01197/11/PL
WP187

Opinia 15/2011 w sprawie definicji zgody

Przyjęta w dniu 13 lipca 2011 r.

Streszczenie

W niniejszej opinii przedstawiono dokładną analizę pojęcia zgody wykorzystywanego obecnie w dyrektywie o ochronie danych oraz w dyrektywie o prywatności i łączności elektronicznej. Opierając się na doświadczeniu członków Grupy Roboczej Art. 29, w opinii podano liczne przykłady zgody ważnej i nieważnej, skupiając się na najistotniejszych aspektach zgody, takich jak znaczenie terminów „wskazanie", „dobrowolny", „konkretny", „jednoznaczny", „wyraźny", „świadomy" itp. W opinii zamieszczono ponadto wyjaśnienia dotyczące pewnych kwestii związanych z pojęciem zgody, na przykład momentu, w którym należy uzyskać zgodę, różnicy między prawem sprzeciwu a zgodą itp.

Zgoda jest jedną z kilku podstaw prawnych przetwarzania danych osobowych. Odgrywa ona ważną rolę, co nie wyklucza jednak możliwości – w zależności od kontekstu – zaistnienia bardziej odpowiednich podstaw prawnych z punktu widzenia zarówno administratora danych, jak i osoby, której dane dotyczą. Właściwie wykorzystywana zgoda stanowi narzędzie umożliwiające osobie, której dane dotyczą, kontrolę nad ich przetwarzaniem. W przypadku jej niewłaściwego wykorzystania kontrola ze strony osoby, której dane dotyczą, staje się złudna, a sama zgoda stanowi nieodpowiednią podstawę przetwarzania.

Niniejszą opinię wydaje się częściowo w odpowiedzi na wniosek Komisji w kontekście trwającego przeglądu dyrektywy o ochronie danych. W związku z tym zawiera ona zalecenia, które należy uwzględnić podczas przeglądu. Zalecenia te obejmują:

i) wyjaśnienie znaczenia „jednoznacznej" zgody i wskazanie, że ważna jest wyłącznie zgoda oparta na oświadczeniach lub działaniach wyrażających przyzwolenie;

ii) wymaganie od administratorów danych, aby wdrożyli mechanizmy umożliwiające wykazanie zgody (w ramach ogólnego obowiązku rozliczalności);

iii) wprowadzenie wyraźnego wymogu dotyczącego jakości i dostępności informacji stanowiących podstawę zgody; oraz

iv) pewną liczbę sugestii dotyczących małoletnich i innych osób nieposiadających pełnej zdolności do czynności prawnych.

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 oraz art. 30 ust. 1 lit. a) i ust. 3 wspomnianej dyrektywy,

uwzględniając swój regulamin,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. Wprowadzenie

Zgoda osoby, której dane dotyczą, stanowi od zawsze podstawowe pojęcie w dziedzinie ochrony danych, nie zawsze jest jednak jasne, kiedy niezbędna jest zgoda, i jakie warunki trzeba spełnić, aby zgoda była ważna. Może to prowadzić do różnic w podejściu i rozbieżnych poglądów na to, co jest dobrą praktyką, w poszczególnych państwach członkowskich. To z kolei może pogarszać sytuację osób, których dane dotyczą. Problem ten staje się coraz poważniejszy, gdyż przetwarzanie danych osobowych zarówno w środowisku *on-line*, jak i *off-line*, często odbywające się na terytorium różnych państw członkowskich, jest coraz istotniejszym elementem funkcjonowania nowoczesnego społeczeństwa. Dlatego też Grupa Robocza Art. 29 postanowiła gruntownie zbadać ten temat w ramach swojego programu prac na lata 2010–2011.

Ponadto zgoda jest jednym z zagadnień, o informacje na temat którego Komisja wnioskowała w kontekście przeglądu dyrektywy 95/46/WE. W komunikacie Komisji „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”[1] stwierdza się: „Komisja zbada możliwości wyjaśnienia i udoskonalenia przepisów dotyczących zgody”. W komunikacie zostało to wyjaśnione[2] w następujący sposób:

Zgodnie z obowiązującymi przepisami, jeżeli wymagane jest świadome wyrażenie zgody przez osobę fizyczną na przetwarzanie jej danych osobowych, zgoda ta powinna stanowić „konkretne i świadome, dobrowolne wskazanie” woli tej osoby, za pośrednictwem którego zgadza się ona na przetwarzanie tych danych. Jednakże poszczególne państwa członkowskie różnie interpretują te warunki, poczynając od ustanowienia ogólnego wymogu pisemnej zgody po akceptowanie zgody dorozumianej.

Ponadto w środowisku internetowym – ze względu na niejasne reguły dotyczące prywatności – osoby fizyczne mają większe trudności z uzyskaniem informacji o przysługujących im prawach oraz wyrażaniem świadomej zgody. Sytuację komplikuje

1 COM(2010)609 wersja ostateczna z dnia 4 listopada 2010 r.

2 Już w pierwszym sprawozdaniu Komisji na temat wykonania dyrektywy o ochronie danych (95/46/WE) (COM(2003)265 wersja ostateczna) wspomina się na stronie 17: „Zwłaszcza pojęcie »jednoznacznej zgody« (art. 7 lit. a)), w porównaniu z pojęciem »wyraźnej zgody«, o której mowa w art. 8, wymaga dalszych wyjaśnień i ujednolicenia interpretacji. Podmioty muszą wiedzieć, co stanowi ważną zgodę, w szczególności w środowisku internetowym”.

dodatkowo fakt, że w niektórych przypadkach nie jest nawet jasne, co stanowiłoby konkretną i świadomą, dobrowolną zgodę na przetwarzanie danych, tak jak w przypadku reklamy behawioralnej, kiedy to, według stanowiska niektórych podmiotów, użytkownik wyraża zgodę przez same ustawienia przeglądarki internetowej.

Dlatego należy wyjaśnić warunki uzyskania zgody osoby, której dane dotyczą, by zagwarantować, by zgoda była zawsze wyrażana świadomie oraz zapewnić, by osoba fizyczna była zawsze w pełni świadoma wyrażania zgody oraz tego, jakiego przetwarzania danych ona dotyczy, zgodnie z art. 8 Karty praw podstawowych UE. Jasność w zakresie zasadniczych pojęć może również sprzyjać rozwojowi inicjatyw samoregulacyjnych służących opracowaniu praktycznych rozwiązań zgodnych z prawem UE.

