązek informacyjny, który musi zostać zrealizowany najpóźniej przy pierwszej komunikacji z osobą i przedstawiony w sposób jasny i odrębny od innych informacji, co ma dodatkowo wyeksponować możliwość podjęcia określonej decyzji przez uprawnionego⁶. W istocie administrator ma obowiązek już w trakcie pozyskiwania

2 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 (Dz.Urz. UE L 119), dalej: rozporządzenie 2016/679.

3 E. Gudowska-Natanek, *Niezależny organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych*, [w:] *Z prawem ustrojowym porównawczym przez ponad półwiecze. Księga Jubileuszowa dedykowana Profesorowi Marianowi Grzybowskiemu z okazji 55-lecia pracy naukowej*, red. B. Przywora, A. Rogacka-Łukasik, K. Skotnicki, Częstochowa 2022, s. 791–793.

4 E. Gudowska-Natanek, G. Kuca, *Prawo ochrony danych osobowych i prawo do informacji publicznej. Zarys wykładu*, Warszawa 2024, s. 88–89.

5 B. Fischer, M. Sakowska-Baryła, *Charakterystyka praw osób, których dane dotyczą na gruncie RODO*, [w:] *Realizacja praw osób, których dane dotyczą na podstawie RODO*, red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017, s. 24.

6 „Administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to

danych osobowych poinformować osobę, której dane dotyczą, że ma prawo do sprzeciwu, co wynika wprost z art. 13 ust. 2 lit. b oraz art. 14 ust. 2 lit. c rozporządzenia 2016/679. Zgodnie z art. 15 ust. 1 lit. e rozporządzenia 2016/679 osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz wniesienia sprzeciwu. Prawo dostępu do danych może być etapem poprzedzającym wniesienie sprzeciwu.

Prawo do wniesienia sprzeciwu nie przysługuje w każdym przypadku przetwarzania danych osobowych. W zakresie art. 21 ust. 1 i 6 rozporządzenia 2016/679 nie można się na nie powołać, jeśli osoba wyraziła zgodę na przetwarzanie danych (art. 6 ust. 1 lit. a rozporządzenia 2016/679), lecz również gdy podstawę przetwarzania stanowi: konieczność realizacji umowy (art. 6 ust. 1 lit. b rozporządzenia 679/2016), niezbędność wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c rozporządzenia 2016/679) lub niezbędność ochrony żywotnych interesów osoby, której dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d rozporządzenia 2016/679). W przypadku, gdy dane są przetwarzane na potrzeby marketingu bezpośredniego, podstawą do przetwarzania danych osobowych może być art. 6 ust. 1 lit. a, art. 6 ust. 1 lit. b, art. 6 ust. 1 lit. f rozporządzenia 2016/679, a złożenie skutecznego sprzeciwu wiąże się z bezwzględnym zakazem dalszego przetwarzania danych w celach marketingowych⁷.

Skutkiem wykonania sprzeciwu może być nie tylko zaprzestanie przetwarzania danych, ale także zaprzestanie profilowania czy usunięcie przetwarzanych danych, a samo wniesienie sprzeciwu może spowodować czasowe ograniczenie przetwarzania. Administrator danych nie powinien przetwarzać danych w celach objętych sprzeciwem, chyba że wykáže istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, albo podstaw do ustalenia, dochodzenia lub obrony roszczeń (art. 21 ust. 1 rozporządzenia 2016/679). Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 rozporządzenia 2016/679, administrator może dalej przetwarzać takie dane, jeśli udowodni, że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym. Również i w tym przypadku będzie musiał ocenić wagę szczególnej sytuacji podmiotu danych.

Warto zwrócić uwagę, że sprzeciw bywa często utożsamiany z cofnięciem zgody na przetwarzanie danych osobowych. Utożsamianie najwyraźniej wynika z podobnych skutków, jakie występują przy wykorzystaniu obu mechanizmów. Wniesienie sprzeciwu może nastąpić jedynie w ściśle określonych przypadkach, do których nie należy przetwarzanie

również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania (art. 4 pkt 7 rozporządzenia 2016/679).

⁷ Zob. decyzję Prezesa Urzędu Ochrony Danych Osobowych (PUODO) z dnia 5 grudnia 2019 r., ZKE.440.49.2019, zgodnie z którą „[...] sprzeciw wniesiony przez Panią M. K. wobec przetwarzania jej danych osobowych na potrzeby marketingu został odnotowany w systemie informatycznym Banku i zarówno Bank, jak i podmiot, któremu Bank powierzył przetwarzanie danych osobowych Skarżącej, tj. Spółka zaprzestali przetwarzania jej danych osobowych w tych celach. Wskazać także należy, że dane osobowe Skarżącej już od [...] października 2015 r. nie są w Spółce przetwarzane”. Por. decyzję PUODO z dnia 29 listopada 2019 r., ZKE.440.14.2019.

danych osobowych na podstawie zgody (poza przesłanką marketingu bezpośredniego). Osoba, która wyraziła zgodę na przetwarzanie danych osobowych, może ją odwołać, co powoduje, że administrator nie jest już uprawniony do dalszego przetwarzania danych. Z kolei w przypadku sprzeciwu dalsze przetwarzanie jest dopuszczalne, jeśli zaistnieją określone warunki⁸. W przypadku, gdy przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. b–d rozporządzenia 2016/679, osoba, której dane dotyczą, nie może skorzystać ze sprzeciwu ujętego w art. 21 ust. 1 rozporządzenia 2016/679 ani podnosić, że nie wyraziła zgody na przetwarzanie danych.

2. Zakres podmiotowo-przedmiotowy prawa do sprzeciwu

Zgodnie z art. 21 rozporządzenia 2016/679 osoba, której dane dotyczą, ma prawo wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych. Prawo do sprzeciwu odnosi się do czterech sytuacji. Osoba, której dane dotyczą, ma prawo:

1. w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania danych osobowych zgodnie z art. 6 ust. 1 lit. e rozporządzenia 2016/679, w tym profilowania na podstawie tych przepisów – to znaczy, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń;
2. w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania danych osobowych zgodnie z art. 6 ust. 1 lit. f rozporządzenia 2016/679, w tym profilowania na podstawie tych przepisów – to znaczy, gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń;

⁸ Zob. decyzję PUODO z dnia 18 stycznia 2019 r., ZSPR.440.998.2018, zgodnie z którą administrator odnotował sprzeciw skarżącego co do przetwarzania jego danych osobowych w celach marketingowych, w tym profilowania, i powiadomił, że dane osobowe skarżącego nie będą przetwarzane w tych celach, a także poinformował skarżącego o nieuwzględnieniu jego sprzeciwu wobec przetwarzania jego danych osobowych na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679 ze względu na to, że przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora. Skarżący nie wykazał istnienia po swojej stronie szczególnej sytuacji, która uzasadnia wniesienie sprzeciwu.

