

KRYTERIUM LEGALNOŚCI ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH W OBRODZIE ELEKTRONICZNYM

STRESZCZENIE

W prawodawstwie europejskim podstawowym aktem prawnym z zakresu ochrony danych osobowych jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Uzasadnieniem uregulowania zasad ochrony danych osobowych stała się skala zbierania i wymiany danych osobowych. Celem niniejszej pracy jest analiza i ocena najnowszych europejskich regulacji prawnych z zakresu ochrony danych osobowych i ich rozwiązań, w tym praw i obowiązków podmiotów danych oraz osób przetwarzających dane osobowe, w zakresie zwiększenia kontroli nad przepływem danych osobowych różnego rodzaju.

SŁOWA KLUCZOWE

Dane osobowe, przetwarzanie danych, RODO

1. WPROWADZENIE

W prawodawstwie europejskim podstawowym aktem prawnym z zakresu ochrony danych osobowych jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE² (dalej: RODO). Uzasadnieniem dla uregulowania zasad ochrony danych osobowych stała się skala zbierania i wymiany danych osobowych. Powyższe wynika z postępu technologicznego i globalizacji, przy jednoczesnym obserwowanym wzroście nadużyć czy przestępstw związanych z nieuprawnionym wykorzystywaniem danych osobowych. Uregulowanie zasad

¹ Instytutu Nauk Prawnych Polskiej Akademii Nauk.

² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Dz.U. UE L 119/1 z 4.5.2016).

ochrony danych osobowych miało na celu zapobieganie naruszeniom swobodnego przepływu danych osobowych w Unii Europejskiej (dalej: UE), przy uwzględnieniu praw jednostki do ochrony jej danych osobowych³. Forma rozporządzenia została wybrana z uwagi na konieczność stworzenia spójnej regulacji w zakresie ochrony danych osobowych w UE.

Celem niniejszej pracy jest analiza i ocena najnowszych europejskich regulacji prawnych z zakresu ochrony danych osobowych i ich rozwiązań, w tym praw i obowiązków podmiotów danych oraz osób przetwarzających dane osobowe, w zakresie zwiększenia kontroli nad przepływem danych osobowych różnego rodzaju.

2. DEFINICJE LEGALNE

Zgodnie art. 4 pkt 1 RODO dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Dane osobowe dzieli się na: dane osobowe zwykłe, typu: imię i nazwisko, adres zamieszkania, identyfikatory internetowe, numer telefonu, płeć, kolor oczu, waga, wzrost oraz dane osobowe szczególne (inaczej wrażliwe), którymi są m.in. dane o orientacji seksualnej, dane biometryczne i dane genetyczne, dane ujawniające pochodzenie rasowe lub etniczne, czy dane z rejestru skazanych⁴.

Zgodnie z definicją, którą znajdziemy w art. 4 pkt 2 RODO, przetwarzanie danych osobowych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. Przetwarzaniem danych osobowych jest każde działanie dokonane na zbiorze danych osobowych niezależnie od tego, czy odbywa się techniką tradycyjną czy przy wykorzystywaniu systemów informatycznych i obejmuje wszystkie możliwe formy operacji wobec danych osobowych⁵.

W tym miejscu należy wskazać, że nawet zgoda nie może legitymizować nieadekwatnego, ani nadmiarowego przetwarzania danych w stosunku do celu zbierania danych.

³ *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. KAWECKI, T. OSIEJA, Warszawa 2017, s. 12.

⁴ *RODO. Ogólne rozporządzenie o ochronie danych*, red. E. BIELAK-JOMAA, D. LUBASZ, Warszawa 2018, s. 171.

⁵ GIODO, *Gotowi na RODO*, https://uodo.gov.pl/data/filemanager_pl/641.pdf (data dostępu: 22 czerwca 2019, godz. 20:48.).

3. ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH W OBRODIE TRADYCYJNYM

W rozumieniu art. 4 pkt 11 RODO zgoda na przetwarzanie danych osobowych oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli w formie oświadczenia lub wyraźnego działania. Istotne, że zgoda wyrażana przez wyraźne działanie potwierdzające może być stosowana tylko wobec danych osobowych zwykłych, gdyż przy przetwarzaniu danych osobowych wrażliwych podstawą prawną może być tylko zgoda wyraźna, czyli wyrażana poprzez pisemne oświadczenie woli⁶.

Dobrowolność oznacza, że podmiot danych musi mieć możliwość wyboru pomiędzy wyrażeniem zgody a jej niewyrażeniem, bez wpływu na relacje z administratorem w obszarach nieobjętych zgodą⁷. Dobrowolna jest zgoda, która stanowić będzie decyzję podjętą z własnej inicjatywy przez osobę będącą w pełni władz umysłowych oraz bez jakiegokolwiek przymusu o charakterze społecznym, finansowym, psychologicznym czy innym⁸. Dlatego też wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

Zgodnie z Motywem (43) RODO zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą a administratorem danych osobowych, w szczególności, gdy administrator jest organem publicznym. Iluzoryczna byłaby dobrowolność zgody we wszystkich przypadkach, gdy administratorem będzie organ administracji.

Wyżej wymieniona przesłanka dobrowolności oceniana jest przez pryzmat czterech kryteriów, tj. kryterium równowagi stron, kryterium niezbędności zgody do wykonania umowy, kryterium świadczenia charakterystycznego, a także kryterium rozsądnej alternatywy. To ostatnie kryterium nie wynika wprost z przepisów. Zdaniem E. Bielak-Jamaa i D. Lubasza powinno zabraniać się uzależniania świadczenia usług przez administratora od zgody na przetwarzanie danych osobowych, o ile w przypadku niewyrażenia zgody podmiot danych nie będzie mógł otrzymać równoważnego świadczenia w ogóle bądź na rozsądnych warunkach⁹.

⁶ A. SAGAN-JEŻOWSKA, *Klauzule RODO. Wzory klauzul z praktycznym komentarzem*, Warszawa 2018, s. 24.

