*Teka Komisji Prawniczej PAN Oddział w Lublinie, t. XII, 2019, nr 2, s. 377–391*
*https://doi.org/10.32084/tekapr.2019.12.2-29*

# NOWE OBOWIĄZKI ADMINISTRATORÓW DANYCH OSOBOWYCH[1]

Dr hab. Marzena Toumi, prof. ASzWoj

Katedra Historii i Teorii Prawa, Instytut Prawa Akademii Sztuki Wojennej
e-mail: marzenatoumi@gmail.com; https://orcid.org/0000-0003-3838-1315

**Streszczenie.** Pojęcie prywatności dotyka niemal wszystkich aspektów życia człowieka, zaś rozwój kultury i technologii nieustannie zmienia perspektywę jej postrzegania. Zmiany zachodzące we współczesnym świecie oraz rozwój technicznych środków zbierania, gromadzenia i wyszukiwania informacji dotyczących innych osób sprawia, że bardzo silnie wzrasta konieczność prawnej ochrony ludzkiego prawa do prywatności – prawa do bycia pozostawionym samemu sobie. W erze demokracji cyfrowej zaistniała konieczność przyjęcia takich rozwiązań systemowych, które uwzględniłyby zarówno nowe zagrożenia, jak i sposoby naruszeń praw i wolności człowieka. Na gruncie europejskim odpowiedzią na takie zapotrzebowanie było wdrożenie RODO (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 ogólne rozporządzenie o ochronie danych), które weszło w życie z dniem 25 maja 2018 r.

**Słowa kluczowe:** dane osobowe, ogólne rozporządzenie o ochronie danych (RODO), przetwarzanie danych osobowych, prawo do prywatności, prawo do bycia zapomnianym

## 1. UWAGI WPROWADZAJĄCE

Pojęcie prywatności[2] dotyka niemal wszystkich aspektów życia człowieka, zaś rozwój kultury i technologii nieustannie zmienia perspektywę jej postrzegania [Chrabonszczewski 2012, 19]. Zmiany zachodzące we współczesnym świecie oraz rozwój technicznych środków zbierania, gromadzenia i wyszukiwania informacji dotyczących innych osób sprawia, że bardzo silnie wzrasta konieczność prawnej ochrony ludzkiego prawa do prywatności – prawa do

[1] Tekst publikacji jest efektem realizacji zadania badawczego „System cyberbezpieczeństwa RP – model rozwiązań prawnych" w ramach programu GRANT BADAWCZY MON (Nr umowy GB/4/2018/2018/DA).

[2] Prawo do prywatności jest pojęciem szerokim i złożonym. W doktrynie używane są różne terminy na określenie, co oznacza „prywatność", „życie prywatne" i „prawo do prywatności", które używane są zamiennie [Zawadzka 2013, 96].

bycia pozostawionym samemu sobie (the right "to be let alone")[3]. Tymczasem już w 1999 r., Scott McNealy, prezes zarządu Sun Microsystems powiedział, że kwestia prywatności konsumentów jest świadomie głoszoną nieprawdą. „Nie macie żadnej prywatności. Pogódźcie się z tym" [Sprenger 1999].

Łącząc się z Internetem stajemy się częścią bazy danych, a tym samym jesteśmy narażeni na wszelkie niebezpieczeństwa związane z siecią. Czasy, gdy można było swobodnie po niej surfować, w przekonaniu o swojej całkowitej i nienaruszalnej anonimowości, dawno minęły. Wszyscy staliśmy się pionkami w grze zwanej marketingiem[4]. Nowa rzeczywistość wymusiła potrzebę wyznaczenia i zagwarantowania sfery życia osobistego, przynależnego każdemu człowiekowi, w którą nikt nieupoważniony nie będzie ingerował[5]. W erze „demokracji cyfrowej" zaistniała konieczność przyjęcia takich rozwiązań systemowych, które uwzględniłyby zarówno nowe zagrożenia, jak i sposoby naruszeń praw i wolności człowieka. Na gruncie europejskim odpowiedzią na takie zapotrzebowanie było wdrożenie RODO (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 ogólne rozporządzenie o ochronie danych)[6], które weszło w życie z dniem 25 maja 2018 r.

RODO wynikało zarówno z konieczności dostosowania przepisów prawa do rozwoju nowoczesnych technologii, jak i z potrzeby wprowadzenia jednolitych zasad ochrony danych osobowych we wszystkich państwach Unii Europejskiej. Zatem nowy system ochrony danych oparty został o przepisy

[3] W bezpośrednim związku z prawem do prywatności pozostaje m.in. ochrona danych osobowych. Sąd Najwyższy w pierwszym wyroku uznającym prywatność za dobro osobiste wskazał, że ochrona prawna obejmuje: ujawnienie faktów z życia osobistego i rodzinnego, nadużywanie uzyskanych informacji, zbieranie w drodze prywatnych wywiadów informacji i ocen ze sfery intymności, aby je opublikować i w inny sposób rozgłaszać. Zatem za naruszenie uznaje się także gromadzenie informacji w celu ich ujawnienia, zob. Wyrok SN z dnia 18 stycznia 1984 r., I CR 400/83.