3. w dowolnym momencie wnieść sprzeciw wobec przetwarzania danych osobowych na potrzeby marketingu bezpośredniego, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. Jeżeli osoba, której dane dotyczą, wnieśnie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów;
4. wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania danych osobowych zgodnie z art. 89 ust. 1 rozporządzenia – to znaczy, gdy dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Zdekodowanie istoty wymienionych przesłanek wiąże się z koniecznością scharakteryzowania poszczególnych określeń w nich użytych. Do zupełnie podstawowych pojęć należą „osoba, której dane dotyczą” oraz „przetwarzanie danych osobowych”. „Osoba, której dane dotyczą” to osoba fizyczna, której dane osobowe są przetwarzane. Przepisy nie odnoszą się do osób nieżyjących ani osób prawnych czy jednostek organizacyjnych niebędących osobami prawnymi. Bez znaczenia jest to, czy osoba posiada pełną, czy ograniczoną zdolność do czynności prawnych, czy jest cudzoziemcem, bezpaństwowcem, czy obywatelem RP. Zgodnie z art. 4 pkt 1 rozporządzenia 2016/679 dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Natomiast „przetwarzanie danych osobowych” to dokonywanie operacji lub zestawu operacji na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. Przetwarzaniem danych osobowych jest zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie⁹.

Pierwszą sytuacją, na którą wskazuje unijny prawodawca, uprawniającą do wniesienia sprzeciwu, jest przetwarzanie danych na podstawie art. 6 ust. 1 lit. e rozporządzenia 2016/679, to jest wtedy, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Tego rodzaju przetwarzanie danych musi znaleźć odzwierciedlenie w prawie UE lub w prawie państwa członkowskiego. Chodzi tutaj o przepis prawa, który będzie wskazywał na zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, co z natury rzeczy powiązane jest z realizacją szeroko rozumianych zadań publicznych. W przepisach krajowych odnaleźć można wiele tego typu zadań, których realizacja następuje w związku z przetwarzaniem

⁹ Katalog ten nie jest zamknięty, a zawiera jedynie przykłady najczęściej dokonywanych operacji przetwarzania danych osobowych.

danych osobowych. Unijny prawodawca wskazuje na niezbędność przetwarzania, co oznacza, że musi istnieć prawnie relewantna sytuacja koniecznego przetwarzania danych, by wykonać zadanie lub sprawować władzę, przy czym istotne jest zachowanie pewnej proporcjonalności, która znajduje wyraz w art. 51 Konstytucji RP¹⁰. Niezbędne przetwarzanie to takie, które warunkuje wykonanie zadania lub sprawowanie władzy publicznej. Przy ustalaniu tego warunku z pewnością nie można się jednak wystrzec potencjalnych nadużyć. Dlatego na administratorze danych ciąży obowiązek wykazania tej niezbędności.

Wydawać by się mogło, że zadanie określone w omawianej przesłance może wykonywać wyłącznie podmiot publiczny¹¹. Wyjaśnienie tej problematyki wprowadza motyw 45 preambuły rozporządzenia 2016/679, który podkreśla, że to „prawo Unii lub prawo państwa członkowskiego powinno określać także, czy administratorem wykonującym zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powinien być organ publiczny czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu, na przykład zrzeszenie zawodowe, jeżeli uzasadnia to interes publiczny, w tym cele zdrowotne, takie jak zdrowie publiczne, ochrona socjalna oraz zarządzanie usługami opieki zdrowotnej”. W efekcie na przesłankę mogą się powołać także podmioty prawa prywatnego, jeśli tylko wykonują zadania publiczne¹². W tym przypadku jako tego rodzaju czynności wskazuje się niewładcze formy działania na przykład w zakresie pomocy socjalnej czy walki z terroryzmem, co wyklucza działania władcze takie choćby jak wydawanie decyzji administracyjnych.

Druga sytuacja odnosi się do przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679, gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem¹³. Oparcie przetwarzania danych na tej podstawie będzie możliwe pod warunkiem przewagi prawnie uzasadnionych interesów administratora lub strony trzeciej nad interesami lub podstawowymi prawami i wolnościami podmiotu danych¹⁴. Podobnie jak art. 6 ust. 1 lit. e rozporządzenia 2016/679 podstawa ta dotyczy niezbędności przetwarzania danych do realizacji określonych celów administratora. Zatem i tutaj dojdzie do oceny interesów obu stron. Brak niezbędności przetwarzania do realizacji celów administratora

¹⁰ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. nr 78 poz. 483, z późn. zm.).

¹¹ P. Fajgielski, *Ochrona danych osobowych w administracji publicznej*, Warszawa 2021, s. 129.

¹² Zob. M. Jabłoński, K. Wygoda, *Legalność pozyskiwania i przetwarzania danych osobowych w sferze publicznej. Aspekty praktyczne*, Warszawa 2021, s. 80.

¹³ „Strona trzecia” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe (art. 4 pkt 10 rozporządzenia 2016/679).

¹⁴ Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE, s. 3, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pl.pdf [dostęp: 13 listopada 2023 r.].

nie pozwoli na skorzystanie z omawianej przesłanki. W piśmiennictwie podkreśla się, że administrator już na etapie początkowym, a zatem zanim zacznie przetwarzać dane, powinien ocenić wagę swoich interesów i interesów osoby, której dane miałyby przetwarzać¹⁵. Z kolei z momentem wniesienia sprzeciwu administrator powinien dokonać wagi tych interesów. W przesłance zwrócono szczególną uwagę na pozycję dziecka. Można z tego wywnioskować, że administrator nie powinien opierać przetwarzania danych osobowych dziecka na podstawie art. 6 ust. 1 lit. f rozporządzenia 2016/679.

Prawnie uzasadniony interes administratora lub strony trzeciej nie dotyczy przetwarzania dokonywanego przez organ publiczny w ramach realizacji zadań publicznych (poza kwestiami cywilnoprawnymi). Zasadniczo przyjmuje się, że podmioty publiczne nie powinny korzystać z omawianej przesłanki, bowiem są uprawnione opierać swoje przetwarzanie na przepisie poprzedzającym, tj. art. 6 ust. 1 lit. e rozporządzenia 2016/679¹⁶.

Pojęcie prawnie uzasadnionych interesów jest pojęciem niedookreślonym, przez co pozwala na podjęcie uznaniowej, a często błędnej decyzji, stanowiącej naruszenie praw podmiotu danych osobowych.

Motywy zawarte w preambule rozporządzenia 2016/679 mogą stanowić wskazówki co do spełnienia przez administratora przesłanki prawnie uzasadnionego interesu. Wedle motywu 47 preambuły rozporządzenia 2016/679 prawnie uzasadniony interes zachodzi wtedy, gdy podmiot danych jest klientem administratora, gdy przetwarzanie danych osobowych jest niezbędne do zapobiegania oszustwom czy wtedy, gdy dane osobowe są przetwarzane do celów marketingu bezpośredniego. Z kolei w motywie 48 preambuły wskazano, że „administratorzy, którzy są częścią grupy przedsiębiorstw lub instytucji powiązanych z podmiotem centralnym, mogą mieć prawnie uzasadniony interes w przesyłaniu danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników”. Z motywu 49 preambuły wynika, że „przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji – tj. zapewnienia odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjemne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych – oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest prawnie uzasadnionym interesem administratora, którego sprawa dotyczy. Może to obejmować na przykład zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów,

15 M. Czerniawski, *Art. 21, [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 558.

16 Zob. K. Wygoda, *Modyfikacja przesłanek dopuszczalności przetwarzania danych zwykłych w oparciu o art. 6 RODO a działania podmiotów sektora publicznego, [w:] Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, red. M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, Wrocław 2017, s. 41.

przerywanie ataków typu «odmowa usługi», a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej».