⁷ Tamże.

⁸ RODO. *Ogólne rozporządzenie...*, *op. cit.*, s. 247.

⁹ Tamże, s. 4267.

Co ważne, zgody nie uważa się za dobrowolną, jeżeli nie można wyrazić jej z osobna na różne operacje przetwarzania danych osobowych. Od zgody uzależnione jest wykonanie umowy, w tym świadczenie usługi, chociaż do wykonania umowy zgoda nie jest niezbędna. Przykładowo, w sytuacji uczestnictwa w projekcie, które jest uwarunkowane udzieleniem zgody na przetwarzanie danych dla celów marketingowych, wyrażona zgoda nie będzie w takim przypadku spełniać wymogu dobrowolności. Dopiero podzielenie zgody na przetwarzanie danych na potrzeby wykonania umowy i na przetwarzanie danych dla celów marketingowych będzie stanowiło o dobrowolności wyrażenia zgody na cele marketingowe, o ile brak wyrażenia tej zgody nie będzie uniemożliwiać uczestnictwa w projekcie.

Kolejną przesłanką kryterium legalności zgody na przetwarzanie danych to konkretność, co oznacza, że musi dotyczyć konkretnej sytuacji przetwarzania danych osobowych do celów i zakresu przetwarzania. Zgoda konkretna powinna być również dokładnie określona, precyzyjna i rzeczowa, a także musi odnosić się do celu, w którym dane osobowe będą przetwarzane. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele z osobna. Zgoda konkretna musi zawierać jasno sprecyzowane cele przetwarzania. Jedna zgoda może obejmować kilka czynności przetwarzania, o ile wszystkie służą temu samemu celowi. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

Cecha jednoznaczności oznacza, że oświadczenie musi precyzyjnie wskazywać na to, że osoba, której dane dotyczą, zgodę wyraziła, a zatem zgoda nie może być domniemana. Jednoznaczność jako cecha wyrażenia zgody oznacza brak wątpliwości co do zamiaru wyrażenia zgody przez osobę, której dane dotyczą¹⁰. W tym miejscu wskazać należy, że wyrażenie zgody według RODO oparte jest na systemie *opt-in*, co wymaga określonej aktywności podmiotu danych i jednoznacznego okazania woli. Niedopuszczalne są więc wszelkie modele *opt-out*, jako opierające się na bierności, milczeniu, nieuwadze, czy też bezwolności, np. poprzez domyślnie zaznaczone okienka zgód (tzw. *checkbox'y*) w trakcie korzystania ze stron internetowych, czy akceptację regulaminu usługi określającej kwestię zgody w zakresie wykraczającym poza realizację usługi¹¹. Właściwe jest także inne oświadczenie, wyrażone w motywie (32) RODO przy zachowaniu, które będzie jasno

¹⁰ RODO. *Ogólne rozporządzenie...*, op. cit., s. 255.

¹¹ Tamże, s. 352.

wskazywać, że podmiot danych zaakceptował proponowane przetwarzanie jego danych osobowych.

Pozostaje jeszcze do omówienia czwarta kategoria, tzn. świadomość, która oznacza, że podmiot danych musi mieć świadomość tego, na co zgodę wyraża, a ponadto powinien znać przynajmniej tożsamość administratora i zamierzone cele przetwarzania danych osobowych. Dobrowolność oznacza zaś, że podmiot danych musi mieć możliwość wyboru pomiędzy wyrażeniem zgody a jej niewyrażeniem bez wpływu na relacje z administratorem w obszarach nieobjętych zgodą¹².

4. PRZETWARZANIE DANYCH ZGODNE Z PRAWEM

Adekwatnie do art. 6 RODO przetwarzanie danych jest zgodne z prawem, o ile spełniony jest co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- 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.

¹² Tamże.

Zgoda może być wyrażona z zastrzeżeniem warunku i może obowiązywać po ziszczeniu się tego warunku, a także może być zgodą terminową z uwagi na określenie terminu ważności zgody, z którego upływem zgoda wygaśnie. Zgoda może być także ograniczona terytorialnie, np. do przetwarzania na obszarze danego państwa. Zgoda może być też udzielona ze wskazaniem podmiotowym, tzn. z zastrzeżeniem, że przetwarzanie może być dokonywane jedynie przez oznaczoną osobę. Zdaniem J. Barty i P. Fajgielskiego, zgoda na przetwarzanie danych może być również zgodą częściową, tzn. dotyczyć nie wszystkich operacji wchodzących w zakres pojęcia przetwarzania danych osobowych¹³.

Zgoda na przetwarzanie danych to czynność prawna zgodnie z art. 17 kodeksu cywilnego¹⁴ (dalej k.c.). Zasadniczo, zgodę uznaje się za czynność zbliżoną do oświadczenia woli, chociaż RODO nie zawiera w tym zakresie wskazówek¹⁵. Jednakże ma to istotne znaczenie praktyczne, z uwagi na możliwość składania oświadczenia woli przez pełnomocnika bądź kwestię stosowania przepisów o wadach oświadczenia woli do zgody. Zatem możliwe jest, aby osoba, która wyraziła początkowo zgodę na przetwarzanie danych osobowych, następnie pod wpływem błędu uchyliła się od skutków prawnych oświadczenia woli poprzez złożenie pisemnego oświadczenia, wskutek czego wyrażona uprzednio zgoda będzie nieważna od samego początku. Rodzi to wówczas konsekwencje dla administratora danych w wyniku niezgodnego z prawem przetwarzania danych osobowych. Przepis art. 60 w zw. z art. 84 § 1 k.c. o wadach oświadczenia woli może stanowić podstawę uchylecia się przez osobę, której dane dotyczą, od skutków prawnych zgody na przetwarzanie danych, wyrażonej przez nią pod wpływem istotnego błędu, wynikającego z przekazania tej osobie przez administratora danych niedostatecznej lub nieprawdziwej informacji o celu ich zbierania, lub o odbiorcach danych. Bezskuteczność uchylecia się od skutków prawnych zgody na przetwarzanie danych przez osobę, której dane dotyczą, wyrażonej pod wpływem błędu jest uzależniona od prawidłowości spełnienia wobec niej obowiązku informacyjnego. W konsekwencji zgoda będzie nieważna w przypadku, gdy podmiot danych znajduje się w stanie wyłączającym swobodne lub świadome wyrażenie woli. Podobnie nieważna będzie zgoda wyrażona pod wpływem istotnego błędu, podstępny, czy bezprawnej groźby¹⁶.