[4] Zob. *Złudna anonimowość w sieci*, https://docplayer.pl/15133366-Zludna-anonimowosc-w-sieci.html [dostęp: 11.12.2019].

[5] „Poszanowanie" prawa do prywatności oznacza nie tylko zakaz ingerowania przez państwo w prywatność swoich obywateli, ale nakłada także obowiązki na nie, aby stworzyło warunki umożliwiające jego obywatelom korzystanie z tego prawa. „Ochrona sfery życia prywatnego zaliczana jest do praw człowieka pierwszej generacji i jako prawo fundamentalne podlega ochronie w większości współczesnych systemów prawnych" [Pryciak 2010, 211].

[6] Ogólne rozporządzenie o ochronie danych, Dz. Urz. UE, L 119/1, 4.5.2016. Dnia 10 maja 2018 r. Sejm RP VIII kadencji uchwalił nową ustawę o ochronie danych osobowych (Dz. U. poz. 1000), która zastąpiła ustawę z 1997 r. (Dz. U. Nr 133, poz. 883). Ustawa zapewnia stosowanie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, które obowiązuje w polskim porządku prawnym bezpośrednio i ma zastosowanie od dnia 25 maja 2018 r. oraz ustanawia nowy organ właściwy w sprawie ochrony danych osobowych – Prezesa Urzędu Ochrony Danych Osobowych. Ustawa weszła w życie dnia 25 maja 2018 r.

europejskiego rozporządzenia, które we wszystkich krajach Unii Europejskiej jest stosowane bezpośrednio, a nowe prawo, w sposób jednolity reguluje prawa wszystkich osób przebywających na terenie Unii Europejskiej i obowiązki podmiotów, które gromadzą i wykorzystują ich dane osobowe, czyli wszelkie informacje o osobie fizycznej, takie jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczegółów określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (art. 4, pkt 1 RODO). Wśród nich, szczególną kategorię stanowią dane wrażliwe, czyli dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne lub dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej). Wymogom RODO podlegają również dane poddane pseudonimizacji[7], ale już dane zanonimizowane[8] – nie, ponieważ anonimizacja jest nieodwracalna i nie można powrotnie zidentyfikować osób, do których dane należą, a więc *de facto* przestają one być danymi osobowymi.

## 2. NOWE UPRAWNIENIA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE I ODPOWIADAJĄCE IM OBOWIĄZKI ADMINISTRATORÓW

RODO, będąc swoistego rodzaju „konstytucją" dla ochrony prywatności i danych ustanowiło nie tylko zasady ochrony prywatności dla użytkowników, ale również wprowadziło ścisłe wymogi dotyczące prywatności i bezpieczeństwa dla firm i instytucji, które dane użytkowników przetwarzają.

RODO, osobom których dane są przetwarzane, nie tylko przyznało dodatkowe uprawnienia, ale wyposażyło je w zestaw kluczowych informacji dotyczących sposobu i celu przetwarzania ich danych, dając im prawo: dostępu do danych i informacji; żądania sprostowania i uzupełnienia danych; sprzeciwu wobec przetwarzania danych; do przeniesienia danych oraz najsilniejsze z nich – prawo do bycia zapomnianym (*a right to be forgotten*), czyli prawo żądania usunięcia danych przez administratora. Uprawnienia te przekładają się bezpośrednio na obowiązki, którymi obciążeni zostali administratorzy danych osobowych.

---

[7] Pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie bez użycia dodatkowych informacji; pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte technicznymi i organizacyjnymi środkami bezpieczeństwa, które uniemożliwiają ich wykorzystanie w celu zidentyfikowania osoby fizycznej (art. 4, pkt 5 RODO).

[8] Anonimizacja – proces uniemożliwiający zidentyfikowanie osoby fizycznej na podstawie określonych danych, Motyw 26, Preambuła RODO.

Europejski ustawodawca nakazuje, aby ochrona prywatności była brana pod uwagę i stosowana w praktyce przy prowadzeniu wszelkich projektów i działań, tak w sferze publicznej, jak i prywatnej. Oznacza to prawnie wiążący obowiązek uwzględnienia ochrony danych w fazie projektowania (szczególny nacisk położony został na dwa podejścia: analizę ryzyka i konieczność wykonywania ocen skutków dla ochrony danych oraz wdrożenie metodologii *privacy by design* (prywatność na etapie projektowania produktu bądź usługi – PAP), jak i zasadę domyślnej ochrony danych (*privacy by default*)[9].