Odpowiadając na wniosek Komisji o wniesienie wkładu oraz realizując swój program prac na lata 2010–2011, Grupa Robocza Art. 29 zobowiązała się sporządzić opinię. Celem opinii jest wyjaśnienie pewnych zagadnień, aby zapewnić jednolitą interpretację istniejących ram prawnych. Działania Grupy Roboczej wynikają zarazem z podobnych pobudek, jak w przypadku poprzednich opinii dotyczących innych kluczowych przepisów dyrektywy[3]. Potencjalne zmiany istniejących ram będą wymagać pewnego czasu, zatem wyjaśnienie obecnego pojęcia „zgody" i jego głównych elementów ma swoje zalety. Wyjaśnienie istniejących przepisów pomoże również wskazać obszary wymagające poprawy. Tak więc, w oparciu o dokonaną analizę, w opinii podjęta zostanie próba sformułowania zaleceń dotyczących polityki, aby pomóc Komisji i decydentom w rozważeniu zmian obowiązujących ram prawnych ochrony danych.

Niniejsza opinia składa się z następujących zasadniczych elementów: po ogólnym przedstawieniu historii prawodawstwa i roli zgody w prawodawstwie dotyczącym ochrony danych zbadano poszczególne elementy oraz wymagania warunkujące ważność zgody w świetle obowiązującego prawa, w tym stosowne przepisy dyrektywy 2002/58/WE o prywatności i łączności elektronicznej. Analizę zilustrowano praktycznymi przykładami opartymi na doświadczeniach krajowych. Leży ona u podstaw zaleceń zawartych w ostatniej części opinii, zgodnie z którymi w celu ubiegania się o ważną zgodę i uzyskania jej na mocy dyrektywy niezbędne są pewne elementy. Przedstawiono również zalecenia, które decydenci powinni wziąć pod rozwagę w kontekście przeglądu dyrektywy 95/46/WE.

II. Ogólne spostrzeżenia i zagadnienia dotyczące polityki

II.1. Rys historyczny

Chociaż w niektórych krajowych przepisach o ochronie danych i prywatności przyjętych w latach 70. XX wieku określano zgodę jako jedną z podstaw prawnych przetwarzania danych osobowych[4], nie znalazło to odzwierciedlenia w konwencji 108

[3] Na przykład Opinii 8/2010 o prawie właściwym przyjętej w dniu 16 grudnia 2010 r. (WP 179) oraz Opinii 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" przyjętej w dniu 16 lutego 2010 r. (WP 169).

[4] Zob. na przykład art. 31 francuskiego Loi n 78-17 z dnia 6 stycznia 1978 r. „relative a l'informatique, aux fichiers et aux libertés".

Rady Europy[5]. Trudno wskazać powody, dla których zgoda nie odgrywa większej roli w tej konwencji[6].

Na szczeblu UE zgodę planowano wykorzystać jako kryterium legalności czynności przetwarzania danych osobowych od samego początku procesu legislacyjnego, którego ostatecznym wynikiem było przyjęcie dyrektywy 95/46/WE. W art. 12 wniosku Komisji[7] z 1990 r. określono cechy zgody niezbędne, aby zapewnić legalność czynności przetwarzania danych: musiała ona być „wyraźnie udzielona" i „konkretna". W art. 17 dotyczącym danych szczególnie chronionych znalazł się wymóg, aby zgoda była „wyraźna i pisemna". W zmienionym wniosku Komisji[8] z 1992 r. wprowadzono sformułowanie bliskie definicji „zgody osoby, której dane dotyczą" w obowiązującym obecnie art. 2 lit. h), który zastąpił pierwotny art. 12. Stwierdzono tam, że zgoda musi być „dobrowolna i konkretna". Sformułowanie „wyraźnie udzielona" zastąpiono określeniem zgody jako „wyraźnego wskazania woli (osoby, której dane dotyczą)". W uzasadnieniu towarzyszącym zmienionemu wnioskowi[9] z 1992 r. stwierdzono, że zgoda może zostać udzielona ustnie lub pisemnie. W przypadku danych szczególnie chronionych zachowano wymóg zgody „pisemnej". W zmienionym wniosku Komisji z 1992 r. przeformułowano treść poprzedniego wniosku, wprowadzając art. 7 dotyczący podstaw prawnych przetwarzania. W art. 7 lit. a) stwierdzono, że przetwarzanie może być prowadzone, gdy „osoba, której dane dotyczą, wyraziła na to zgodę"; pierwotna lista obejmowała, podobnie jak obecnie, pięć dodatkowych podstaw prawnych (oprócz zgody), które można wykorzystać w celu legalnego przetwarzania danych.

We wspólnym stanowisku Rady[10] z 1995 r. wprowadzono ostateczną (obecnie obowiązującą) definicję zgody. Określono ją jako „konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych". Główna zmiana w stosunku do stanowiska Komisji z 1992 r. polegała na usunięciu słowa „wyraźne" poprzedzającego słowo „wskazanie". W art. 7 lit. a) dodano zarazem słowo „jednoznacznie", zatem brzmi on następująco: „gdy osoba, której dane dotyczą, jednoznacznie wyraziła na to zgodę". Wymóg pisemnej zgody w przypadku danych szczególnie chronionych zastąpiono „wyraźną zgodą".

W uzasadnieniu Rady[11] nie podano konkretnych wyjaśnień wprowadzonych zmian. Na stronie 4 stwierdzono jednak: „[…] wprowadzono […] pewne zmiany w celu […] uzyskania pewnej elastyczności, która gwarantuje równoważną ochronę […] ale nie

---

5 Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (zwana „konwencją 108"). Weszła ona w życie w dniu 1 października 1985 r.

6 W konwencji 108 wprowadzono pojęcia „zgodnego z prawem przetwarzania" i „usprawiedliwionego celu" (art. 5), ale w przeciwieństwie do dyrektywy 95/46/WE nie przedstawiono wykazu kryteriów legalności przetwarzania danych. Zgoda osoby, której dane dotyczą, odgrywała rolę jedynie w kontekście wzajemnej pomocy (art. 15). O wymogu uzyskania „zgody" wspominano jednak później wielokrotnie w różnych zaleceniach Komitetu Ministrów.

7 Wniosek dotyczący dyrektywy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych, COM(90)314 wersja ostateczna, SYN 287 i 288, Bruksela, 13 września 1990 r.