¹³ J. BARTA, P. FAJGIELSKI, R. MARKIEWICZ, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, s. 452-453.

¹⁴ Ustawa z 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. Nr 16, poz. 93 ze zm.).

¹⁵ B. KACZMAREK-TEMPLIN, *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia*, [w:] *Polska i europejska reforma ochrony danych osobowych*, red. E. BIELAK-JOMAA, D. LUBASZ, Warszawa 2016, s. 104-105.

¹⁶ Tamże, s. 454.

4.2. SPOSOBY I FORMY UDZIELENIA ZGODY NA PRZETWARZANIE DANYCH

Zgoda może być wyrażona w różnej formie. W praktyce zgoda ma często formę pisemnego oświadczenia w obrocie tradycyjnym lub formę elektroniczną. Polegać może wtedy na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług (np. *online*), bądź ma też formę ustnego oświadczenia. Dopuszczalna jest każda inna forma oświadczenia bądź zachowania, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. W przypadku zgody wyrażanej za pośrednictwem poczty elektronicznej, wiadomości tekstowych czy komunikatorów będzie ona skuteczna, o ile dają one możliwość ustalenia tożsamości osoby składającej oświadczenie. Zgodą będzie zatem jedynie wyraźne działanie potwierdzające, z którego jednoznacznie wynika, że osoba potwierdzająca zgadza się na przetwarzanie jej danych w konkretnym celu, a takie wyraźne działanie potwierdzające to np. wręczenie wizytówki, wypełnienie formularza kontaktowego w celu wiadomym, wysłanie danych osobowych konkretnemu administratorowi w określonym celu¹⁷.

Przepisy dopuszczają wyrażenie zgody w formie ustnej, jednakże w praktyce zgoda taka musi być udokumentowana, a takim dowodem na wyrażenie zgody byłoby zasadniczo nagrywanie rozmowy, dlatego przeważają inne formy udzielenia zgody. Jednocześnie wyrażenie zgody na przetwarzanie danych powoduje konieczność wywiązywania się z obowiązków informacyjnych wynikających z art. 14 ust. 2 RODO, natomiast zgodnie z art. 12 ust. 1 RODO informacje o prawach osoby mogą być udzielane ustnie, o ile osoba, której dane dotyczą, tego zażąda, a ponadto innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. Jednocześnie obowiązek udowodnienia posiadania zgody na przetwarzanie danych spoczywa na administratorze.

Z preambuły RODO wynika, że jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania. Zapytanie o zgodę powinno być przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, co ważne, opisaną jasnym i prostym językiem zarówno w pisemnej zgodzie, jak i ustnej. Najczęściej oświadczenie o wyrażeniu zgody na

¹⁷ Tamże, s. 25.

przetwarzanie danych przygotowane jest przez administratora i nie powinno zawierać nieuczciwych warunków. Weryfikacja spełnienia tych przesłanek wymaga wyodrębnienia klauzuli zgody w treści umowy.

Zgodę na przetwarzanie danych wywołującą skutki prawne wyraża co do zasady każda osoba fizyczna samodzielnie. Jednakże RODO chroni szczególnie dzieci w zakresie zgody na usługi społeczeństwa informacyjnego, czyli usługi oferowane i realizowane w trybie *online*. Jeżeli dziecko nie ukończyło 16 lat, to przetwarzanie danych jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody. Dopiero dzieci po ukończeniu 16 lat mogą samodzielnie wyrażać zgodę na przetwarzanie danych w zakresie usług społeczeństwa informacyjnego. Według RODO zgoda nie jest jednak wymagana w zakresie, w jakim świadczenie usług dotyczy doradztwa lub profilaktyki oferowanej bezpośrednio dziecku¹⁸. Administrator, uwzględniając dostępną technologię, powinien podjąć rozsądne starania w celu zweryfikowania, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała. Sposoby weryfikacji nie są określone, ale może to być weryfikacja z wykorzystaniem tzw. przelewów groszowych, czy nawiązywanie kontaktu telefonicznego w celu weryfikacji danych. Wątpliwości może budzić weryfikacja poprzez żądanie potwierdzenia wyrażenia zgody za pośrednictwem poczty elektronicznej.

RODO nie reguluje kwestii warunków wyrażania zgody na przetwarzanie danych osobowych przez osoby niepełnoletnie w zakresie przetwarzania innego niż dotyczące usług społeczeństwa obywatelskiego. Stąd też co do skuteczności zgody osoby fizycznej znajdują zastosowanie przepisy prawa cywilnego z zakresu zdolności do czynności prawnych, gdyż zgoda na przetwarzanie danych osobowych jest oświadczeniem woli. Zgodnie z art. 12 k.c. osoba mająca mniej niż 13 lat nie może złożyć skutecznego oświadczenia woli, a zatem na przetwarzanie jej danych osobowych wymagana jest zgoda opiekuna wyrażona przed złożeniem oświadczenia przez małoletniego. Sytuacja wygląda analogicznie w przypadku osób ubezwłasnowolnionych¹⁹. Małoletni w wieku 13–18 lat, który ma ograniczoną zdolność do czynności prawnych, może składać skutecznie oświadczenia woli. Zgodnie z art. 18 k.c., w niektórych przypadkach – np. potwierdzenie ważności umowy zawartej przez osobę ograniczoną w zdolności do czynności prawnych – wymagane jest potwierdzenie oświadczenia przez jego przedstawiciela ustawowego.