Uwzględnianie ochrony danych w fazie projektowania zakłada, że ochrona prywatności powinna być wbudowana w każdy nowy projekt, co w praktyce oznacza, że prywatność ma być chroniona nie poprzez dodatki do systemu lub nakładki przygotowane na już istniejące rozwiązania, lecz być wbudowana w jego konstrukcję od początku, jako składowa projektu. Obowiązek ten został nałożony na administratora[10], który według art. 25 ust. 1 RODO, „uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, […] wdraża odpowiednie środki techniczne i organizacyjne […], w celu nadania przetwarzaniu niezbędnych zabezpieczeń oraz ochrony praw osób, których dane dotyczą".

Zatem zasada domyślnej ochrony danych oznacza w praktyce konieczność zapewnienia jak najdalej posuniętych zabezpieczeń prywatności w ustawieniach początkowych każdego systemu, czy platformy internetowej. Zabezpieczenia mają być ustawione domyślnie, bez konieczności jakiegokolwiek działania osób, których dane dotyczą, i to w kluczowym dla użytkownika momencie, przyłączenia się do danego systemu lub wejścia na stronę internetową. Co więcej, domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu, dla którego zostały zebrane (minimalizacja danych – art. 5 ust. 1 lit. c RODO), a poszerzenie zakresu udostępnianych

[9] Przyjmuje się, iż ochrona danych jest domyślnym prawem każdego obywatela. Mimo, iż nie jest dokładnie sprecyzowane, jakie środki techniczne i organizacyjne należy wdrożyć, rozporządzenie podpowiada, że takie środki mogą polegać, m.in. na minimalizacji przetwarzania danych osobowych, ich pseudonimizacji, przejrzystości, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń. Co ważne, środki te mają zapewniać, aby domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób fizycznych.

[10] „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 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 RODO).

danych może nastąpić jedynie na podstawie zmiany ustawień dokonanych przez samego użytkownika.

Na administratorze spoczywa również obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, za które odpowiada (art. 30 RODO). Obowiązek ten nie ma jednak zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób (chyba że przetwarzanie, którego dokonuje, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą; nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa).

W sytuacji, w której przetwarzanie danych osobowych, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele, z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator ma obowiązek dokonania oceny skutków planowanych operacji przetwarzania danych przed rozpoczęciem ich przetwarzania (art. 35 RODO).

Ustawodawca europejski w art. 37 rozporządzenia nałożył na administratorów obowiązek wyznaczenia Inspektora Ochrony Danych (gdy przetwarzania dokonuje organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości)[11].

W przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki, w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, ma obowiązek zgłoszenia naruszenia do organu nadzorczego oraz zawiadamiania o tym osoby, której dane te dotyczą, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 i 34 RODO). Obowiązek ten wiąże się bezpośrednio ze zobowiązaniem administratora do dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym ich okoliczności, skutków oraz podjętych działań zaradczych.

Nowe przepisy wymusiły na administratorach opracowanie sprawnych procedur przetwarzania danych osobowych, a gdy przetwarzane były automatycznie, dostosowanie funkcjonalności systemów. W wypadku uchybienia jakimkolwiek ze swoich obowiązków, administratorzy danych muszą się liczyć z dotkliwymi karami finansowymi.

[11] Przez organy i podmioty publiczne obowiązane do wyznaczenia IOD, o których mowa w art. 37 ust. 1 lit. a RODO, rozumie się jednostki sektora finansów publicznych (np. jednostki samorządu terytorialnego, uczelnie publiczne), instytuty badawcze oraz Narodowy Bank Polski (art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych).

## 3. PRAWO DOSTĘPU DO DANYCH I INFORMACJI

Zgodnie z art. 15 RODO administrator jest obowiązany udzielić dostępu do przetwarzanych danych osobie, której dane dotyczą, jeśli zgłosi ona takie żądanie[12]. Jednak w żadnym wypadku realizacja prawa dostępu do danych nie powinna naruszać praw lub wolności innych osób, co oznacza, że administrator danych osobowych powinien dopilnować, aby udzielenie informacji nie spowodowało przypadkowego ujawnienia danych także innych osób.