Prawnie uzasadniony interes to taki, który ma oparcie w przepisach prawa. Dotyczy to sytuacji, gdy administrator danych mocą na przykład ustawy otrzymuje uprawnienia, które może wcielić w życie jedynie wtedy, gdy przetwarza dane osobowe. Z drugiej strony, w przypadku podmiotu danych prawodawca unijny zwraca uwagę nie tylko na podstawowe prawa i wolności osoby, której dane dotyczą, ale też jej interesy. Tym samym zaakcentowane w rozporządzeniu 2016/679 interesy dotyczą zarówno administratora, jak i podmiotu danych. Różnica polega jednak na tym, że administrator ma mieć uzasadniony interes w przetwarzaniu danych osobowych, a osoba, której dane dotyczą, każdy interes, niekoniecznie uzasadniony. Oprócz tego interes administratora musi być nie tylko zgodny z prawem, lecz również konkretny, jasno określony i aktualny¹⁷. Arkadiusz Sobczyk stwierdza przy tym, że pojęcie interesu osoby, której dane dotyczą „trzeba rozumieć w oderwaniu od norm prawnych i objąć nim subiektywne przekonanie podmiotu danych o tym, co dla niego korzystne”¹⁸. W tym przypadku, zanim administrator podejmie decyzję o uwzględnieniu sprzeciwu, musi zatem poznać istotę interesu podmiotu danych osobowych.

Administrator danych winien na samym początku określić, co jest jego prawnie uzasadnionym interesem, czy zachodzi przesłanka niezbędności przetwarzania danych do urzeczywistnienia celu, który wynika z tegoż interesu, a dopiero następnie powinien dokonać oceny, czy nie występuje taka sytuacja, która ma charakter nadrzędny wobec interesu administratora, tj. w zakresie interesów, praw oraz wolności podmiotu danych (ważenie dóbr chronionych prawem). Administrator powinien się zastanowić, czy w inny sposób mógłby osiągnąć zamierzony cel, a także jakie negatywne skutki mogłyby się pojawić w przypadku decyzji o nieprzetwarzaniu danych. Jego interes musi być konieczny i proporcjonalny do celu. Nieodzowny test równowagi ma na celu porównanie uzasadnionego interesu administratora danych lub osób trzecich z interesami, prawami lub wolnościami osób, których dane dotyczą. Administrator, w ramach zasady rozliczalności ujętej w art. 5 ust. 2 rozporządzenia 2016/679, ma obowiązek wykazać, że wynik przeprowadzonej oceny wskazywał na jego interes prawny. Słusznie stwierdzają Dominik Lubasz i Witold Chomiczewski, że „dokonując, w ramach wyważania dwóch dóbr prawem chronionych, oceny, które z powyższych wartości mają charakter nadrzędny, należy wziąć pod uwagę wszelkie okoliczności danego stanu faktycznego. Konieczne jest zwrócenie szczególnej uwagi na charakter interesu realizowanego przez administratora lub przez stronę trzecią, interesu podmiotu danych, rodzaj prawa podstawowego lub wolności, rodzaj przetwarzanych danych osobowych, sposób przetwarzania danych, wynikające z niego zagrożenia dla interesów, praw i wolności podmiotu danych, relację między podmiotem danych a administratorem lub stroną trzecią, łatwość, z jaką podmiot danych może doprowadzić do konieczności zaniechania dalszego przetwarzania jego danych, a także indywidualną sytuację konkretnego podmiotu danych, w tym jego wiek”¹⁹.

17 Prawnie uzasadnionym interesem będzie korzyść administratora pod postacią np. zysku ekonomicznego.

18 A. Sobczyk, *RODO. Rozproszona władza publiczna*, Kraków 2019, s. 175.

19 D. Lubasz, W. Chomiczewski, Art. 6, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018, s. 396–397.

Kolejna podstawa prawna uprawniająca do wniesienia sprzeciwu dotyczy sytuacji, gdy dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym²⁰. W ten sposób ujęte cele dotyczą trzech obszarów poznawczych²¹. Cele badań naukowych zgodnie z motywem 159 preambuły rozporządzenia 2016/679 „należy interpretować szeroko, obejmując tym pojęciem na przykład rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych”. Tak sformułowana wskazówka sugeruje, że w ramach dziedziny badań naukowych można zawrzeć wiele, co w pewien sposób stawia pod znakiem zapytania trafność jej brzmienia. Z kolei cele badań historycznych nie zostały w ogóle zdefiniowane, co może sprawiać trudności, czy będą to wszelkie cele związane z badaniem wszystkiego, co dotyczy przeszłości, czy tylko określonej materii. Cele statystyczne zostały opisane w motywie 162 preambuły rozporządzenia 2016/679 i oznaczają „każdą operację zbierania i przetwarzania danych osobowych niezbędnych do badań statystycznych lub do opracowywania wyników statystycznych”. Podkreślono jednocześnie, że wynikiem przetwarzania danych do celów statystycznych są dane zbiorcze, nie dane osobowe. Warto także zwrócić uwagę, że mocą art. 89 ust. 2 każde państwo członkowskie w ramach swoich krajowych regulacji lub prawa UE może wyłączyć wobec takiego przetwarzania niektóre prawa podmiotów, tj. prawo dostępu do danych, prawo do sprostowania danych, prawo do ograniczenia przetwarzania i prawo do sprzeciwu. Możliwość wprowadzenia wyłączeń obwarowana jest prawdopodobieństwem, że korzystanie z uprawnień uniemożliwi lub poważnie utrudni przetwarzanie danych dla tych celów i jeśli wyjątki takie są konieczne do realizacji celów.

W art. 21 ust. 6 rozporządzenia 2016/679 nie użyto sformułowania „administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń”, tak jak to uczyniono w art. 21 ust. 1 rozporządzenia 2016/679 dotyczącym przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. e i f. Osoba, której dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych, może wnieść sprzeciw, chyba że przetwarzanie jej danych osobowych jest niezbędne do wykonania zadania realizowanego w interesie publicznym. Podobnie jak w przypadku art. 6 ust. 1 lit. e rozporządzenia 2016/679 tak tutaj zachodzi konieczność zbadania przez administratora warunku niezbędności przetwarzania do wykonania

²⁰ Zgodnie z art. 89 ust. 1 rozporządzenia 2016/679 przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele. Jeżeli cele te można zrealizować w drodze dalszego przetwarzania danych, które nie pozwalają albo przestały pozwalać na zidentyfikowanie osoby, której dane dotyczą, cele należy realizować w ten sposób.

²¹ Zob. uwagi autora na temat rozróżnienia celów badawczych: P. Fajgielski, *Ochrona danych osobowych w administracji publicznej*, Warszawa 2021, s. 742.

zadania. Niezbędność przetwarzania winna być zestawiona z przesłanką szczególnej sytuacji podmiotu danych.

Jak to już zostało zauważone, w trzech wyżej określonych sytuacjach wskazano, że sprzeciw może być wniesiony przez osobę „w związku z jej szczególną sytuacją” wobec przetwarzania danych osobowych. Użyte przez unijnego prawodawcę pojęcie szczególnej sytuacji nie zostało nigdzie sprecyzowane. Brak wyjaśnienia sprzyja dowolnemu rozumieniu sformułowania, co w efekcie może się także przełożyć na rezygnację podmiotu danych ze skorzystania z przysługującego prawa. Oprócz tego konieczność dokonania interpretacji przez administratora danych, czy w danej sytuacji ziszcza się szczególna sytuacja podmiotu danych, cechuje się niewątpliwym ryzykiem popełnienia błędu.