¹⁸ A. SAGAN-JEŻOWSKA, *op. cit.*, s. 34-35.

¹⁹ J. BARTA, P. FAJGIELSKI, R. MARKIEWICZ, *op. cit.*, s. 452.

4.4. WYCOFANIE GODY NA PRZETWARZANIE DANYCH

Zgoda jest ważna zasadniczo aż do momentu jej cofnięcia przez podmiot danych. Wobec tego, zgody pozyskane wcześniej – pod rządami poprzednich regulacji Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, uchylonej z dniem 25 maja 2018 r. są ważne, a w rezultacie możliwe jest przetwarzanie danych w oparciu o te zgody. Zaleca się jednak tzw. *reconsenting*, czyli odświeżanie zgód w odpowiednich odstępach czasu, aby zapewnić świadomość osób, których dane dotyczą, nawet jeśli okoliczności tego przetwarzania nie uległy znaczącej modyfikacji²⁰.

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę, przy czym wycofanie zgody musi być równie łatwe, jak jej wyrażenie. Przy wycofaniu zgody nie ma jednak konieczności składania oświadczenia woli w tej samej formie, w jakiej zgoda była wyrażana, a więc forma wycofania może być inna, o ile pochodzi od osoby, której dane dotyczą. Za nieważne byłoby ustalenie, że skuteczne odwołanie jest możliwe wyłącznie w formie listu poleconego, jako nakładające nadmierne obowiązki na osobę, której dane dotyczą. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania danych osobowych, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym jednocześnie informowana przed wycofaniem zgody. Ponadto osobom fizycznym administratorzy powinni uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z przetwarzaniem, w tym administratorzy mają prawny obowiązek poinformowania osoby o możliwości wycofania zgody, co jest elementem obowiązków informacyjnych towarzyszących gromadzeniu danych osobowych. Wycofanie zgody wywiera skutki *ex nunc*, czyli wywołuje skutki od chwili jego złożenia. W konsekwencji, osoba wycofująca zgodę nie może w żaden sposób zakwestionować legalności przetwarzania danych w okresie pomiędzy wyrażeniem zgody a jej wycofaniem.

Oczywistym jest, że zgoda osoby, której dane dotyczą, może zostać wyrażona wyłącznie przed rozpoczęciem przetwarzania danych przez administratora. Każda zgoda musi być uprzednia względem każdego nowego celu przetwarzania, a zatem nie jest dopuszczalna zgoda o charakterze następczym²¹.

²⁰ A. SAGAN-JEŻOWSKA, *op. cit.*, s. 32-33.

²¹ RODO. *Ogólne rozporządzenie...*, *op. cit.*, s. 356.

Zgody na przetwarzanie danych osobowych uzyskane w ramach obowiązujących wcześniejszych przepisów ustawy o ochronie danych osobowych uchylonej 25 maja 2018 r. nie tracą ważności. Jeżeli pozyskane zostały zgodnie z wymaganiami określonymi w RODO, to znaczy, jeżeli pierwotny sposób wyrażenia zgody odpowiada warunkom RODO. Każdy administrator z chwilą wejścia w życie RODO musiał ocenić, czy pozyskane przez niego zgody spełniają kryteria opisane w art. 4 pkt 11 (dobrowolności, konkretności, świadomości i jednoznaczności), art. 6 ust. 1 lit. a w związku z art. 7 oraz art. 9 ust. 2 lit. a RODO.

5. ZGODA NA PRZETWARZANIE DANYCH W OBRODIE EUROPEJSKIM

Dnia 25 maja 2018 roku miało wejść w życie rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)²² (dalej: rozporządzenie ePrivacy). Przepisy niniejszej dyrektywy uzupełniają Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych²³ oraz Dyrektywę 97/66/WE Parlamentu Europejskiego i Rady z 15 grudnia 1997 r. dotyczącą przetwarzania danych osobowych oraz ochrony prywatności w sektorze telekomunikacyjnym²⁴.

Z kolei poziom bezpieczeństwa ocenia się w świetle przepisów art. 17 dyrektywy 95/46/WE a zawarte w niej regulacje stanowią uzupełnienie i uszczegółowienie RODO w odniesieniu do danych pochodzących z łączności elektronicznej kwalifikujących się jako dane osobowe. Rozporządzenie ePrivacy ma zastąpić dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej²⁵, jednakże z uwagi na cały czas

²² Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej) COM/2017/010 final – 2017/03 (COD).

²³ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. UE 23.11.1995 L 281/31).

²⁴ Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze telekomunikacyjnym (Dz.U. 30.1.1998 L 24).

²⁵ Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201, s. 37, 31.7.2002) zmieniona Dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z 25 listopada 2009 r. zmieniającą dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE

trwające negocjacje, ostateczne brzmienie regulacji na dzień opracowywania niniejszego tekstu nie było znane.

Celem rozporządzenia ePrivacy jest wzmocnienie ochrony użytkowników urządzeń końcowych przed nadmiernym ingerowaniem w sferę ich prywatności. Zapewnia ono ochronę danych osobowych w sektorze łączności elektronicznej. W ciągu ostatnich lat nastąpiły na rynku ważne zmiany technologiczne i gospodarcze, stąd nowe regulacje mają dostosować przepisy do postępu technologicznego i obecnych realiów rynkowych oraz zwiększyć zaufanie do usług cyfrowych. Istotne, że rozporządzenie ePrivacy zapewnia ochronę w sieci nie tylko osobom fizycznym, ale też osobom prawnym.