Prawu dostępu do danych i informacji odpowiada obowiązek administratorów danych do przekazywania osobie fizycznej podczas pozyskiwania jej danych, a przed rozpoczęciem ich przetwarzania, w szczególności następujących informacji: tożsamości i danych kontaktowych administratora; celu przetwarzania danych osobowych, informacji o odbiorcach (lub kategoriach odbiorców) danych, ze szczególnym uwzględnieniem podmiotów pochodzących z państw trzecich; okresu, przez jaki dane osobowe będą przetwarzane, a gdy nie można go dokładnie określić, kryteriów ustalania tego okresu (np. przez okres trwania umowy); informacji o zautomatyzowanym podejmowaniu decyzji (w tym o profilowaniu), a także możliwych wynikających z tego konsekwencjach dla osoby, której dane dotyczą; informacji o prawie wniesienia skargi do organu nadzorczego; informacji o źródle pozyskania danych (jeśli nie zostały one pozyskane od osoby, której dotyczą); informacji o prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania; a także o prawie do przenoszenia danych

[12] Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Obejmuje to prawo dostępu osób, których dane dotyczą, do danych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi. Dlatego też każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania. W miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji. Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie, Motyw 63, Preambuła RODO.

oraz, gdy ma to zastosowanie – informacji o zamiarze przekazania danych osobowych poza Unię Europejską oraz wzmianki o odpowiednich zabezpieczeniach danych osobowych stosowanych przez podmiot, któremu dane są przekazywane.

Ponadto osoba, której dane dotyczą[13] może żądać od administratora uzyskania dostępu do tych danych oraz, jeśli zajdzie taka potrzeba, uzyskania ich kopii. Żądanie takie może przybrać formę zarówno elektroniczną, jak i papierową. Jednak w sytuacji, gdy żądanie będzie miało formę elektroniczną, kopia powinna również, w miarę możliwości, przybrać taką samą formę (chyba, że żądający wskaże inaczej). Kopia ta powinna zostać wydana bezpłatnie za pierwszym razem, przy kolejnych prośbach może zostać nałożona na wnioskującego rozsądna opłata, wynikająca z poniesionych kosztów administracyjnych.

## 4. PRAWO DO SPROSTOWANIA DANYCH

Zgodnie z art. 16 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych. Przepis ten przewiduje dwa odrębne uprawnienia przysługujące osobom, których dane dotyczą, a mianowicie: prawo do sprostowania danych nieprawidłowych i prawo do uzupełnienia danych niekompletnych[14].

W pierwszym wypadku podmioty danych mogą żądać poprawienia danych nieprawidłowych, a więc takich, których treść nie odpowiada rzeczywistemu stanowi, co odpowiada ogólnej zasadzie z art. 5 ust. 1 lit. d. RODO, która wymaga od administratorów, aby przetwarzane dane były prawidłowe, jak również, aby dane błędne, niezwłocznie (możliwie szybko) usunięto lub sprostowano.

W drugim przypadku, zgodnie z RODO, prawo do uzupełnienia danych niekompletnych przysługuje z uwzględnieniem celów przetwarzania. Zatem, jeśli do administratora zgłosi się podmiot danych, który zażąda uzupełnienia katalogu danych o te, które nie są administratorowi niezbędne do działania, administrator nie musi rozpatrywać takiego wniosku pozytywnie, nie mniej jednak powinien poinformować żądającego o podjętych działaniach, najpóźniej w terminie miesiąca od otrzymania żądania – termin można wydłużyć

[13] Administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. Administrator nie powinien zatrzymywać danych osobowych wyłącznie w celu reagowania na ewentualne żądania, Motyw 64, Preambuła RODO.

[14] Nie są to nakazy nowe, ustawa o ochronie danych osobowych z 1997 r. w art. 32 ust. 1 pkt 6 również przewidywała taki obowiązek.

o kolejne dwa miesiące, ale tylko ze względu na skomplikowany charakter żądania lub ich liczbę.

Ustawodawca uregulował w rozporządzeniu również kwestię sposobu przeprowadzania procedury rozpatrywania żądań o sprostowanie danych. Przede wszystkim, zgodnie z art. 12 ust. 1 RODO, wszelka komunikacja z osobą, której dane dotyczą powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka. Adresat ma zrozumieć przeznaczony dla niego komunikat. Ponadto administrator powinien podejmować działania, które ułatwiają osobie, której dane dotyczą wykonanie przysługujących jej praw oraz nie powinien odmawiać podjęcia działań na żądanie tej osoby, chyba że wykaże, że nie jest w stanie jej zidentyfikować (co oznacza, że aby odmówić rozpatrzenia żądania należy uprzednio podjąć wszelkie rozsądne środki w celu zidentyfikowania osoby, która z nim wystąpiła).

Działania podejmowane na podstawie żądania o sprostowanie lub uzupełnienie danych powinny być wolne od opłat (art. 12 ust. 5 RODO), lecz jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne (np. ze względu na swój ustawiczny charakter) administratorowi przysługuje prawo do pobrania rozsądnej opłaty, która uwzględnia administracyjne koszty prowadzenia komunikacji i podjętych działań lub odmowa podejmowania działań. Są to jednak środki wyjątkowe i powinny być stosowane jedynie w sytuacjach, w których nie ma żadnych wątpliwości co do nieuzasadnionego lub nadmiernego charakteru żądania – szczególnie, że obowiązek wykazania takich cech w ewentualnym postępowaniu przed organem nadzorczym spoczywa na administratorze, a nie na osobie kierującej żądanie.