8 Zmieniony wniosek dotyczący dyrektywy Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, COM(92)422 wersja ostateczna – SYN 287, Bruksela, 15 października 1992 r.

9 Zob. s. 11 zmienionego wniosku dotyczącego dyrektywy Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, COM(92)422 wersja ostateczna – SYN 287, Bruksela, 15 października 1992 r.

10 Wspólne stanowisko Rady w sprawie wniosku dotyczącego dyrektywy Parlamentu i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, (00/287) COD, przyjęte 15 marca 1995 r.

11 Zob. s. 4 wspólnego stanowiska.

skutkuje obniżeniem poziomu ochrony; umożliwiają one efektywne i pozbawione biurokratycznych obciążeń stosowanie ogólnych zasad, uwzględniając znaczną różnorodność sposobów […] przetwarzania danych".

Rolę zgody wyraźnie uznano w Karcie praw podstawowych Unii Europejskiej w części dotyczącej ochrony danych osobowych. W art. 8 ust. 2 stwierdza się, że dane osobowe można przetwarzać „za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą". Tak więc zgodę uznaje się za zasadniczy aspekt podstawowego prawa do ochrony danych osobowych. Jednocześnie zgodnie z kartą zgoda nie stanowi jedynej podstawy prawnej umożliwiającej przetwarzanie danych osobowych; w karcie wyraźnie uznano, że w prawie można określić inne uzasadnione podstawy, co uczyniono w dyrektywie 95/46/WE.

Podsumowując, historia prawodawstwa, w szczególności unijnego, wskazuje, że zgoda odgrywa ważną rolę w koncepcjach ochrony danych oraz prywatności. Równocześnie widać, iż nie jest ona uznawana za jedyną podstawę prawną legalności czynności przetwarzania danych. Historia powstawania dyrektywy 95/46/WE dowodzi względnego konsensusu co do warunków ważnej zgody – musi ona mianowicie być dobrowolna, konkretna i świadoma. Wskazuje też jednak na niepewność co do możliwych sposobów wyrażenia zgody – czy musi być ona wyraźna, pisemna itp. Poniżej przedstawiono dalszą analizę tych zagadnień.

II.2. Rola pojęcia: podstawa legalności

Podstawa ogólna/szczególna

Zgoda jest traktowana w dyrektywie zarówno jako ogólna podstawa legalności (art. 7), jak i jako podstawa szczególna w konkretnych przypadkach (art. 8 ust. 2 lit. a), art. 26 ust. 1 lit. a)). W art. 7 zgodę wymienia się jako pierwszą z sześciu podstaw legalności przetwarzania danych osobowych, natomiast w art. 8 dopuszcza się możliwość wykorzystania zgody jako podstawy legalności przetwarzania szczególnych kategorii (szczególnie chronionych) danych, które w przeciwnym wypadku byłoby zabronione. W ostatnim przypadku stawia się wyższe wymagania co do uzyskiwanej zgody, gdyż musi ona wyjść poza ogólną normę ustanowioną dla zgody, a mianowicie być zgodą „wyraźną".

Ponadto w dyrektywie dopuszcza się wzajemne oddziaływanie z innymi przepisami, o czym mowa jest w motywie 23: „Państwa Członkowskie są upoważnione do zapewnienia ochrony osobom fizycznym zarówno poprzez ogólne przepisy prawa o ochronie jednostek w odniesieniu do przetwarzania danych osobowych oraz poprzez ustawodawstwo sektorowe". Funkcjonowanie tego systemu w praktyce jest złożone: państwa członkowskie przyjęły odmienne podejścia, co w pewnych przypadkach doprowadziło do rozbieżności.

Na szczeblu krajowym pojęcie zgody nie zawsze jest transponowane dosłownie. Na przykład zgoda jako pojęcie ogólne nie jest zdefiniowana we francuskim ustawodawstwie o ochronie danych, ale jej znaczenie zostało precyzyjnie i spójnie wyjaśnione w orzecznictwie organu ochrony danych (CNIL) w nawiązaniu do definicji zawartej w dyrektywie o ochronie danych. W Zjednoczonym Królestwie pojęcie to

zostało wypracowane w prawie zwyczajowym w nawiązaniu do brzmienia przepisów dyrektywy. Dodatkowo zgodę definiuje się czasem wyraźnie w konkretnych sektorach, na przykład w kontekście prywatności w łączności elektronicznej, administracji elektronicznej czy e-zdrowia. W związku z tym pojęcia wypracowane w przepisach szczególnych i w ogólnym prawodawstwie o ochronie danych wzajemnie na siebie oddziałują.

Zgoda jest również pojęciem stosowanym w innych dziedzinach prawa, zwłaszcza w prawie zobowiązań. W tym kontekście ważność umowy jest analizowana z punktu widzenia kryteriów innych niż wymienione w dyrektywie, takich jak wiek, bezprawny nacisk itp. Prawo cywilne i dyrektywa nie są ze sobą w sprzeczności, lecz zakresy ich zastosowań pokrywają się: dyrektywa nie odnosi się do ogólnych warunków ważności zgody w kontekście prawa cywilnego, nie wykluczając ich zarazem. Oznacza to na przykład, że w celu oceny ważności umowy w kontekście art. 7 lit. b) dyrektywy trzeba wziąć pod uwagę wymagania prawa cywilnego. Poza zastosowaniem ogólnych warunków ważności zgody określonych w prawie cywilnym zgoda wymagana w art. 7 lit. a) musi również być interpretowana z uwzględnieniem art. 2 lit. h) dyrektywy.

To wzajemne oddziaływanie z pozostałym prawodawstwem jest widoczne nie tylko na szczeblu krajowym, ale także europejskim. Podobną interpretację elementów dyrektywy stosuje się również w innych kontekstach, czego dowodzi wyrok Trybunału Sprawiedliwości w dziedzinie prawa pracy[12]: w kontekście rezygnacji z prawa socjalnego wymagana była zgoda. Trybunał zinterpretował pojęcie zgody w kontekście dyrektywy 93/104 dotyczącej niektórych aspektów organizacji czasu pracy. Stwierdził on, że „zgoda pracownika" wymaga zgody samego pracownika (a nie zgody związku w imieniu pracownika), uznając, iż „zgoda" oznacza dobrowolną i świadomą zgodę. Trybunał uznał też, że sytuacja, w której pracownik podpisuje umowę o pracę odnoszącą się do układu zbiorowego zezwalającego na przekroczenie czasu pracy, nie spełnia wymogów, aby zgoda była wyrażona dobrowolnie i wyraźnie, przy pełnej znajomości wszystkich faktów. Ta interpretacja zgody w konkretnym kontekście jest bardzo zbliżona do brzmienia dyrektywy 95/46/WE.