Rozporządzenie ePrivacy zobowiązuje dostawców usług łączności elektronicznej do uzyskania zgody użytkowników końcowych na przetwarzanie metadanych pochodzących z łączności elektronicznej, które powinny obejmować dane dotyczące lokalizacji urządzenia wygenerowane na potrzeby udzielenia i utrzymania dostępu do usługi oraz połączenia z nią. Użytkownicy końcowi mogą wyrazić zgodę na przetwarzanie swoich metadanych w celu uzyskania konkretnych usług, takich jak usługi ochrony przed oszustwami poprzez analizowanie danych o korzystaniu, lokalizacji i koncie klienta w czasie rzeczywistym. Metadane pochodzące z łączności elektronicznej to: dane przetwarzane w sieci łączności elektronicznej do celów przesyłania, dystrybuowania lub wymiany treści łączności elektronicznej; w tym dane służące do śledzenia i zidentyfikowania źródła i miejsca docelowego przypadku łączności, dane dotyczące lokalizacji urządzenia wygenerowane w związku ze świadczeniem usług łączności elektronicznej oraz daty, godziny, czasu trwania oraz rodzaju łączności. Metadane dostarczają zatem szczególnie chronionych informacji, jak: lokalizacja użytkownika, historia przeglądarki, godzina połączenia bądź czas wysłania wiadomości.

Według art. 6 rozporządzenia ePrivacy dostawcy usług łączności elektronicznej mogą przetwarzać treść łączności elektronicznej w celu świadczenia konkretnej usługi na rzecz użytkownika końcowego, o ile dany użytkownik końcowy lub dani użytkownicy końcowi wyrazili zgodę na przetwarzanie treści ich łączności elektronicznej i usługa ta nie może być świadczona bez przetwarzania tej treści lub jeżeli wszyscy użytkownicy końcowi, których to dotyczy, wyrazili zgodę na przetwarzanie treści ich łączności elektronicznej dla jednego celu

dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Dz.U. L 337, s. 11, 18.12.2009).

lub dla kilku celów, które nie mogą być zrealizowane przez przetwarzanie informacji poddanych anonimizacji, natomiast dostawca skonsultował się z organem nadzorczym.

Dla celów rozporządzenia ePrivacy zgoda użytkownika końcowego – niezależnie od tego, czy jest on osobą fizyczną czy prawną – powinna mieć takie samo znaczenie i podlegać takim samym warunkom, jak zgoda osoby, której dane dotyczą. W rozporządzeniu ePrivacy podkreślono, że zgodę można wyrazić poprzez wykorzystanie właściwych ustawień technicznych oprogramowania umożliwiającego dostęp do Internetu. Również uzyskanie dostępu do informacji dotyczących zdjęcia w telefonie czy kontaktów będzie musiało być poprzedzone zgodą użytkownika urządzenia.

Zgoda na przetwarzanie danych zgodnie z rozporządzeniem ePrivacy powinna spełniać przesłanki określone w RODO, czyli zgoda ta musi być: dobrowolna, jednoznaczna oraz świadoma. Jednocześnie zgoda na przetwarzanie danych związanych z korzystaniem z Internetu lub komunikacją głosową nie będzie ważna, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego i swobodnego wyboru lub nie może odmówić bądź wycofać zgody bez szkody. Poza tym użytkownicy końcowi mają możliwość wycofania swojej zgody w dowolnej chwili, a dostawcy usług elektronicznych powinni przypominać użytkownikom o takiej możliwości co sześć miesięcy przez cały okres przetwarzania.

Idąc dalej, w obrocie elektronicznym rozporządzenie ePrivacy przewiduje zmiany dotyczące plików *cookies*, które służą do zapamiętywania preferencji i personalizowania stron internetowych w zakresie wyświetlanych treści. Osoby fizyczne korzystające z usług internetowych za pomocą identyfikatorów plików *cookies* można bowiem łatwo identyfikować poprzez pozostawiane tzw. ślady elektroniczne, które w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskanymi przez serwery, mogą być dalej wykorzystywane do tworzenia profili poszczególnych osób i ich identyfikacji²⁶. Przeglądarki powinny być wyposażone w dodatkowe ustawienia, które mają służyć pozyskiwaniu jednoznacznych zgód na wykorzystanie *cookies* w odniesieniu do skonkretyzowanego celu przetwarzania danych osobowych. Tylko w przypadku plików *cookies* niestanowiących zagrożenia dla prywatności użytkownika końcowego nie będzie potrzeby wyrażenia zgody. Zwolnione z uzyskania zgody użytkownika będą zatem pliki *cookies*, które mają ułatwiać użytkownikowi korzystanie ze strony, np. gdy zapamiętują zawartość koszyka, a także plików *cookies*, które służą do liczenia wejść użytkowników na daną stronę internetową²⁷.

²⁶ M. OLSZEWSKA, *Prawne zasady dotyczące plików cookies a ochrona danych osobowych użytkownika Internetu*, Internetowy Kwartalnik Antymonopolowy i Regulacyjny, 7(6)/2017, s. 42.

²⁷ Tamże, s. 46.

W art. 5 ust. 3 rozporządzenia ePrivacy uregulowano, że przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowanych w urządzeniu użytkownika jest dozwolone tylko pod warunkiem, że wyraził on na to zgodę; po otrzymaniu jasnych i pełnych informacji, między innymi o celach przetwarzania. Zgoda użytkownika może być jednocześnie udzielona w jakikolwiek sposób umożliwiający swobodne i świadome wyrażenie woli użytkownika, a zwłaszcza poprzez zaznaczenie okna wyboru podczas przeglądania witryny internetowej. Według rozporządzenia ePrivacy nie jest konieczne uzyskanie zgody w przypadku każdej operacji dotyczącej dostępu do lub przechowywania informacji na urządzeniu użytkownika, bowiem informacja i prawo do odmowy mogą być oferowane jednorazowo w odniesieniu do różnego rodzaju narzędzi instalowanych w urządzeniu użytkownika w czasie tego samego połączenia, jak również mogą obejmować wszelkie dalsze korzystanie z tych narzędzi w trakcie kolejnych połączeń²⁸. Jednakże zgoda nie może być wyprowadzana z faktu korzystania z usługi, bowiem zgoda musi mieć charakter wyraźny, a nie dorozumiany czy wyrażony *per facta concludentia*.