Na administratorze natomiast spoczywa obowiązek poinformowania wszystkich odbiorców, którym ujawniono dane o fakcie dokonania sprostowania. Wyjątkowo może tego nie robić, gdy działanie takie okazałoby się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.

## 5. PRAWO DO SPRZECIWU ORAZ NIEPODLEGANIU DECYZJI OPARTYCH NA ZAUTOMATYZOWANYM PRZETWARZANIU

Prawo sprzeciwu uregulowane w art. 21 RODO mówi, że osoba, której dane dotyczą ma prawo nie zgodzić się na to, aby jej dane były wykorzystywane do celów podejmowania decyzji opartych na zautomatyzowanym przetwarzaniu (np. profilowania), które powodują skutek prawny dla osoby[15]. Konsekwencją

[15] RODO nie wprowadza zakazu profilowania, nie zezwala jedynie, by na podstawie profilowania były podejmowane zautomatyzowane decyzje, wywołujące skutki prawne lub istotnie wpływające na osobę, gdy brakuje innych niż zgoda przesłanek legalizujących tego typu działanie.

skorzystania z tego uprawnienia jest zakaz dla administratora przetwarzania tych danych, 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. Wyjątkiem jest sytuacja, w której dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego. Wówczas osoba, której dane dotyczą, ma prawo w dowolnym momencie, bezpłatnie, wnieść sprzeciw wobec tego przetwarzania (pierwotnego lub dalszego – w tym profilowania). Prawo to powinno zostać wyraźnie, oddzielnie od wszelkich innych informacji, podane do wiadomości osobie, której dane dotyczą.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, osoba, której dane dotyczą, ma prawo wnieść sprzeciw, z przyczyn związanych z jej szczególną sytuacją, wobec przetwarzania dotyczących jej danych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Nawet, jeżeli dane są przetwarzane zgodnie z prawem, gdy ich przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym, lub w ramach sprawowania władzy publicznej powierzonej administratorowi, lub ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej, każdej osobie, której dane dotyczą, przysługuje prawo sprzeciwu wobec przetwarzania danych dotyczących jej szczególnej sytuacji. Za wykazanie, że ważne prawnie, uzasadnione interesy administratora mają nadrzędny charakter wobec interesów lub podstawowych praw i wolności osoby, której dane dotyczą, odpowiada administrator.

Prawo sprzeciwu, może być wykonane za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne, a sprzeciw taki nie wymaga uzasadnienia i jest wiążący dla administratora danych, który nie może zasłaniać się swoimi uzasadnionymi interesami. Skorzystanie z tego prawa nie spowoduje, że administrator automatycznie usunie wszystkie informacje, które o nas posiada, ale spowoduje, że przestanie z ich korzystać. Do tego, żeby dane zostały usunięte, konieczne jest skorzystanie z innego prawa – do bycia zapomnianym (czyli do żądania usunięcia danych).

## 6. PRAWO DO OGRANICZENIA PRZETWARZANIA DANYCH

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia ich przetwarzania w następujących przypadkach (art. 18 RODO): gdy osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych (na okres pozwalający administratorowi sprawdzić prawidłowość tych danych); przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia

ich wykorzystywania; administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń; osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania (ograniczenie obowiązuje do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą).

Jeżeli przetwarzanie zostało ograniczone, takie dane można przetwarzać, (z wyjątkiem przechowywania) wyłącznie za zgodą osoby, której dane dotyczą lub w celu ustalenia, dochodzenia lub obrony roszczeń, a także w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego[16].

Fakt ograniczenia przetwarzania danych osobowych należy wyraźnie zaznaczyć w systemie, natomiast przed uchyleniem ograniczenia przetwarzania administrator musi poinformować o tym osobę, która żądała ograniczenia.

## 7. PRAWO DO PRZENOSZENIA DANYCH POMIĘDZY RÓŻNYMI PODMIOTAMI (ADMINISTRATORAMI)

Prawo do przenoszenia danych (art. 20 RODO) jest ściśle związane z prawem dostępu do danych (art. 15 RODO) i polega na prawie żądania od administratora informacji (kopii danych), które osoba fizyczna mu przekazała na potrzeby zawarcia i realizacji umowy lub na podstawie udzielonej zgody (np. na przetwarzanie danych w celach marketingowych).Jeśli żądanie takie zostało wystosowane, administrator ma obowiązek przekazać osobie komplet zgromadzonych danych na jej temat, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego.