Zgoda nie jest jedyną podstawą legalności

W dyrektywie jednoznacznie przedstawiono zgodę jako jedną z podstaw legalności. Niektóre państwa członkowskie traktują ją wszakże jako preferowaną podstawę, bliską czasem zasadzie konstytucyjnej związanej z faktem, że ochrona danych jest prawem podstawowym. Inne państwa członkowskie mogą z kolei postrzegać ją jako jedną z sześciu możliwości, w charakterze wymogu operacyjnego, który nie ma pierwszeństwa przed innymi opcjami. Wyjaśnienie relacji między zgodą a innymi podstawami legalności – np. w odniesieniu do umów, zadań wykonywanych w interesie publicznym czy uzasadnionych interesów administratora danych oraz prawa sprzeciwu – pomoże uwydatnić rolę zgody w konkretnych przypadkach.

Kolejność, w jakiej wymieniono podstawy prawne w art. 7, jest istotna, ale nie oznacza, że zgoda jest zawsze najbardziej odpowiednią podstawą legalności przetwarzania danych osobowych. W art. 7 wymienia się najpierw zgodę, wskazując następnie inne

[12] Wyrok Trybunału (wielka izba) z dnia 5 października 2004 r., Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller, Döbele w sprawach połączonych C-397/01 do C-403/01.

podstawy, w tym umowy i zobowiązania prawne, i stopniowo przechodząc do równowagi interesów. Należy zauważyć, że w przypadku pięciu pozostałych podstaw wymienionych po zgodzie niezbędne jest zastosowanie kryterium konieczności, które ściśle ogranicza okoliczności, w jakich mogą one mieć zastosowanie. Nie oznacza to, że wymóg zgody pozostawia większe pole manewru od pozostałych podstaw wymienionych w art. 7.

Ponadto uzyskanie zgody nie zwalnia administratora danych z obowiązków na mocy art. 6 związanych z rzetelnością, koniecznością i proporcjonalnością, jak też jakością danych. Na przykład nawet jeżeli użytkownik wyraził zgodę na przetwarzanie danych osobowych, nie czyni to legalnym gromadzenia danych nadmiernych w stosunku do określonego celu.

Uzyskanie zgody nie pozwala też ominąć innych przepisów, jak na przykład art. 8 ust. 5. Zgoda może być podstawą legalności czynności przetwarzania danych, które byłyby w przeciwnym razie zabronione, tylko w nielicznych okolicznościach, w szczególności w odniesieniu do przetwarzania niektórych danych szczególnie chronionych (art. 8) lub też w przypadku wykorzystania danych osobowych w celu dalszego przetwarzania niezależnie od tego, czy jest to zgodne z pierwotnym celem. Co do zasady, zgody nie powinno się uważać za zwolnienie z wymogu przestrzegania pozostałych zasad ochrony danych, ale za zabezpieczenie. Jest ona przede wszystkim podstawą legalności i nie uchyla zastosowania innych zasad.

Wybór najbardziej odpowiedniej podstawy prawnej nie zawsze jest oczywisty, szczególnie jeżeli chodzi o wybór między podstawami z art. 7 lit. a) i art. 7 lit. b). Zgodnie z art. 7 lit. b) przetwarzanie danych musi być konieczne dla realizacji umowy lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy, i nic ponadto. Administrator danych wykorzystujący art. 7 lit. b) jako podstawę prawną w kontekście zawarcia umowy nie może go rozszerzyć, by uzasadnić przetwarzanie danych wychodzące poza konieczny zakres; na dodatkowe przetwarzanie musi on uzyskać konkretną zgodę, której będą dotyczyć wymogi art. 7 lit. a). Dowodzi to potrzeby szczegółowego sformułowania warunków umowy. W praktyce oznacza to, że konieczne może być uzyskanie zgody jako dodatkowego warunku dotyczącego części czynności przetwarzania. Przetwarzanie musi być konieczne dla realizacji umowy, albo trzeba uzyskać (dobrowolną) zgodę.

W przypadku niektórych transakcji zastosowanie może mieć jednocześnie kilka podstaw prawnych. Innymi słowy, każda czynność przetwarzania danych musi zawsze pozostawać w zgodzie z jedną lub większą liczbą podstaw prawnych. Nie wyklucza to jednoczesnego wykorzystywania kilku podstaw pod warunkiem ich wykorzystania we właściwym kontekście. Niektóre czynności gromadzenia i dalszego przetwarzania danych mogą być niezbędne na mocy umowy z osobą, której dane dotyczą – art. 7 lit. b); przetwarzanie w innym zakresie może być konieczne w związku ze zobowiązaniem prawnym – art. 7 lit. c); gromadzenie dodatkowych informacji może wymagać odrębnej zgody – art. 7 lit. a); jeszcze inne czynności przetwarzania mogą być legalne w ramach równowagi interesów – art. 7 lit. f).

Przykład: kupno samochodu
Administrator danych może być uprawniony do przetwarzania danych osobowych w różnych celach i na różnych podstawach:
- danych niezbędnych w celu kupna samochodu – art. 7 lit. b);
- w celu przetwarzania dokumentów samochodu: art. 7 lit. c);
- w celu zarządzania klientami (np. aby zapewnić serwisowanie samochodu przez powiązane przedsiębiorstwa w UE): art. 7 lit. f);
- w celu przekazania danych osobom trzecim dla ich własnych działań marketingowych: art. 7 lit. a).

II.3. Pojęcia powiązane

Kontrola

Pojęcie zgody tradycyjnie wiąże się z ideą, że osoba, której dane dotyczą, powinna mieć kontrolę nad sposobem wykorzystywania jej danych. Kontrola sprawowana poprzez zgodę jest ważnym pojęciem z punktu widzenia praw podstawowych. Jednocześnie – i z tego samego punktu widzenia – decyzja osoby fizycznej o zgodzie na czynność przetwarzania danych powinna podlegać rygorystycznym wymogom, zwłaszcza biorąc pod uwagę fakt, że podejmując taką decyzję, osoba ta może zrzekać się prawa podstawowego.