Jakkolwiek powinno się przyjąć, że szczególna sytuacja zachodzi wtedy, gdy przetwarzanie danych osobowych narusza interes osoby, której dane osobowe się przetwarza, a zatem, gdy przetwarzanie danych osobowych może powodować w stosunku do podmiotu danych negatywne następstwa. Chodzi tutaj o niebezpieczeństwo w zakresie szeroko pojętej prywatności osoby. Według Janusza Barty, Pawła Fajgielskiego i Ryszarda Markiewicza szczególna sytuacja „wiązać się może z groźbą ujawnienia przez takie przetwarzanie danych związanych ze sferą prywatności lub życia rodzinnego, w przypadku gdy wykorzystywanie tych danych w konkretnej sytuacji nie jest bezwzględnie konieczne”²². Trafność sformułowanego w ten sposób poglądu została odnotowana w orzecznictwie sądów administracyjnych²³. Wskazuje się również, że szczególną sytuacją jest taki stan, który nie istniał w momencie zbierania danych bezpośrednio od osoby lub istniał, ale nie był znany administratorowi, gdy zbierał dane w sposób niebezpośredni²⁴. Najistotniejsze jednak wydaje się to, że interes podmiotu danych, w ślad za którym idzie ochrona jego prywatności, powinien mieć większą wartość aniżeli potrzeba przetwarzania danych przez administratora. Z motywu 69 preambuły rozporządzenia 2016/679 wynika, że administrator ma prawo nie uwzględnić sprzeciwu, jeśli wykaże, że jego interesy są ważniejsze od interesów podmiotu danych, co sprowadza się do udowodnienia, który interes przeważa. Przy tym kwestia dowodowa nierozzerwalnie wiąże się z odpowiedzialnością prawną administratora za przestrzeganie ogólnych zasad przetwarzania danych, w tym zgodności z prawem obejmującym przestrzeganie przepisów prawa materialnego i formalnego, rzetelności przetwarzania danych będącej postępowaniem uczciwym i w dobrej wierze, ale też rozliczalności polegającej na ponoszeniu przez administratora ciężaru dowodu. Jeśli administrator nie udowodni, że jego interes ma charakter nadrzędny w stosunku do interesów osoby, której dane dotyczą, będzie zobowiązany zaprzestać dalszego przetwarzania danych. Administrator musi więc ocenić, czy zachodzi przesłanka szczególnej sytuacji podmiotu danych, uzasadniającej uwzględnienie sprzeciwu. Czas oceny może być długotrwały, dlatego w celu zabezpieczenia się przed potencjalnym

22 J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych, Komentarz*, Warszawa 2015, s. 531.

23 Wyrok WSA w Warszawie z dnia 18 sierpnia 2022 r., II SA/Wa 3231/21, LEX nr 3486552. Por. wyrok WSA w Warszawie z dnia 8 października 2021 r., II SA/Wa 2028/20, LEX nr 3414679.

24 P. Litwiński, P. Barta, M. Kawecki, [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018, s. 426.

skorzystaniem przez podmiot danych z przysługujących środków prawnych (pозew, skarga), w sytuacji gdy sprzeciw mógłby być zasadny, administrator powinien na ten czas ograniczyć przetwarzanie danych.

W 2019 r. Prezes Urzędu Ochrony Danych Osobowych wydał decyzję, w której odniósł się do przesłanki szczególnej sytuacji podmiotu danych, nie uwzględniając zasadności sprzeciwu wobec przetwarzania danych²⁵. Sprawa dotyczyła publikacji przez fundację danych, które według pełnomocnika strony mogły spowodować, że „dowolna osoba może w dowolnej chwili uzyskać pełną wiedzę co do daty urodzenia mojego Mocodawcy, przebiegu zatrudnienia, współpracowników biznesowych i przyjaciół. Tak daleko idące informacje tworzą realne zagrożenie dla mojego Mocodawcy – czuje się on przez to niekomfortowo i obawia wykorzystania tych danych w sposób, które pozwolą na wyrządzenie mu realnej szkody. W kontekście wieku mojego Mocodawcy, nie chce on aby każda dowolna osoba, po wpisaniu jego nazwiska do ogólnie dostępnej wyszukiwarki, mogła dowiedzieć się ile ma lat. [...] tworzy to realne utrudnienia związane chociażby z procesami rekrutacyjnymi do potencjalnych nowych pracodawców i miejsc zatrudnienia. Może to także komplikować życie prywatne, osobiste i rodzinne [...]”. PUODO uznał, że przetwarzane dane są danymi powszechnie dostępnymi i w związku z tym nie można przyjąć, że ich przetwarzanie prowadzi do ingerencji w prywatność.

W zakresie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. e–f rozporządzenia 2016/679, ale także w zakresie przetwarzania na potrzeby marketingu bezpośredniego, wskazano, że sprzeciw może być wniesiony „w dowolnym momencie”. W ten sposób sformułowany zakres czasowy oznacza, że na każdym etapie przetwarzania danych, np. podczas zbierania, udostępniania czy modyfikowania danych, podmiot tych danych może skorzystać z przysługującego uprawnienia. Należy stwierdzić, że dowolny moment dotyczy też przetwarzania danych osobowych do celów badań naukowych, historycznych lub do celów statystycznych ujętych w art. 21 ust. 6 rozporządzenia 2016/679, mimo iż z nieznanymi powodów prawodawca unijny nie dookreślił tego uprawnienia, wprowadzając wątpliwości, czy wskazana podstawa prawna daje możliwość wniesienia sprzeciwu w każdej chwili. Dowolny moment oznacza, że sprzeciw można wnieść w każdym czasie przetwarzania dokonywanego na podstawie art. 6 ust. 1 lit. e–f rozporządzenia 2016/679, na potrzeby marketingu bezpośredniego, lecz również do celów badań naukowych, historycznych lub do celów statystycznych.

Ostatnie pojęcie dotyczy „profilowania”²⁶. Na profilowanie zwrócono uwagę przy przetwarzaniu danych na podstawie art. 6 ust. 1 lit. e–f rozporządzenia 2016/679, a także przy przetwarzaniu na potrzeby marketingu bezpośredniego. Pojęcie to umiejscowione w art. 4 pkt 4 rozporządzenia oznacza „dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej,

²⁵ Decyzja PUODO z dnia 30 stycznia 2019 r., ZSPU.440.574.2018.

²⁶ Szerzej M. Ciechomska, *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy” 2017, nr 5, s. 37–42.

zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się”. Profilowanie obejmuje działania wykonywane wyłącznie za pośrednictwem urządzeń zautomatyzowanych i polega na tworzeniu swoistej charakterystyki osoby w ramach przetwarzanych danych²⁷. Taka charakterystyka może posłużyć różnym celom. Popularny przykład stanowi zbieranie informacji dotyczących preferencji w zakresie produktów użytkowników stron internetowych i kierowanie skrojonych na miarę danego użytkownika ofert. Wiedza o preferencjach ma oczywisty wpływ na poziom sprzedaży produktów. Z drugiej strony profilowanie może stanowić istotne zagrożenie poprzez zbyt głęboką ingerencję w obszar prywatności osoby. Zapewne z tego powodu zdecydowano, by podmiot danych mógł w ramach sprzeciwu zażądać zaprzestania profilowania dotyczących go informacji.