Prawo do przenoszenia danych może być zrealizowane, jeżeli dane uprawnionej osoby są przetwarzane w sposób zautomatyzowany; na podstawie zgody osoby, której dane dotyczą (bez względu na to, czy zgoda dotyczy danych zwykłych, czy wrażliwych) lub na podstawie umowy, której stroną jest osoba, której dane dotyczą[17].

---

[16] Do metod ograniczających przetwarzanie danych osobowych należą m.in.: czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania czy uniemożliwienie użytkownikom dostępu do wybranych danych lub czasowe usunięcie opublikowanych danych ze strony internetowej. W zautomatyzowanych zbiorach danych przetwarzanie należy zasadniczo ograniczyć środkami technicznymi w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane.

[17] Ustawodawca mówi tutaj o sytuacji, w której przetwarzanie danych jest niezbędne do wykonania umowy zawartej z tą osobą lub gdy przetwarzanie danych jest niezbędne do podjęcia określonych działań na żądanie tej osoby przed zawarciem umowy.

Z tego uprawnienia wynika, że można żądać od administratora danych zebrania ich w ustrukturyzowanej formie, a następnie przekazania ich innemu administratorowi, bez względu np. na to, czy odbiorca jest przedsiębiorcą działającym w tej samej, czy też w innej branży, o ile jest to technicznie możliwe.

W przypadku skierowania określonego żądania przez osobę, której dane dotyczą, administrator zobowiązany jest do udzielenia informacji o podjętych działaniach w związku ze złożonym żądaniem, w terminie miesiąca od jego otrzymania. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub dużą liczbę żądań. W takim jednak wypadku w terminie miesiąca od otrzymania żądania administrator musi poinformować osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

Jeżeli administrator nie zamierza podejmować działań w związku z żądaniem osoby, której dane dotyczą, jest zobowiązany niezwłocznie, najpóźniej w terminie miesiąca od otrzymania żądania, poinformować taką osobę, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

## 8. PRAWO DO BYCIA ZAPOMNIANYM

Najsilniejszym uprawnieniem przyznanym przez ustawodawcę w rozporządzeniu jest prawo do bycia zapomnianym, czyli prawo żądania usunięcia danych przez administratora (art. 17 RODO)[18]. Ma ono zastosowanie, gdy dane są przetwarzane w sposób niezgodny z prawem; naruszają dobre imię;

[18] Choć na takie wygląda, nie jest to całkowicie nowe uprawnienie. Trybunał Sprawiedliwości Unii Europejskiej w 2014 r. orzekł, że prawo do bycia zapomnianym wynika z przepisów dyrektywy 95/46/WE (poprzedniego aktu unijnego dotyczącego ochrony danych osobowych, który implementował polski ustawodawca). Sprawa C-131/12: Wyrok Trybunału (wielka izba) z dnia 13 maja 2014 r. – *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi*. Wniosek o wydanie orzeczenia w trybie prejudycjalnym: Audiencia Nacional – Hiszpania. Dane osobowe – ochrona osób fizycznych w zakresie przetwarzania tego typu danych – Dyrektywa 95/46/WE – art. 2, 4, 12 i 14 – zakres rzeczowy i terytorialny – wyszukiwarki internetowe – przetwarzanie danych zawartych na stronach internetowych – wyszukiwanie, indeksowanie i przechowywanie tego typu danych – odpowiedzialność operatora wyszukiwarki – prowadzenie działalności gospodarczej na terytorium państwa członkowskiego – zakres obowiązków zainteresowanego operatora i praw osoby, której dane dotyczą – Karta praw podstawowych Unii Europejskiej – art. 7 i 8, Dz. U. C 212 z 7.7.2014, s. 4-5, https://tizydorczyk.pl/lib/tsue/TSUE_wyr_C-131-12.pdf; www.eur-lex.europa.eu [dostęp: 11.12.2019]. Orzeczenie to zostało wydane w związku ze sprawą Hiszpana, któremu zlicytowano dom, a informacja o tym cały czas pojawiała się w wyszukiwarce, choć spłacił swoje długi. Trybunał uznał, że jeśli informacje dotyczące jakiejś osoby są niewłaściwe, niestosowne bądź nadmierne w stosunku do celów, w jakich są przetwarzane przez operatora wyszukiwarki, powinny zostać usunięte.

bądź nie są już niezbędne do spełnienia celu, w jakim były zbierane, niezależnie od tego, czy zostały umieszczone przez osobę, której dotyczą czy przez osoby trzecie. Już w preambule rozporządzenia, ustawodawca unijny podkreślił prawo każdej osoby do bycia zapomnianym, o ile zatrzymanie jej danych narusza RODO, prawo Unii lub prawo Państwa Członkowskiego, któremu podlega administrator. Uwypuklono zwłaszcza przypadek wyrażenia zgody na przetwarzanie danych przez dziecko. Zgodnie z RODO dzieci, które ukończyły 16 lat, mogą samodzielnie decydować o przekazywaniu swoich danych osobowych firmom internetowym. Ustawodawca wyszedł jednak z założenia, że należy im się szczególna ochrona, bo mogą nie być świadome ryzyka i konsekwencji z tym związanych (szczególnie kiedy w grę wchodzi wykorzystywanie danych do celów marketingowych lub tworzenia profili osobowych). Dlatego dziecku przysługuje bezwzględne prawo rozmyślenia się i zażądania usunięcia przekazanych wcześniej danych.