Chociaż zgoda odgrywa pewną rolę w przekazaniu kontroli osobom, których dane dotyczą, nie jest ona jedynym sposobem osiągnięcia tego celu. W dyrektywie wskazano inne środki kontroli, w szczególności prawo sprzeciwu, ale jest ono odrębnym instrumentem wykorzystywanym na innym etapie przetwarzania, tj. po jego rozpoczęciu, i opiera się na innej podstawie prawnej.

Zgoda wiąże się z koncepcją informacyjnego samostanowienia. Autonomia osoby, której dane dotyczą, jest zarówno warunkiem wstępnym, jak i konsekwencją zgody: umożliwia ona tej osobie wywieranie wpływu na przetwarzanie danych. Jak wykazano jednak w następnym rozdziale, zasada ta ma pewne ograniczenia i istnieją przypadki, gdy osoba, której dane dotyczą, nie ma możliwości podjęcia rzeczywistej decyzji. Administrator danych może chcieć wykorzystać zgodę osoby, której dane dotyczą, aby przenieść swoją odpowiedzialność na osobę fizyczną. Osoba fizyczna może na przykład ponieść szkody, zgadzając się na publikację danych osobowych w Internecie lub na ich przekazanie podejrzanemu podmiotowi w państwie trzecim, a administrator danych może twierdzić, że osoba, której dane dotyczą, wyraziła na to zgodę. Dlatego też ważne jest, aby pamiętać, że w pełni ważna zgoda nie zwalnia administratora danych z jego obowiązków, ani też nie czyni legalnym przetwarzania, które byłoby w przeciwnym razie nierzetelne zgodnie z art. 6 dyrektywy.

Pojęcie kontroli wiąże się też z faktem, że osoba, której dane dotyczą, powinna mieć możliwość odwołania zgody. Odwołanie takie nie działa wstecz, ale powinno co do zasady zapobiegać dalszemu przetwarzaniu danych osoby fizycznej przez

administratora danych. Działanie tego mechanizmu w praktyce zostanie szerzej omówione poniżej (w Rozdziale III).

Przejrzystość

Drugi wymiar zgody dotyczy informacji: przejrzystości wobec osoby, której dane dotyczą. Przejrzystość jest warunkiem sprawowania kontroli i ważności zgody. Przejrzystość jako taka nie jest wystarczającą podstawą legalności przetwarzania danych osobowych, ale jest niezbędnym warunkiem zapewnienia ważności zgody.

Aby zgoda była ważna, musi być świadoma. Oznacza to, że w chwili zwracania się o zgodę trzeba przedstawić wszystkie niezbędne informacje i powinny one dotyczyć istotnych aspektów przetwarzania, za podstawę legalności którego ma posłużyć zgoda. Zazwyczaj chodzi tutaj o informacje określone w art. 10 dyrektywy, ale jest to też uzależnione od momentu zwracania się o zgodę, i od okoliczności, w jakich ma to miejsce.

Niezależnie od tego, czy zgoda zostanie udzielona, czy też nie, przejrzystość przetwarzania danych jest też warunkiem rzetelności, która pozostaje istotna także po przedstawieniu wstępnych informacji.

Działanie i czas: sposoby wyrażenia zgody

Trzeci wymiar odnosi się do sposobu sprawowania kontroli: w jaki sposób można wyrazić zgodę i kiedy należy się o nią zwrócić, aby zapewnić jej rzeczywisty charakter? Te pytania mają decydujący wpływ na sposób wyrażenia i interpretacji zgody.

Chociaż w dyrektywie nie określono momentu, w którym należy zwrócić się o zgodę, jasno wynika on z treści poszczególnych przepisów, które wskazują, że ogólną zasadą jest, iż zgoda musi zostać udzielona przed rozpoczęciem przetwarzania[13]. Uzyskanie zgody przed rozpoczęciem przetwarzania danych jest zasadniczym warunkiem legalności ich przetwarzania. Kwestię tę omówiono szerzej w Rozdziale III.B dotyczącym dyrektywy o prywatności i łączności elektronicznej.

Zgoda postrzegana jako upoważnienie ze strony osoby fizycznej do przetwarzania dotyczących jej danych może zostać wyrażona na różne sposoby: w art. 2 lit. h) jest mowa o „wskazaniu"; musi ona być jednoznaczna (art. 7 lit. a)) i wyraźna w odniesieniu do danych szczególnie chronionych (o których mowa w art. 8). Trzeba jednak podkreślić fakt, że zgoda różni się od prawa sprzeciwu określonego w art. 14. Podczas gdy na mocy art. 7 lit. a) administrator danych nie może przetwarzać danych, dopóki nie uzyska zgody osoby, której one dotyczą, na mocy art. 7 lit. f) administrator danych może przetwarzać dane po spełnieniu warunków i zapewnieniu zabezpieczeń, dopóki osoba, której one dotyczą, nie wyrazi sprzeciwu. Jak stwierdzono w dokumencie roboczym WP 114 Grupy Roboczej: „Wymóg udzielenia zgody wyklucza w zasadzie możliwość istnienia systemu, w którym podmiot danych miałby prawo sprzeciwić się przekazaniu danych dopiero po fakcie"[14].

[13] Na przykład w niemieckiej wersji dyrektywy (i w niemieckiej federalnej ustawie o ochronie danych) stosuje się termin „Einwilligung". W niemieckim kodeksie cywilnym definiuje się go jako „uprzednią zgodę".

[14] WP 114 – Dokument roboczy Grupy Roboczej Art. 29 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.

Z powyższych powodów prawa sprzeciwu, o którym mowa w art. 14 dyrektywy, nie należy mylić ze zgodą. Ta ostatnia jest podstawą prawną przetwarzania danych osobowych, o której mowa w art. 7 lit. a), art. 8 ust. 2 lit. a) i art. 26 ust. 1, jak również w pewnych przepisach dyrektywy 2002/58/WE.

II.4. Właściwe wykorzystanie zgody jako podstawy prawnej

Należy podkreślić, ze zgoda nie zawsze jest podstawowym lub najbardziej pożądanym środkiem zapewniającym legalność przetwarzania danych osobowych.