6. ZGODA NA PRZETWARZANIE DANYCH W *CLOUD COMPUTINGU*

Cloud computing to model świadczenia usług pozwalający na dostęp na żądanie, przez sieć, do dzielonej puli zasobów technologii informacyjnej (dalej: IT), jak również otrzymanie skalowalnych i elastycznych usług IT²⁹. Zasoby te mogą być zamawiane przez klientów i w odpowiedni sposób konfigurowane w zależności od potrzeb użytkowników oraz dostarczane na żądanie i udostępniane przy minimalnym zaangażowaniu odbiorcy usługi. Zatem *cloud computing* obejmuje przeniesienie danych oraz oprogramowania do serwerów zewnętrznych i zapewnienie użytkownikowi dostępu do nich, wraz z możliwością wprowadzania i zapisywania zmian z dowolnego komputera podłączonego do sieci Internet. Powyższe to kolokacja danych, która może mieć różny charakter. Dane osobowe, aby były dostępne są klonowane pomiędzy różnymi lokalizacjami, a prawie zawsze w ramach klastra czy macierzy. Dotyczy to też kopii zapasowych u samego usługodawcy, który może trzymać kopie danych klientów w innej serwerowni etc. Rozróżnia się chmury prywatne dostępne dla jednej organizacji oraz chmury publiczne dostępne przez łącza internetowe dla różnych

²⁸ Tamże, s. 50.

²⁹ E. DYBKA, D. FALKOWSKI, R. GAJDA i in., *Cloud computing w sektorze finansowym. Raport Forum Technologii Bankowych przy Związku Banków Polskich* s. 6, https://zbp.pl/getmedia/c6fc00fd-6f7e-4cd0-9965-e6f4d143377d/Raport_Cloud_computing_w_sektorze_finansowym_2013-_z_recenzjami (data dostępu: 24 czerwca 2019 r., godz.: 22:36).

użytkowników, a także chmury hybrydowe stanowiące połączenie chmury prywatnej i publicznej, gdzie część pracuje \ w środowisku organizacji a część w środowisku publicznym. W każdej chmurze mogą być gromadzone dane, a m.in. przedsiębiorcy masowo wykorzystują udostępnianą im przestrzeń w chmurze do przechowywania dokumentacji kadrowej zawierającej dane osobowe pracowników i kandydatów do pracy. Użytkownik chmury nie nabywa jednak określonego nośnika, na którym może przechowywać dane, czy też egzemplarza programu komputerowego – uzyskuje jedynie możliwość dostępu i wykorzystania rozproszonych zasobów. Z punktu widzenia ochrony danych osobowych, co do zasady, przetwarzanie w chmurze stanowi powierzenie przetwarzania danych osobowych innemu podmiotowi lub sieci podmiotów. Z drugiej strony dostawca chmury musi zapewnić odbiorcy chmury, który odpowiada za dane osobowe przetwarzane w chmurze, że przetwarzanie danych osobowych w chmurze nastąpi zgodnie z zasadami wiążącymi odbiorcę chmury. Przetwarzanie danych osobowych w chmurze będzie zgodne z prawem, o ile przestrzegane są odpowiednie przepisy dotyczące ochrony danych osobowych, gdyż nie istnieją odrębne regulacje prawne, dotyczące bezpośrednio zagadnienia *cloud computingu*. Dlatego w celu realizacji przetwarzania danych w chmurze musi zostać zawarta odpowiednia umowa o świadczenie usług w technologii *cloud computingu* umożliwiająca kontrolowanie baz danych osobowych i zakazująca nielegalnego przekazywania danych będąca umową o powierzenie przetwarzania danych osobowych z dostawcą usługi *cloud computingu*. Poza tym, dla przetwarzania danych osobowych również w ten sposób konieczne jest wyrażenie zgody, przez osobę, której dane dotyczą. Bez zgody podmiotu danych dostawca chmury, ani odbiorca usługi nie mają możliwości dokonywania jakiegokolwiek operacji z zakresu przetwarzania danych osobowych.

7. ZGODA NA PRZETWARZANIE DANYCH A POGLĄDY JUDYKATURY

Problematyka zgody na przetwarzanie danych osobowych znajduje swoje odzwierciedlenie również w orzecznictwie. W świetle orzecznictwa polskiego, jeszcze na mocy poprzednich przepisów Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych przyjmowano, że zgoda nie może być domniemana, dorozumiana czy abstrakcyjna, natomiast osoba ją wyrażająca musi rozumieć jej istotę, cel i skutki³⁰. Poza tym zgoda na przetwarzanie danych musi być wyraźna, zaś jej umieszczenie jako dodatkowego elementu innego zobowiązania niezawierającego informacji o celach i zakresie przetwarzania tych danych nie spełnia tego wymagania³¹. NSA w wyroku z 6 września 2011 r., I OSK 1476/10, OSP

³⁰ Wyrok NSA z 10 stycznia 2013 r., I OSK 2029/11.

³¹ Wyrok NSA z 4 kwietnia 2003 r., II SA 2135/02, Wokanda 2004/6/30.

2013/10/104, podkreśla również całkowitą swobodę udzielenia zgody, o czym świadczy możliwość jej odmowy bez poniesienia szkody³². Z drugiej strony, wyrażona na życzenie pracodawcy pisemna zgoda pracownika na pobranie i przetworzenie jego danych osobowych w tym zakresie narusza prawa pracownika i swobodę wyrażenia przez niego woli³³. W orzecznictwie polskim przyjmuje się również, że zgoda może być udzielona jedynie w formie oświadczenia, a nie poprzez wyraźne działanie potwierdzające, co ma miejsce w innych państwach europejskich.