Administrator danych nie powinien przetwarzać danych w celach objętych sprzeciwem, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, albo podstaw do ustalenia, dochodzenia lub obrony roszczeń. Na temat interesów, praw i wolności osoby, której dane dotyczą była już mowa. Tutaj warto odnieść się do podstaw do ustalenia, dochodzenia lub obrony roszczeń. Nie ulega wątpliwości, że wydzielenie tej przesłanki do odmowy uwzględnienia sprzeciwu nie było konieczne. Ustalenie, dochodzenie lub obrona roszczeń to ważne prawnie uzasadnione podstawy do przetwarzania danych. Niemniej trzeba uznać, że przesłanka ta dotyczy roszczeń nie tylko w postępowaniu sądowym, a zatem tym mającym charakter cywilny, karny, administracyjny, bez względu na rodzaj i tryb postępowania, ale także w postępowaniu administracyjnym przed organem. Jej wystąpienie niweczy możliwość uwzględnienia sprzeciwu.

Inaczej sprawa wygląda przy przetwarzaniu danych w związku z marketingiem bezpośrednim. Mocą art. 21 ust. 2 rozporządzenia 2016/679 zdecydowano, że 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 marketingiem bezpośrednim. Ustęp kolejny wskazuje nadto, że wniesienie sprzeciwu wobec przetwarzania do celów marketingu bezpośredniego danych osobowych powoduje, że nie wolno już przetwarzać do takich celów. Jest to zakaz bezwzględny i dotyczy tak samego marketingu bezpośredniego, jak profilowania do celów marketingu bezpośredniego. Rozporządzenie 2016/679 nie definiuje pojęcia marketingu bezpośredniego, niemniej przyjmuje się, że marketing bezpośredni to czynności mające na celu promowanie danej usługi lub produktu. Kierowane są one bezpośrednio do osoby w celu poinformowania jej o określonych usługach lub produktach. W ramach marketingu bezpośredniego używane są łączności elektroniczne takie jak e-mail, SMS czy MMS. Z kolei podstawą do przetwarzania danych osobowych dla marketingu bezpośredniego może być art. 6 ust. 1 lit. a, art. 6 ust. 1 lit. b, art. 6 ust. 1 lit. f rozporządzenia 2016/679.

²⁷ W. Chomiczewski, *Profilowanie w ogólnym rozporządzeniu o ochronie danych*, [w:] *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016, s. 130.

Sprzeciw wobec przetwarzania danych na potrzeby marketingu bezpośredniego jest sprzeciwem o charakterze bezwzględny. Administrator musi uwzględnić żądanie osoby, z tą jednak uwagą, że może dalej przetwarzać dane, ale w innych celach, np. związanych z dochodzeniem roszczeń. Prawodawca unijny nie zdecydował, by żądanie to było obwarowane jakimkolwiek warunkiem czy obowiązkiem jego uzasadnienia²⁸. Regulacja w tym zakresie nie wyczerpuje się w art. 21 rozporządzenia, a ma swoje odniesienie w motywie 70 preambuły, który podnosi dwie kwestie. Po pierwsze, prawo do wniesienia sprzeciwu powinno zostać wyraźnie podane do wiadomości osobie, której dane dotyczą, oraz powinno być przedstawione jasno i oddzielnie od wszelkich innych informacji. W ten sposób sformułowane wytyczne mają służyć temu, by komunikat o przysługującym prawie dotarł skutecznie do podmiotu danych. Po drugie, prawo do sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego powinno być bezpłatne i dotyczy przetwarzania zarówno pierwotnego, jak i dalszego, co ma na celu usunięcie bariery mogącej zniechęcić osobę do skorzystania z uprawnienia. O kwestii bezpłatności będzie mowa w dalszych fragmentach opracowania.

3. Forma sprzeciwu

Unijny prawodawca nie określił formy, w jakiej powinien zostać złożony sprzeciw wobec przetwarzania danych osobowych. Jedynie w art. 21 ust. 5 rozporządzenia 2016/679 wskazał, że osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne. Takie skorzystanie wystąpi najpewniej w sytuacji zagwarantowania, przez administratora przetwarzającego dane, odpowiedniej funkcjonalności technicznej. To oznacza, że podmiot danych powinien mieć o tym wiedzę. Niepoinformowanie o funkcjonalności będzie zasadniczo powodowało, że sprzeciw przy użyciu drogi zautomatyzowanej nie wpłynie do administratora. W związku z tym należałoby przyjąć, że brak normatywnej określoności w zakresie formy żądania oznacza, że każdy sposób (forma) wniesienia sprzeciwu jest sposobem dopuszczalnym. Sposób ten rzecz jasna musi się wiązać ze skutecznym zakomunikowaniem administratorowi o skorzystaniu przez osobę z przysługującego jej prawa²⁹. Komunikat może zostać przekazany drogą mailową, telefoniczną, listownie czy

28 Powszechne jest zjawisko polegające na oferowaniu przez podmioty z branży usług telekomunikacyjnych, telewizyjnych czy Internetu określonych rabatów za zgody marketingowe, gdzie wycofanie zgody powoduje utratę rabatu. Zob. więcej J. Styczyński, *Firmy mają dobry patent na zgody marketingowe: Darmowa usługa za zgodę na przetwarzanie danych osobowych*, <https://prawo.gazetaprawna.pl/artykuly/111-3729,firmy-marketingowe-rabaty-za-zgode-na-przetwarzanie-danych-osobowych.html> [dostęp: 13 listopada 2023 r.].

29 Zob. wyrok WSA w Warszawie z dnia 29 sierpnia 2019 r., II SAB/Wa 157/19, LEX nr 2865980, w świetle którego „z akt sprawy nie można wyprowadzić wniosku, że skarżący wniósł do firmy [...] sprzeciw w trybie art. 21 ust. 2 rozporządzenia 2016/679, zgodnie z którym, 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

w bezpośrednim kontakcie z administratorem³⁰. Osoba, która wnosi sprzeciw, nie jest zobowiązana do użycia słowa sprzeciw w treści swojego żądania, ale z treści musi wynikać, jakie jest jej żądanie.

Nie jest również jasne, czy osoba wnosząca sprzeciw musi w jakikolwiek sposób uzasadnić skorzystanie z przysługującego jej prawa ani czy powinna wnieść opłatę. W motywie 70 preambuły do rozporządzenia 2016/679 zawarto niefortunne postanowienie, że sprzeciw wobec przetwarzania danych osobowych na cele marketingowe powinien być bezpłatny. Wykładnia takiego sformułowania może sugerować, że w pozostałych przypadkach osoba ma obowiązek wnieść opłatę, co naturalnie trudno pogodzić z ochroną praw osób, skoro skorzystanie z prawa służącego ochronie wiąże się z warunkiem fiskalnym. Jakkolwiek przesądzający przy tej interpretacji jest przepis art. 12 ust. 5 rozporządzenia 2016/679, który stanowi, że działania podejmowane na mocy art. 21 są wolne od opłat. Jedynie w przypadku ewidentnie nieuzasadnionych lub nadmiernych żądań administrator może pobrać opłatę. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

Jeśli idzie o kwestie braku informacji co do obowiązku uzasadnienia sprzeciwu, to tutaj wyłaniają się dwa problemy. Podmiot danych, który nie ma prawnego obowiązku uzasadnienia swojego sprzeciwu, co do zasady nie zdecyduje się na zawarcie w żądaniu argumentacji wskazującej na to, dlaczego jego sprzeciw jest zasadny. Z kolei w przypadku administratora kwestia uzasadnienia sprzeciwu wydaje się być kluczowa, ponieważ administrator, który nie zna przyczyny żądania strony (poza sprzeciwem w zakresie marketingu bezpośredniego), nie może zrealizować prawa podmiotu danych. To powoduje, że procedura niepotrzebnie się przedłuża o czas powzięcia przez administratora informacji co do sytuacji podmiotu danych osobowych.