Zgoda bywa niewystarczającą podstawą uzasadniającą przetwarzanie danych osobowych i traci wartość, gdy usiłuje się rozszerzyć lub ograniczyć jej zakres, aby dopasować go do sytuacji, w których nigdy nie przewidywano jej wykorzystania. Decydujące jest wykorzystanie zgody „we właściwym kontekście". Jeżeli wykorzystuje się ją w okolicznościach, w których nie jest to właściwe, gdyż zazwyczaj nie towarzyszą im elementy składające się na ważną zgodę, prowadzi to do poważnych zagrożeń i w praktyce *osłabia* pozycję osób, których dane dotyczą.

Grupa Robocza i EIOD wyrazili już swoje poparcie dla takiego podejścia, wnosząc wkład do dyskusji na temat nowych ram ochrony danych. W szczególności stwierdza się: „Nie zawsze jednak jasne jest, co stanowi prawdziwą, jednoznaczną zgodę. Niektórzy administratorzy danych wykorzystują tę niejasność stosując metody nieodpowiednie do otrzymania prawdziwej, jednoznacznej zgody"[15], wbrew warunkom określonym w art. 6 dyrektywy. W tym samym duchu Grupa Robocza Art. 29 zauważa: „złożoność praktyk w zakresie gromadzenia danych, modeli biznesowych, relacji ze sprzedawcami i zastosowań technicznych przewyższa w wielu przypadkach zdolność lub gotowość osób fizycznych do podejmowania decyzji mających na celu kontrolę wykorzystania i przekazywania informacji w oparciu o aktywnie dokonywane wybory"[16].

Ważne jest zatem lepsze objaśnienie granic zgody i zagwarantowanie, że jako zgoda traktowana będzie jedynie zgoda interpretowana w sposób zgodny z prawem[17].

III. Analiza przepisów

Niniejsza analiza skupi się w Rozdziale III.A na dyrektywie 95/46/WE. W rozdziale III.B przeanalizowane zostaną pewne istotne przepisy dyrektywy 2002/58/WE o prywatności i łączności elektronicznej. Warto zaznaczyć, że dyrektywy te nie wyłączają się wzajemnie. Ogólne warunki ważności zgody określone w dyrektywie 95/46/WE mają zastosowanie zarówno w środowisku *off-line*, jak i *on-line*. W dyrektywie 2002/58/WE określono te warunki dla pewnych konkretnych usług internetowych,

[15] Opinia Europejskiego Inspektora Ochrony Danych z dnia 14 stycznia 2011 r. dotycząca komunikatu Komisji „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej".

[16] „Przyszłość prywatności. Wspólny wkład w konsultacje Komisji Europejskiej w sprawie ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych" (*The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*), 1 grudnia 2009 r., WP 168.

[17] Opinia Europejskiego Inspektora Ochrony Danych z dnia 14 stycznia 2011 r., *op. cit.*

zawsze w kontekście ogólnych warunków wskazanych w dyrektywie o ochronie danych.

III.A. Dyrektywa 95/46/WE

Pojęcie „zgody osoby, której dane dotyczą" jest zdefiniowane w art. 2 lit. h), a następnie wykorzystywane w art. 7, 8 i 26. O roli zgody mowa jest również w motywach 30 oraz 45. Przepisy te i wszystkie istotne szczegóły zostaną omówione odrębnie, jak również w niniejszym rozdziale.

III.A.1. Artykuł 2 lit. h)

Zgodnie z art. 2 lit. h) „zgoda osoby, której dane dotyczą" oznacza „konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych". Definicja ta zawiera pewne kluczowe elementy, które zostaną omówione poniżej.

„[…] wskazanie […] na to, że wyraża […]"

Co do zasady nie ma ograniczeń co do formy, jaką może przyjąć zgoda. Aby jednak była ona ważna, zgodnie z dyrektywą powinna być wskazaniem. Nawet jeżeli może być to dowolna forma wskazania, należy jasno określić, co dokładnie mieści się w definicji wskazania.

Dyrektywa nie określa formy wskazania (tj. sposobu wyrażenia woli). Dla zachowania elastyczności w ostatecznym tekście nie zamieszczono sformułowania o zgodzie „pisemnej". Należy podkreślić, że w dyrektywie mowa jest o „dowolnym" wskazaniu woli (ang. *any indication of a wish*). Pozwala to szeroko rozumieć zakres takiego wskazania. Minimalne wymagania wobec wyrażenia wskazania spełnia dowolny rodzaj sygnału wystarczająco jasnego, aby mógł on wskazywać wolę osoby, której dane dotyczą, oraz aby był zrozumiały dla administratora danych. Słowa „wskazanie" oraz „wyraża" przemawiają za tym, że niezbędne jest w istocie działanie (w przeciwieństwie do sytuacji, w której zgodę można byłoby wywnioskować z braku działania).

Pojęcie zgody powinno obejmować dowolne wskazanie woli, za pośrednictwem którego osoba, której dane dotyczą, *wyraża* swoje przyzwolenie: może to być odręczny podpis złożony na dole formularza papierowego, ale też ustne oświadczenia wyrażające przyzwolenie lub zachowanie, z którego można w uzasadniony sposób wnioskować o zgodzie. W związku z tym w zakres tej definicji mogłoby wchodzić, poza klasycznym przykładem podpisu, włożenie wizytówki do szklanego naczynia. To samo dotyczy sytuacji, w której osoba fizyczna przesyła organizacji swoje nazwisko i adres w celu uzyskania od niej informacji. W tym przypadku jej działanie należy rozumieć jako zgodę na przetwarzanie tych danych w zakresie niezbędnym do rozpatrzenia wniosku i udzielenia odpowiedzi.

W swojej opinii w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną (WP 115) Grupa Robocza zbadała, w jaki sposób należy umożliwić osobom fizycznym wyrażenie zgody na usługi wymagające automatycznego określenia ich lokalizacji (np. możliwość połączenia z określonym numerem telefonu w celu uzyskania informacji o warunkach pogodowych

w miejscu, w którym się znajdują). W tym przypadku uznano, że pod warunkiem dostarczenia użytkownikom z wyprzedzeniem pełnych informacji na temat przetwarzania danych o ich lokalizacji, zainicjowanie połączenia z określonym numerem telefonu jest równoznaczne z wyrażeniem zgody na określenie lokalizacji.