W Niemczech problematyka skuteczności zgody była przedmiotem, cieszącej się zainteresowaniem mediów, sprawy rozpatrywanej przez sąd z powództwa Federacji Niemieckich Organizacji Konsumenckich (*Verbraucherzentrale Bundesverband*) przeciwko Facebookowi. Skarżący podnosił, że domyślne ustawienia prywatności przewidziane przez serwis nie zapewniają użytkownikom pełnej wiedzy na temat udostępniania ich danych, stąd też wyrażana przez nich zgoda nie jest w pełnym tego słowa znaczeniu świadoma.

Jednocześnie skoro zgoda podmiotu na przetwarzanie danych musi być świadoma, to dostawcy usług muszą przedstawić mu jasną i łatwą do zrozumienia informację o charakterze oraz zakresie celu przetwarzania danych.

Wątpliwości budzi kwestia, czy oświadczenie o zgodzie musi być ograniczone do jednego celu przetwarzania, a poglądy w tej materii są zróżnicowane. W doktrynie niemieckiej zaprezentowane zostało stanowisko, że oświadczenie o zgodzie nie musi być ograniczone do jednego celu przetwarzania, co wynika ze sformułowania art. 6 ust. 1 lit. a RODO, zgoda obejmuje przetwarzanie danych osobowych w jednym lub większej liczbie określonych celów. Przyjmowano dotychczas, że dla każdego z oddzielnych celów przetwarzania konieczne jest odebranie osobnej zgody, przez co spełniona zostaje przesłanka konkretności zgody³⁴. Zapewne w tej kwestii konieczne będzie z czasem wydanie przez Trybunał Sprawiedliwości Unii Europejskiej (TSUE) rozstrzygnięcia, które zapewni prawidłową wykładnię przepisu.

Z orzecznictwa TSUE wynika natomiast obowiązek poszanowania życia prywatnego w kontekście przetwarzania danych osobowych, które stanowi prawo podstawowe każdego człowieka i odnosi się do wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej³⁵. Danymi osobowymi są m.in. imię, nazwisko, data

³² Wyrok NSA z 6 września 2011 r., I OSK 1476/10, OSP 2013/10/104.

³³ Wyrok NSA z 6 września 2011 r., I OSK 1476/10, LEX nr 965912,

³⁴ *RODO. Ogólne rozporządzenie...*, *op. cit.*, s. 355.

³⁵ Wyrok TSUE z 9 listopada 2010 r. w sprawach połączonych C-92/09 i C-93/09 V. i M. Schecke, H. Eifert przeciwko Land Hessen, Zb. Orz. 2010, s. I-11063, pkt 52.

i miejsce urodzenia, narodowość, stan cywilny, płeć, historia wjazdów na terytorium państwa, historia opuszczania tego terytorium, status pobytu, szczegóły dotyczące kolejnych paszportów, historia wpisów meldunkowych, oznaczenie urzędów i służb, które dane przekazały³⁶, a także dane dotyczące dochodu z tytułu działalności zarobkowej, czy z kapitału lub dane dotyczące majątków osób fizycznych³⁷. TSUE uznał również za przetwarzanie danych gromadzenie ich w oparciu o dokumenty urzędowe, a także opublikowanie ich w formie obszernej listy, czy udostępnianie ich na potrzeby wykorzystania do celów komercyjnych.

Według TSUE ustanowiony został zamknięty i wyczerpujący wykaz podstaw, dla legalnego przetwarzania danych osobowych, dlatego też państwa członkowskie nie mogą dodawać nowych kryteriów legalności przetwarzania danych osobowych ani też ustanawiać dodatkowych wymogów, które prowadziłyby do modyfikacji tychże podstaw³⁸. Ponadto prawo do ochrony danych osobowych nie jest jednak prawem absolutnym i powinno być analizowane w kontekście funkcji, jaką pełni w społeczeństwie³⁹. Ta ostatnia teza umożliwi zwolnienie niektórych rodzajów plików *cookies* z konieczności uzyskania świadomej zgody użytkownika Internetu, ponieważ w przeciwnym razie korzystanie przez użytkowników z wielu usług w Internecie byłoby wobec wymogu uzyskania zgody utrudnione czy wręcz niemożliwe.

8. ZAKOŃCZENIE

Ochrona danych osobowych wywodzi się z prawa do prywatności, stanowiącego prawo podstawowe każdego człowieka. Od tego czasu zakres przetwarzania danych osobowych, charakter zbieranych danych czy sposób ich przetwarzania – w wyniku postępu technologicznego i globalizacji – uległy radykalnej zmianie. Nowe technologie umożliwiają, bowiem przetwarzanie danych osobowych na niespotykaną wcześniej skalę. Osoby w zdecydowanie większym wymiarze udostępniają dane osobowe publicznie i globalnie, nierzadko nawet bez pełnej wiedzy i świadomości udzielenia zgody.

Nowe regulacje, tj. RODO i rozporządzenie ePrivacy, mają na celu zapewnienie osobom fizycznym kontroli nad własnymi danymi osobowymi. RODO przyjmuje bardziej restrykcyjne podejście do kwestii zgody. W świetle nowych regulacji prawnych redefinicji uległa zgoda na przetwarzanie danych osobowych jako kryterium legalizacyjne przetwarzania

³⁶ Wyrok TSUE z 16 grudnia 2008 r. w sprawie C-524/06 H. Huber przeciwko Bundesrepublik Deutschland, Zb. Orz. 2008, s. I-09705

³⁷ Wyrok TSUE z 16 grudnia 2008 r. w sprawie C-73/07 Tietosuojavaltuutettu przeciwko Satakun-nan Markkinapörssi Oy i Satamedia Oy, Zb. Orz. 2008, s. I-09831.

³⁸ Wyrok TS z 19 października 2016 r., C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, CURIA.