4. Postępowanie administratora w związku ze złożonym sprzeciwem

Z przepisów rozporządzenia 2016/679 z powodzeniem można zdekodować procedurę, wedle której powinien postępować administrator danych. Wprawdzie procedura ta nie została zasadniczo wysłowiona wprost, ale część reguł niewątpliwie podlega wyinterpretowaniu chociażby w związku z zasadami przetwarzania danych osobowych.

Wniesienie sprzeciwu wiąże się w pierwszej kolejności z obowiązkiem zweryfikowania przez administratora danych, czy osoba, która złożyła sprzeciw, jest do tego uprawniona.

bepośrednim. Nie wynika to w szczególności z załączonego do wniosku »przykładowego żądania zaprzestania danych osobowych«, w którym nie powołano ww. podstawy prawnej, ani nie sformułowano w sposób jednoznaczny żądania o treści odpowiadającej dyspozycji ww. przepisu”.

30 Zob. decyzja PUODO z dnia 17 września 2021 r., znak DKE.523.33.2021. Podczas rozmowy telefonicznej osoba, której dane były przetwarzane, wniosła skuteczny sprzeciw wobec przetwarzania danych osobowych w celach marketingowych na podstawie 21 ust. 2 rozporządzenia 2016/679. Od tego momentu administrator zaprzestał przetwarzania danych osobowych do celów marketingu, badania satysfakcji oraz preferencji, ale nadal przetwarzał dane w celu realizacji umowy, ustalenia, dochodzenia lub obrony przed ewentualnymi roszczeniami.

Przy tym zagadnieniu istotne są dwie kwestie. Pierwsza dotycząca tego, czy administrator danych jest w stanie na podstawie treści złożonego sprzeciwu ustalić, kto składa sprzeciw i czy przetwarza dane osobowe wnioskodawcy. Druga polegająca na ustaleniu, czy osoba, która złożyła sprzeciw, jest osobą uprawnioną w znaczeniu spełnienia wymogów wynikających z art. 21 rozporządzenia 2016/679.

W przypadku pierwszego problemu, jeżeli administrator, na podstawie informacji dołączonych do sprzeciwu, nie może zidentyfikować wnioskodawcy, powinien zwrócić się do niego i poprosić o dodatkowe dane. Jeśli okaże się, że wnioskodawca wniósł sprzeciw do niewłaściwego podmiotu, administrator powinien poinformować wnoszącego żądanie, że nie może rozpatrzyć sprzeciwu w związku z nieprzetwarzaniem jego danych osobowych. Z kolei w przypadku drugiej kwestii administrator jest zobowiązany odmówić uwzględnienia sprzeciwu, jeśli stwierdzi, że przetwarzanie danych dokonywane jest na podstawie prawnej, od której sprzeciw nie przysługuje.

Jeżeli administrator zidentyfikuje wnioskodawcę i uzna, że przetwarza jego dane, to w przypadku sprzeciwu wobec przetwarzania danych osobowych na potrzeby marketingu bezpośredniego zaprzestaje dalszego przetwarzania danych³¹. Istotne zatem jest tutaj zidentyfikowanie nadawcy komunikatu, nie może to być osoba, której dane nie dotyczą, albo osoba nieuprawniona³².

W pozostałych przypadkach, jeśli administrator zidentyfikuje wnioskodawcę i stwierdzi, że przetwarza jego dane do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej bądź do celów wynikających z prawnie uzasadnionych interesów administratora lub strony trzeciej, bądź do celów badań naukowych lub historycznych lub do celów statystycznych, powinien zaprzestać przetwarzania danych, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Z motywu 59 preambuły rozporządzenia 2016/679 wynika, że „administrator powinien być zobowiązany udzielić odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki – najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania – podać tego przyczyny”. Zgodnie z art. 12 ust. 3 rozporządzenia 2016/679, jeśli administrator nie jest w stanie w ciągu miesiąca udzielić informacji o rozstrzygnięciu, powinien w terminie miesiąca od otrzymania żądania poinformować osobę o przedłużeniu terminu³³. Termin może zostać przedłużony o kolejne dwa miesiące, co może wynikać z obszerności żądania osoby bądź niełatwego charakteru żądania. Informacja o przedłużeniu terminu powinna zawierać uzasadnienie opóźnienia. Z kolei jeżeli administrator

31 Zob. decyzję PUODO z dnia 30 września 2020 r., ZKE.440.32.2019. Po wniesieniu przez podmiot danych sprzeciwu wobec przetwarzania danych osobowych w celach marketingowych administrator danych poinformował pismem o uwzględnieniu sprzeciwu i wskazał, że dane nie będą już wykorzystywane w tym celu.

32 Zob. G. Zanfir-Fortuna, *Article 21 Right to object*, [w:] *The EU General Data Protection Regulation (GDPR). A Commentary*, eds. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oxford 2020, s. 518, „It is enough that the data subject objects for the objection to be successful”.

33 Zob. wyrok WSA w Warszawie z dnia 7 lipca 2022 r., II SA/Wa 3753/21, LEX nr 3509214; wyrok WSA w Warszawie z dnia 13 stycznia 2021 r., II SA/Wa 607/20, LEX nr 3230074.

nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Z art. 18 ust. 1 lit. d rozporządzenia 2016/679 wynika, że osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania, jeśli wniosła sprzeciw na mocy art. 21 ust. 1 rozporządzenia 2016/679. W świetle art. 4 pkt 3 rozporządzenia 2016/679 ograniczenie przetwarzania to „oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania”. Jest możliwe do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą. Przepisy nie przesądzają, by to administrator, bez wniosku osoby, mógł z własnej inicjatywy ograniczyć przetwarzanie danych osobowych, jakkolwiek wydaje się to w pełni uzasadnione. O decyzji o ograniczeniu przetwarzania danych administrator powinien poinformować podmiot danych.

Uwzględnienie przez administratora sprzeciwu powoduje, że nie może on już przetwarzać danych objętych sprzeciwem. Jak zostało zaakcentowane, dalsze przetwarzanie jest możliwe, lecz jedynie wtedy, gdy administrator wskaże inną podstawę prawną przetwarzania³⁴.

Prawo do usunięcia danych w związku z uwzględnieniem sprzeciwu zagwarantowano w art. 17 ust. 1 lit. c rozporządzenia 2016/679. Wynika z niego uprawnienie osoby, której dane dotyczą, do żądania usunięcia tych danych. W takiej sytuacji administrator danych ma obowiązek, zgodnie z żądaniem osoby, usunąć bez zbędnej zwłoki dotychczas przetwarzane dane osobowe.

5. Środki prawne

Kwestie środków ochrony prawnej zostały uwzględnione w rozdziale VIII rozporządzenia 2016/679.