Przykład: tablice reklamowe w systemie Bluetooth
Obserwujemy rozwój nowej formy reklamy polegającej na tym, że tablice wysyłają wiadomości z prośbą o ustanowienie połączenia Bluetooth, aby wysyłać reklamy przechodniom. Wiadomości te są wysyłane do osób, które uaktywniły funkcję Bluetooth w swoim telefonie komórkowym. Sama aktywacja funkcji Bluetooth nie stanowi ważnej zgody (funkcję Bluetooth można uaktywnić w innych celach). Z drugiej strony, gdy osoba poinformowana o tej usłudze zbliża się z telefonem komórkowym do tablicy na odległość kilku centymetrów, jest to zazwyczaj wskazanie woli: pokazuje to, które osoby są naprawdę zainteresowane otrzymywaniem reklam. Tylko takie osoby powinno się uważać za te, które wyraziły zgodę, i tylko one powinny otrzymać wiadomości.

Wątpliwe jest, czy brak jakiegokolwiek zachowania (czy też raczej: zachowanie bierne) można także interpretować jako wskazanie w ściśle określonych okolicznościach (tj. w całkowicie jednoznacznym kontekście). Pojęcie „wskazania" jest szerokie, ale wydaje się oznaczać potrzebę działania. Interpretację tę potwierdzają pozostałe elementy definicji zgody oraz dodatkowy wymóg art. 7 lit. a), aby zgoda była jednoznaczna. Wymaganie, aby osoba, której dane dotyczą, „wyraziła" zgodę, wydaje się wskazywać, że bezczynność nie wystarcza, a zgoda wymaga jakiegoś działania, choć możliwe są różne rodzaje działań, o których ocenie decyduje „kontekst".

W praktyce przy braku aktywności osoby, której dane dotyczą, administrator danych będzie miał problem z weryfikacją, czy milczenie miało w zamierzeniu oznaczać akceptację lub zgodę. Administrator danych może na przykład nie mieć pewności niezbędnej, by założyć zgodę, w następującym przypadku: wyobraźmy sobie sytuację, gdy po wysłaniu do klientów listu informującego o zamierzonym przekazaniu ich danych, jeżeli nie wyrażą sprzeciwu w ciągu dwóch tygodni, odpowie tylko 10% adresatów. W tym przykładzie dyskusyjne jest, czy 90% osób, nie odpowiadając, rzeczywiście zgodziło się na przekazanie ich danych. W takich przypadkach administrator danych nie posiada jasnego wskazania co do intencji osób, których dane dotyczą. Nie będzie ponadto miał dowodów, w związku z czym nie będzie w stanie wykazać, że uzyskał zgodę. W praktyce niejednoznaczność biernej odpowiedzi uczyni spełnienie wymagań dyrektywy trudnym.

„[…] dobrowolne […]"

Zgoda może być ważna tylko jeżeli osoba, której dane dotyczą, ma możliwość dokonania rzeczywistego wyboru, przy czym nie zachodzi ryzyko wprowadzenia w błąd, zastraszenia, przymusu lub znaczących negatywnych konsekwencji, jeśli nie wyrazi zgody. Jeżeli konsekwencje wyrażenia zgody nie dają się pogodzić ze swobodą wyboru, zgoda nie jest dobrowolna. W art. 8 ust. 2 lit. a) samej dyrektywy stwierdza się, że w pewnych przypadkach określonych przez państwa członkowskie zakaz przetwarzania szczególnych kategorii danych osobowych nie może być uchylony przez zgodę osoby, której dane dotyczą.

Przykładem powyższego jest przypadek, gdy administrator danych wywiera wpływ na osobę, której dane dotyczą, na przykład ze względu na stosunek pracy. W tym przykładzie, choć niekoniecznie w każdym przypadku, osoba, której dane dotyczą, może być w sytuacji zależności od administratora danych ze względu na charakter relacji lub szczególne okoliczności – i może obawiać się odmiennego traktowania, jeżeli nie wyrazi zgody na przetwarzanie danych.

Grupa Robocza przeanalizowała w kilku opiniach zagadnienie granic zgody w sytuacjach, gdzie nie może ona być dobrowolna. Dotyczyło to w szczególności opinii w sprawie elektronicznej dokumentacji zdrowotnej (WP 131), przetwarzania danych w kontekście zatrudnienia (WP 48) oraz przetwarzania danych przez Światową Agencję Antydopingową (WP 162).

W dokumencie WP 131 Grupa Robocza stwierdziła: „»dobrowolna« zgoda oznacza decyzję podjętą z własnej inicjatywy przez osobę będącą w pełni władz umysłowych, bez jakiegokolwiek przymusu o charakterze społecznym, finansowym, psychologicznym lub innym. Każda zgoda udzielona pod wpływem groźby odmowy lub obniżenia jakości leczenia nie może być uznana za »dobrowolną« […] [W] przypadku gdy przetwarzanie danych osobowych w systemie EHR przez pracowników medycznych jest koniecznym i niemożliwym do uniknięcia skutkiem zaistniałej sytuacji medycznej, niewłaściwe jest poszukiwanie uzasadnienia w zgodzie osoby. Zależność od uzyskania zgody powinna być ograniczona do przypadków, w których osoba, której dotyczą dane, może dokonać rzeczywistego, wolnego wyboru, przez co rozumie się również możliwość cofnięcia zgody bez żadnego uszczerbku”[18].

Jeżeli po odwołaniu zgody przetwarzanie danych trwa nadal w oparciu o inną podstawę prawną, można podnosić wątpliwości co do pierwotnego wykorzystania zgody jako pierwszej podstawy prawnej: jeśli przetwarzanie mogło od początku mieć miejsce w oparciu o tę inną podstawę, stawianie osoby fizycznej w sytuacji, w której jest ona proszona o zgodę na przetwarzanie, może być uznane za postępowanie wprowadzające w błąd lub z natury nierzetelne. Sytuacja przedstawiałaby się inaczej, gdyby zmieniły się okoliczności – na przykład w trakcie przetwarzania pojawiłaby się nowa podstawa prawna, taka jak nowa ustawa regulująca działanie przedmiotowej bazy danych. Jeżeli te nowe podstawy mogą mieć zastosowanie do przetwarzania danych, może ono trwać nadal. W praktyce jednak takie okoliczności nie występują często. Co do zasady zgodę można uznać za niedostateczną, jeżeli nie jest dozwolone skuteczne jej odwołanie.