W razie skorzystania z tego prawa, administrator ma obowiązek, bez zbędnej zwłoki, usunąć ze wszystkich swoich systemów, dane pochodzące od tej osoby, o ile nie występują nadrzędne prawnie uzasadnione podstawy ich przetwarzania. Zatem administrator powinien usunąć dane, jeżeli nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane[19]; dane osobowe były przetwarzane niezgodnie z prawem; osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania (dotyczy to także zgody na przetwarzanie tzw. danych wrażliwych); osoba, której dane dotyczą wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania; dane osobowe muszą zostać usunięte również w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator oraz gdy zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

Jeżeli administrator uprzednio te dane upublicznił, ma obowiązek, biorąc pod uwagę dostępną technologię i koszt realizacji, podjąć rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych lub ich replikacje. Niemniej jednak, wskazany obowiązek odnosi się jedynie do administratorów, którzy wykorzystują dane wyłącznie na podstawie udzielonej zgody. Jeśli podstawą przetwarzania danych jest umowa, której wykonanie wymaga

[19] Co do zasady, dane zawsze są zbierane w określonym celu i na określony czas (np. dla zrealizowania określonej usługi albo wypełnienia obowiązku prawnego (np. rozliczenie podatku). W dobrze działającym systemie takie żądanie nie powinno być potrzebne, a każda firma/instytucja powinna z własnej inicjatywy usuwać dane, które przestały jej być potrzebne.

przetwarzania danych, wówczas prawo do bycia zapomnianym nie znajduje zastosowania. W takiej sytuacji żądanie usunięcia danych wymaga wcześniejszego rozwiązania umowy.

Administrator może odmówić usunięcia wcześniej upublicznionych danych, jeśli naruszałoby to prawo innych osób do korzystania z wolności wypowiedzi lub prawa do informacji; gdy przetwarzanie danych jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa Państwa Członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Przesłanką negatywną jest również interes publiczny w dziedzinie zdrowia publicznego, tj. gdy przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia.

Dane nie zostaną usunięte również wtedy, gdy ich przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego (takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi) lub w związku z zapewnieniem wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową. Podobnie, gdy dane są przetwarzane do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

W końcu administrator może odmówić usunięcia danych jeżeli są one niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

W przypadku, gdy administrator nie może spełnić żądania osoby, której dane dotyczą, tj. gdy żądanie jest nieuzasadnione lub zachodzi wskazany w RODO, a wyżej wymieniony wyjątek, ma obowiązek poinformować wnioskodawcę o przyczynach swojej odmowy.

Należy pamiętać, że przepis stanowiący prawo do bycia zapomnianym, nie obowiązuje poza krajami Unii Europejskiej oraz Islandią, Norwegią, Szwajcarią i Lichtensteinem. Użytkownicy spoza Starego Kontynentu bez problemu odnajdą ukryte na mocy tego prawa treści. Poza tym korzystając z Internetu, zawsze trzeba pamiętać, że żadne informacje nie znikają zupełnie z sieci. Są wprawdzie kasowane z wyników wyszukiwania, co jedynie mocno utrudnia ich znalezienie, ale nie uniemożliwia[20].

[20] Prawo do bycia zapomnianym było jednym z najgoręcej dyskutowanych aspektów RODO w okresie projektowania, zwłaszcza w świetle sprawy Gonzaleza, której rozstrzygnięcie przy-

## ZAKOŃCZENIE

To, w jaki sposób administratorzy realizują w praktyce nałożone na nich obowiązki, jest oceniane przez organy nadzoru z punktu widzenia podstawowego celu Rozporządzenia – zapewnienia, że osoby udzielające zgody na przetwarzanie danych osobowych są w pełni świadome celu, procesu i konsekwencji przetwarzania ich danych[21]. RODO daje osobom, których dane są przetwarzane realny wpływ na ich kształt oraz możliwość ich kontroli w każdej chwili, a w razie pogwałcenia ich praw, dochodzenia odszkodowania oraz złożenia skargi do organu nadzoru.