Podmiotowi danych przysługuje uprawnienie do wniesienia skargi do organu nadzorczego, nie tylko w przypadku odmowy uwzględnienia sprzeciwu, ale także wtedy, gdy administrator naruszy przepisy rozporządzenia 2016/697, w tym nie podejmie niezwłocznie lub najpóźniej w ciągu miesiąca działań w związku z żądaniem osoby³⁵. Osoba

³⁴ Zob. wyrok WSA w Warszawie z dnia 11 lutego 2022 r., II SA/Wa 1614/21, LEX nr 3366126, zgodnie z którym „Spółka, wychodząc naprzeciw oczekiwaniom Skarżącej, po doprecyzowaniu wniosku Skarżącej, który ostatecznie odnosił się do sprzeciwu wobec przetwarzania przez Komisję jej danych osobowych dotyczących informacji o stanie zdrowia – okresach niezdolności do pracy – oraz po dokonaniu analizy niezbędności danych osobowych, wymaganych do dalszego prowadzenia postępowania wyjaśniającego przez Komisję w przedmiocie zarzutów dotyczących mobbingu i nierównego traktowania w zatrudnieniu, uwzględniła sprzeciw Skarżącej – przez wydzielenie do osobnej koperty danych objętych sprzeciwem, w tym adresu e-mail Skarżącej, poza dokumentację Komisji z oznaczeniem informacji o zgłoszonym sprzeciwie celem zapobieżenia dalszego ich przetwarzania w pracach Komisji”.

³⁵ Zob. decyzję PUODO z dnia 23 kwietnia 2020 r., ZKE.440.79.2019, zgodnie z którą „Skarżąca zażądała usunięcia uchybień w procesie przetwarzania danych osobowych poprzez wypełnienie wobec niej

może dochodzić swoich praw przed organem nadzorczym, a w dalszej kolejności przed sądem administracyjnym.

Prawo do wniesienia skargi do organu nadzorczego wynika z art. 77 rozporządzenia 2016/679. Nie jest ono ograniczone czasem, co oznacza, że skargę można wnieść w dowolnym momencie³⁶. Regulacje prawne nie wskazują na wymóg wcześniejszego skorzystania z innej ścieżki, np. polegającej na wezwaniu do zaprzestania naruszania prawa przez administratora. Jeśli chodzi o termin załatwienia sprawy, tj. rozstrzygnięcie zasadności złożonej skargi, to tutaj zgodnie z dyspozycją zawartą w art. 62 ustawy o ochronie danych osobowych³⁷ zastosowanie znajdują przepisy Kodeksu postępowania administracyjnego³⁸. Obowiązkiem PUODO jest poza informowaniem o postępach prowadzonego postępowania i oczywiście skutkach złożonej skargi wskazywanie, że przysługują inne środki ochrony prawnej. Postępowanie przed organem nadzorczym jest jednoinstancyjne. Decyzja PUODO podlega zaskarżeniu do sądu administracyjnego: Wojewódzkiego Sądu Administracyjnego w Warszawie. Sądem II instancji jest Naczelny Sąd Administracyjny.

W przypadku naruszenia przepisów, w tym niewypełnienia obowiązków z art. 12 ust. 3 rozporządzenia 2016/679, PUODO może, zgodnie z art. 58 ust. 2 lit. b rozporządzenia 2016/679, udzielić administratorowi lub podmiotowi przetwarzającemu upomnienia, zaś zgodnie z art. 58 ust. 2 lit. c rozporządzenia 2016/679 może nakazać administratorowi uwzględnić sprzeciw³⁹. W rozdziale 7 u.o.d.o. opisano postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych. Jednym z uprawnień PUODO jest możliwość zobowiązania podmiotu, któremu zarzuca się naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych, jeśli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki. Mowa tutaj o uprawdopodobnieniu, nie udowodnieniu naruszenia. Termin obowiązywania ograniczenia przetwarzania danych osobowych nie może być dłuższy niż do dnia wydania decyzji kończącej postępowanie

obowiązków wynikających z art. 32 ust. 1 ustawy z 1997 roku« przez Bank, w szczególności zgłosiła sprzeciw wobec przetwarzania jej danych w celach marketingowych na podstawie art. 32 ust. 1 pkt 8 ustawy z 1997 roku. Zgodnie z art. 32 ust. 3 ustawy z 1997 roku Bank zobowiązany był do uwzględnienia sprzeciwu Skarżącej złożonego w [...].02.2015 roku i zaprzestania przetwarzania jej danych osobowych w celach marketingowych. Sprzeciw został uwzględniony dopiero [...].07.2017 roku. W omawianej sprawie zachowanie Banku w okresie od [...].02.2015 roku do [...].07.2017 roku jawi się jako naruszenie przepisów [...].”

36 Skarga złożona w formie tradycyjnej powinna zawierać: imię i nazwisko oraz adres zamieszkania; wskazanie podmiotu, na który składana jest skarga (nazwę/imię i nazwisko oraz adres siedziby/zamieszkania); dokładny opis naruszenia; żądanie (np. usunięcia danych, wypełnienia obowiązku informacyjnego, sprostowania danych, ograniczenia przetwarzania danych itd.); własnoręczny podpis. Skarga może zostać złożona przez pełnomocnika. Do skargi warto dołączyć dowody wskazujące na naruszenie przepisów przez administratora.

37 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781), dalej: u.o.d.o.

38 Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2023 r. poz. 775 z późn. zm.), dalej: k.p.a.

39 Wyrok WSA w Warszawie z dnia 20 maja 2022 r., II SA/Wa 2742/21, LEX nr 3421789.

w sprawie. Postanowienie nakładające na podmiot, któremu zarzucane jest naruszenie przepisów o ochronie danych, obowiązek ograniczenia przetwarzania jest zaskarżalne do sądu administracyjnego. Mimo zaskarżenia postanowienia jest ono skuteczne do momentu ewentualnego uchylecia przez sąd administracyjny⁴⁰.

Kolejnym, ważnym uprawnieniem jest prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu, które zostało uregulowane w art. 78 rozporządzenia 2016/679. Skarga do sądu administracyjnego może dotyczyć decyzji organu nadzorczego bądź bezczynności organu nadzorczego. Przysługuje po pierwsze zarówno osobie fizycznej, jak i osobie prawnej przeciwko wiążącej decyzji organu nadzorczego, po drugie zaś osobie, której dane dotyczą, jeśli organ nie rozpatrzył skargi lub nie poinformował w określonym terminie o postępach lub efektach rozpatrywania skargi wniesionej na podstawie art. 77 rozporządzenia 2016/679. Wniesienie skargi w żaden sposób nie ogranicza w zakresie skorzystania z innych środków prawnych. Warto zauważyć, że tak unormowany element systemu ochrony danych osobowych w postaci sądowej kontroli decyzji PUODO daje możliwość ochrony nie tylko osoby, której dane dotyczą. Z kolei w przypadku bezczynności organu lub przewlekłości prowadzonego postępowania ze środka ochrony prawnej nie może skorzystać administrator ani podmiot przetwarzający.

Artykuł 79 rozporządzenia 2016/679 przewiduje prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu⁴¹. Osoba, której dane dotyczą, może skorzystać z ochrony prawnej przed sądem, jeśli uzna, że jej prawa przewidziane w rozporządzeniu 2016/679 zostały naruszone w wyniku przetwarzania jej danych osobowych. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia rozporządzenia 2016/679, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę⁴². Uszczegółowienie tych przepisów znajduje się w art. 92 u.o.d.o., gdzie ustawodawca wprost wskazuje, że w zakresie nieuregulowanym rozporządzeniem 2016/679 do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 tego rozporządzenia, stosuje się przepisy Kodeksu cywilnego⁴³. Będą to przepisy dotyczące odpowiedzialności z tytułu czynów niedozwolonych oraz naruszenia dóbr osobistych, a sądem właściwym do rozpatrzenia tych spraw będzie sąd okręgowy.