³⁹ Wyrok TS UE z 9.11.2010 w sprawach C-92/09 i 93/09, *op. cit.*

danych. Zgoda na przetwarzanie danych osobowych musi być dobrowolna, konkretna, świadoma i jednoznaczna, dokonana musi być w formie oświadczenia lub wyraźnego działania potwierdzającego, które przyzwala na przetwarzanie jej danych osobowych, a także musi być niekiedy wyraźna. Skuteczność zgody wyłączona została w sytuacji poważnej nierówności pomiędzy podmiotem danych a administratorem.

Należy zauważyć, że RODO przyjmuje odmienny charakter zgody jako przesłanki legalizacyjnej przetwarzania danych osobowych zwykłych oraz danych osobowych szczególnych kategorii. W przypadku danych szczególnych, podwyższono standard udzielenia zgody poprzez sformułowanie wymogu wyraźnej zgody na przetwarzania danych szczególnych. W rezultacie nie będzie wystarczające wówczas wyraźne działanie potwierdzające, ale niezbędne jest wyraźne oświadczenie zawierające taką zgodę⁴⁰. Administratorzy danych muszą pozyskiwać i ewidencjonować zgody w odpowiedni sposób, po to, by w przypadku skargi podmiotu danych, byli w stanie wykazać, że ta osoba rzeczywiście wyraziła zgodę na przetwarzanie swoich danych osobowych. Jeżeli administrator nie wykaże, że pozyskał zgodę na przetwarzanie danych zgodnie z prawem, w tym uzyskał skutecznie zgodę, to naraża się na karę administracyjną, a niekiedy również na odpowiedzialność odszkodowawczą wobec osoby, której dane były przetwarzane niezgodnie z prawem, a osoba ta poniosła szkodę. Poza tym problematyka zgody na przetwarzanie danych łączy się z niektórymi uprawnieniami podmiotów danych, jakimi są prawo do usunięcia danych czy prawo do przenoszenia danych. Jednocześnie niezmiernie istotną kwestią dla administratora danych jest właściwe skonstruowanie klauzuli wyrażającej zgodę na przetwarzanie danych. Chodzi o to, aby w sposób nie wywołujący wątpliwości klauzula określała: w jakim celu, zakresie, a także przez kogo dane osobowe będą przetwarzane, przy czym cele te muszą być prawidłowo określone. W przypadku oświadczenia woli dotyczącego różnych celów przetwarzania, zgoda taka powinna być wyrażona wyraźnie pod każdym z tych celów przetwarzania. Ponadto klauzula musi być odpowiednio wyodrębniona z pozostałej treści umowy bądź dokumentu.

Prawodawca unijny zwraca szczególną uwagę na możliwość wycofania zgody przez podmiot w każdym czasie, a wycofanie zgody musi być tak proste, jak jej złożenie. Wówczas administrator danych, jeżeli nie ma innej podstawy przetwarzania, np. niezbędność dla wykonania umowy, czy szczególna podstawa prawna, musi zaprzestać przetwarzania danych. Wskutek wycofania zgody, dane – wobec braku podstawy do przetwarzania – powinny zostać usunięte ze wszystkich systemów administratora.

⁴⁰ RODO. *Ogólne rozporządzenie...*, *op. cit.*, s. 242.

THE CRITERION OF LEGITIMACY OF CONSENT FOR PROCESSING PERSONAL DATA IN ELECTRONIC COMMERCE

The protection of personal data derives from the right to privacy. Since then, the scope of the processing of personal data, the nature of the data collected and the way in which they are processed have changed radically as a result of technological progress and globalisation. New technologies make it possible to process personal data on an unprecedented scale. The new regulations, i. e. the GDPR and the ePrivacy Regulation, aim to ensure that individuals have control over their personal data. The GDPR takes a more restrictive approach to consent. In the light of new legal regulations, the consent to the processing of personal data as a criterion for the legalization of data processing was redefined. Consent to the processing of personal data must be freely given, specific, informed and unambiguous, must be given in the form of a statement or a clear action which authorises the processing of personal data. Data controllers must obtain and keep records of consent in an appropriate manner so that, in case of a data subject's complaint, they can demonstrate that the data subject has actually consented to the processing of his or her personal data.

BIBLIOGRAFIA

BARTA J., FAJGIELSKI P., MARKIEWICZ R., *Ochrona danych osobowych. Komentarz*, Warszawa 2011.

DYBKA E., FALKOWSKI D., GAJDA R. i in., *Cloud computing w sektorze finansowym. Raport Forum Technologii Bankowych przy Związku Banków Polskich*, [https://zbp.pl/getmedia/c6fc00fd-6f7e-4cd0-9965e6f4d143377d/Raport Cloud computing w sektorze finansowym 2013- z recenzjami](https://zbp.pl/getmedia/c6fc00fd-6f7e-4cd0-9965e6f4d143377d/Raport%20Cloud%20computing%20w%20sektorze%20finansowym%202013-%20z%20recenzjami) (data dostępu: 24 czerwca 2019 r, godz. 22:36).

GIODO, *Gotowi na RODO*, https://uodo.gov.pl/data/filemanager_pl/641.pdf (data dostępu: 22 czerwca 2019, godz. 20:48.).

KACZMAREK-TEMPLIN B., *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia*, [w:] *Polska i europejska reforma ochrony danych osobowych*, red. E. BIELAK-JOMAA, D. LUBASZ, Warszawa 2016.

Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia, red. M. KAWECKI, T. OSIEJA, Warszawa 2017.

OLSZEWSKA M., *Prawne zasady dotyczące plików cookies a ochrona danych osobowych użytkownika Internetu*, Internetowy Kwartalnik Antymonopolowy i Regulacyjny, 7(6)/2017.

RODO. Ogólne rozporządzenie o ochronie danych, red. E. BIELAK-JOMAA, D. LUBASZ, Warszawa 2018.

SAGAN-JEŻOWSKA A., *Klauzule RODO. Wzory klauzul z praktycznym komentarzem*, Warszawa 2018.