Zagrożenie wysokimi karami oraz odpowiedzialność odszkodowawcza przedsiębiorców za naruszenia[22], wymusiły na administratorach danych dostosowanie swojej działalności do nowych wymogów ochrony danych osobowych, co z założenia ma się przyczynić do wzrostu zaufania do przedsiębiorców, w związku z oferowanymi przez nich usługami związanymi z przetwarzaniem danych osobowych.

Czy tak się stało? Jeszcze jest za wcześnie na taką ocenę. Z jednej strony chętnie się podkreśla, że tak szeroki zakres uprawnień przyznanych osobom, których dane są przetwarzane wynika z respektowania, zarówno przez samą UE, jak i przez poszczególne państwa, ich prawa do prywatności, z drugiej strony warto pamiętać, że jeszcze nigdy w historii ludzkości żadna władza nie dysponowała tak potężnymi środkami do sprawowania nadzoru nad swoimi

padło na okres konsultacji RODO (zob. przypis nr 18). Zdecydowany opór wobec proponowanych rozwiązań stawiali przede wszystkim dostawcy usług on-line i serwisów społecznościowych (argumentując, że stanowią one zagrożenie dla ich modeli biznesowych opierających się na wykorzystaniu danych osobowych w celach reklamowych i analitycznych). Poza tym prawo do bycia zapomnianym uważane za kolidujące, do pewnego stopnia, z wolnością wypowiedzi. Postrzegane jest również jako narzędzie ucieczki od przeszłości, po które mogą sięgać np. przestępcy.

[21] W Polsce Prezes Urzędu Ochrony Danych Osobowych zastąpił dotychczasowego Generalnego Inspektora Ochrony Danych Osobowych i jest nowym organem sprawującym nadzór nad danymi osobowymi (art. 34, pkt 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. poz. 1000). Zasadnicze kompetencje Prezesa UODO nie uległy zmianie w porównaniu do kompetencji GIODO, ponieważ wynikają z niezmienionej głównej funkcji tego organu jako organu właściwego w sprawie ochrony danych osobowych. Zyskał on jednak dodatkowy status – organu nadzorczego nie tylko w rozumieniu RODO, ale także w rozumieniu tzw. dyrektywy policyjnej (dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW, Dz. Urz. UE, 4.5.2016, L 119/89.

[22] Kara może wynieść nawet 20 milionów euro, a w przypadku przedsiębiorstwa – do 4% jego całkowitego rocznego obrotu światowego brutto (w zależności od tego, która jest wyższa) – art. 5 RODO.

obywatelami [Ciborski 2015, 9]. Współczesna technologia daje rządom i korporacjom rozbudowane możliwości masowej inwigilacji, która jest wykorzystywana do kontroli tego, co widzimy, co robimy, a ostatecznie tego, co mówimy [Schneier 2017, 12].

## PIŚMIENNICTWO

Chrabonszczewski, Maciej. 2012. *Prywatność. Teoria i praktyka*. Warszawa: Aspra.
Ciborski, Tomasz. 2015. *Ukryta tożsamość. Jak się obronić przed utratą prywatności*. Gliwice: Helion.
Pryciak, Marcin. 2010. „Prawo do prywatności." *Studia Erasmiana Wratislaviensia* 4:211–29.
Schneier, Bruce. 2017. *Dane i Goliat. Ukryta bitwa o Twoje dane i kontrolę nad światem*. Gliwice: Helion.
Sprenger, Polly. 1999. "Sun on privacy: «Get over it»." https://www.wired.com/1999/01/sun-on-privacy-get-over-it/ [dostęp: 11.12.2019].
Zawadzka, Zofia. 2013. *Wolność prasy a ochrona prywatności osób wykonujących działalność publiczną. Problem rozstrzygania konfliktu zasad.* Warszawa: Wolters Kluwer Polska.
„Złudna anonimowość w sieci." https://docplayer.pl/15133366-Zludna-anonimowosc-w-sieci.html [dostęp: 11.12.2019].

## THE NEW RESPONSIBILITIES FOR PERSONAL DATA CONTROLLERS AND PROCESSORS

**Summary.** Privacy is a problem that touches virtually all aspects of human life and the changes occurring in the modern world and the development of technical means for collection, storage and retrieval of information about other people have increased the need to legally protect the human right to privacy, i.e. the right "to be left alone"). In the age of digital democracy, there has emerged a need to adopt systemic solutions that would take into account both new threats and ways of violating human rights and freedoms. On the European ground, the response to such demand was the implementation of the regulation on personal data protection – GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), which entered into force on 25 May 2018.

**Key words:** personal data, General Data Protection Regulation (GDPR), personal data processing, right to privacy, right to be forgotten

**Information about Author:** Marzena Toumi, hab. Ph.D., University Professor – Department of History and Theory of Law, Institute of Law at the War Studies University; e-mail: marzenatoumi@gmail.com; https://orcid.org/0000-0003-3838-1315