Do przesłanek odpowiedzialności odszkodowawczej za naruszenie przepisów zaliczyć należy: powstanie bezprawnej szkody; powstanie zdarzenia, za które grozi odpowiedzialność prawna; związek przyczynowy między zdarzeniem a szkodą; wina. Administrator, a także podmiot przetwarzający dane mogą nie ponieść odpowiedzialności, jeśli wykazą, że wynikłe zdarzenie nie powstało z ich winy. Skutkiem naruszenia może być

40 Postanowienie WSA w Warszawie z dnia 16 czerwca 2020 r., II SA/WA 979/20, LEX nr 3028597.

41 W art. 47 Karty praw podstawowych UE (Dz.Urz. UE z 2007 r. C 303) zagwarantowano prawo do skutecznego środka prawnego przysługującego osobie, której prawa i wolności zagwarantowane przez prawo UE zostały naruszone.

42 Wynika to nie tylko z art. 82 ust. 1 rozporządzenia 2016/679, ale także z motywu 146 preambuły rozporządzenia 2016/679.

43 Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2023 r. poz. 1610), dalej: k.c.

szkoda majątkowa w związku z naruszeniem dóbr mających charakter majątkowy, szkoda majątkowa w związku z naruszeniem dóbr o charakterze niemajątkowym, a także szkoda niemajątkowa będąca krzywdą.

Poniesienie odpowiedzialności ograniczone jest terminem. Roszczenie przedawni się zgodnie z terminem przewidzianym w art. 442¹ k.c. Roszczenia o naprawienie szkody wyrządzonej przez bezprawne przetwarzanie danych osobowych przedawniają się z upływem trzech lat od dnia, w którym podmiot dowiedział się o szkodzie, ale nie dłużej niż dziesięć lat od dnia, w którym szkoda nastąpiła. Jeśli chodzi o szkodę na osobie, będzie to nie wcześniej niż trzy lata od dnia, w którym podmiot dowiedział się zarówno o szkodzie, jak i osobie obowiązanej do jej naprawienia. Warto również zwrócić uwagę, że na podstawie art. 24 k.c. osoba może żądać ochrony dóbr osobistych w związku z przetwarzaniem jej danych osobowych poprzez żądanie zaniechania naruszenia, żądanie usunięcia skutków naruszenia, żądanie zapłaty zadośćuczynienia lub przekazania określonej kwoty na cel społeczny, a także naprawienie szkody.

Wiedza podmiotu danych o czasochłonności postępowania cywilnego może zaważyć nad wyborem ścieżki dochodzenia praw na drodze administracyjnej. Nie jest to jedyny powód. Zgodnie bowiem z art. 95 u.o.d.o. sąd ma obowiązek zawiesić postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych została wszczęta przed Prezesem Urzędu⁴⁴, zaś ustalenia prawomocnej decyzji PUODO o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi w trybie art. 145a § 3 ustawy – Prawo o postępowaniu przed sądami administracyjnymi⁴⁵ wiążą sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów. W przypadku żądań, które mogą być dochodzone wyłącznie w postępowaniu przed sądem cywilnym, PUODO może wytaczać powództwo na rzecz osoby, której dane dotyczą, za jej zgodą, ale również wstępować za zgodą powoda do postępowania w każdym jego stadium.

6. Podsumowanie

Określony w abstrakcie cel opracowania zasadniczo polegał na szczegółowym omówieniu istoty prawa do sprzeciwu oraz wskazaniu nieścisłości normodawczych, ich skutków dla realizacji omawianego prawa, oraz w związku z tym postulatów *de lege ferenda* mogących przełożyć się na zmianę prawa.

Z zarysowanej problematyki instytucji sprzeciwu wobec przetwarzania danych osobowych można wysunąć wiele cząstkowych wniosków, które w mojej ocenie sprowadzają się do trzech kwestii: trudnych w interpretacji, a jednocześnie ujętych w dość rozlicznych

⁴⁴ Art. 94 u.o.d.o. obowiązuje sąd i PUODO do wzajemnej wymiany informacji o toczących się postępowaniach i rozstrzygnięciach.

⁴⁵ Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz.U. z 2023 r. poz. 1634 z późn. zm.).

miejscach w rozporządzeniu 2016/679, przepisów prawa; ważnej, a może i decydującej roli administratora danych; a także czasochłonnych i w niektórych przypadkach nader sformalizowanych ścieżkach dochodzenia swoich praw. Wszystko to można też sprowadzić do stwierdzenia, że przeciętny podmiot danych osobowych bez wsparcia profesjonalnego pełnomocnika pozostanie bezradny.

Prawodawca zainteresowany udoskonaleniem obowiązujących przepisów powinien zastanowić się nad szeregiem drobniuzgowo wymienionych w tekście problemów prawnych, których rozwiązanie spowoduje, że skorzystanie z prawa do sprzeciwu wobec przetwarzania danych osobowych przyjmie formę łatwego do wykorzystania instrumentarium prawnego.

Bibliografia

- Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych, Komentarz*, Warszawa 2015.
- Chomiczewski W., *Profilowanie w ogólnym rozporządzeniu o ochronie danych*, [w:] *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016.
- Ciechomska M., *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy” 2017, nr 5.
- Czerniawski M., *Art. 21*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.
- Fajgielski P., *Ochrona danych osobowych w administracji publicznej*, Warszawa 2021.
- Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022.
- Fischer B., Sakowska-Baryła M., *Charakterystyka praw osób, których dane dotyczą na gruncie RODO*, [w:] *Realizacja praw osób, których dane dotyczą na podstawie RODO*, red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017.
- Gudowska-Natanek E., Kuca G., *Prawo ochrony danych osobowych i prawo do informacji publicznej. Zarys wykładu*, Warszawa 2024.
- Gudowska-Natanek E., *Niezależny organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych*, [w:] *Z prawem ustrojowym porównawczym przez ponad półwiecze. Księga Jubileuszowa dedykowana Profesorowi Marianowi Grzybowskiemu z okazji 55-lecia pracy naukowej*, red. B. Przywora, A. Rogacka-Łukasik, K. Skotnicki, Częstochowa 2022.
- Jabłoński M., Wygoda K., *Legalność pozyskiwania i przetwarzania danych osobowych w sferze publicznej*, Warszawa 2021.
- Lubasz D., Chomiczewski W., *Art. 6*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018.
- Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pl.pdf.
- Sobczyk A., *RODO. Rozproszona władza publiczna*, Kraków 2019.
- Styczyński J., *Firmy mają dobry patent na zgody marketingowe: Darmowa usługa za zgodę na przetwarzanie danych osobowych*, <https://prawo.gazetaprawna.pl/artykuly/1113729,firmy-marketingowe-rabaty-za-zgode-na-przetwarzanie-danych-osobowych.html>.
- Wygoda K., *Modyfikacja przesłanek dopuszczalności przetwarzania danych zwykłych w oparciu o art. 6 RODO a działania podmiotów sektora publicznego*, [w:] *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, red. M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, Wrocław 2017.
- Zanfir-Fortuna G., *Article 21 Right to object*, [w:] *The EU General Data Protection Regulation (GDPR). A Commentary*, eds. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oxford 2020.