Grupa Robocza zajęła konsekwentne stanowisko w sprawie interpretacji dobrowolnej zgody w kontekście zatrudnienia[19]: „w przypadku, gdy od pracownika wymagana jest zgoda, a z jej nieudzieleniem wiąże się rzeczywista lub potencjalna istotna szkoda, zgoda ta nie jest ważna z punktu widzenia warunków art. 7 lub art. 8, gdyż nie jest ona dobrowolna. Jeżeli pracownik nie ma możliwości odmowy, nie jest to zgoda. […] Trudności pojawiają się w przypadku, gdy wyrażenie zgody jest warunkiem

[18] W dokumencie WP 162 dotyczącym Światowej Agencji Antydopingowej przedstawiono taki sam wniosek: „Sankcje i konsekwencje powiązane z ewentualną odmową podporządkowania się przez uczestników kodeksowym obowiązkom (na przykład informowanie o miejscu pobytu) przez uczestników sprawiają, że grupa robocza w żadnym stopniu nie uznaje takiej zgody za udzieloną dobrowolnie”.

[19] Dokument WP 48 w sprawie przetwarzania danych osobowych w kontekście zatrudnienia. Tematu tego dotyczy również WP114 – Dokument roboczy Grupy Roboczej Art. 29 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.

zatrudnienia. W teorii pracownik może odmówić udzielenia zgody, ale konsekwencją może być niezatrudnienie go. W takich okolicznościach zgoda nie jest dobrowolna, a zatem nie jest ważna. Sytuacja jest jeszcze bardziej jednoznaczna, gdy – co jest częste – wszyscy pracodawcy narzucają taki sam lub podobny warunek zatrudnienia".

Przykład: zdjęcia w intranecie
Zgoda w kontekście zatrudnienia może być ważna, co pokazuje następujący przykład: w przedsiębiorstwie postanowiono utworzyć intranet, w którym będą prezentowane nazwiska pracowników i ich podstawowe zadania. Każdy pracownik jest pytany, czy chce, by obok jego nazwiska wyświetlane było zdjęcie. Ci pracownicy, którzy chcą zamieszczenia swoich zdjęć, są proszeni o przesłanie zdjęcia na podany adres. Po uzyskaniu odpowiednich informacji działanie polegające na przesłaniu zdjęcia byłoby uważane za zgodę. Jeżeli przedsiębiorstwo posiada cyfrowe zdjęcia wszystkich pracowników i prosi każdego o zgodę na zamieszczenie zdjęcia w powyższych celach, każdy pracownik, który kliknie przycisk, wyrażając zgodę, również będzie uznany za osobę wyrażającą ważną zgodę. W obydwu przypadkach w pełni uszanowano prawo pracowników do wyboru, czy chcą, aby ich zdjęcia pojawiły się w intranecie.

Kontekst zatrudnienia wymaga szczegółowego omówienia: rolę odgrywają tutaj kulturowe i społeczne aspekty stosunku pracy, podobnie jak sposób, w jaki wzajemnie oddziałują na siebie zasady ochrony danych i pozostałe prawodawstwo. W kontekście zatrudnienia dane osobowe mogą być przetwarzane w różnych celach:

- dane niezbędne w celu wykonywania zadań przez pracownika: zastosowanie znajduje art. 7 lit. b) – konieczne dla umowy;
- w celu określenia uprawnień pracowników do nabycia opcji na akcje: na podstawie zgody (art. 7 lit. a)) lub w ramach uznania za nieodłączny aspekt administracyjny umownego stosunku pracy (art. 7 lit. b));
- przetwarzanie numeru ubezpieczenia społecznego do celów ubezpieczenia społecznego: zobowiązanie prawne (art. 7 lit. c)) lub też ewentualnie obowiązki w dziedzinie prawa pracy (art. 8 lit. b));
- przetwarzanie danych o pochodzeniu etnicznym: w niektórych krajach może to również stanowić obowiązek na mocy prawa pracy (art. 8 lit. b)), w innych natomiast jest surowo zabronione.

Choć może istnieć silne domniemanie, że w takich okolicznościach zgoda jest niewystarczająca, nie wyklucza to całkowicie jej wykorzystania pod warunkiem zagwarantowania w wystarczającym stopniu jej dobrowolności.

Chociaż stosunek podległości jest często główną przyczyną, dla której zgoda nie jest dobrowolna, na decyzję osoby, której dane dotyczą, mogą wpłynąć inne czynniki związane z kontekstem. Mogą one na przykład mieć wymiar finansowy, emocjonalny lub praktyczny. Na zachowanie osoby, której dane dotyczą, może też mieć pewien wpływ fakt, że są one gromadzone przez organ publiczny. Odróżnienie zwykłej zachęty od czynnika mającego realny wpływ na swobodę wyboru osoby, której dane dotyczą, może jednak być trudne. Poniższe przykłady służą ilustracji różnego charakteru wysiłków wymaganych od osób fizycznych lub ponoszonych przez nie kosztów, które mogą wpłynąć na ich decyzję.

Przykład – elektroniczna dokumentacja zdrowotna

W wielu państwach członkowskich podejmuje się kroki w kierunku stworzenia podsumowania dokumentacji zdrowotnej pacjentów w postaci elektronicznej. Pozwoli to świadczeniodawcom uzyskać dostęp do najważniejszych informacji niezależnie od miejsca, gdzie pacjent potrzebuje leczenia.

- W pierwszym scenariuszu utworzenie podsumowania jest w pełni dobrowolne, a pacjent będzie nadal leczony niezależnie od tego, czy wyraził zgodę na utworzenie podsumowania, czy też nie. W tym przypadku zgoda na utworzenie podsumowania jest dobrowolna, ponieważ pacjent nie znajdzie się w niekorzystnej sytuacji, jeżeli nie udzieli zgody lub jej odmówi.
- W drugim scenariuszu istnieje umiarkowana zachęta finansowa do wybrania elektronicznej dokumentacji zdrowotnej. Pacjenci odmawiający zgody na jej utworzenie nie znajdują się w niekorzystnej sytuacji w tym sensie, że koszty przez nich ponoszone nie ulegają zmianie. W tym przypadku też można uznać, że mają oni swobodę wyboru, czy wyrazić zgodę na nowy system, czy też nie.
- W trzecim scenariuszu pacjenci odmawiający zgody na przystąpienie do systemu e-zdrowia muszą ponieść znaczne dodatkowe koszty w porównaniu do poprzedniego systemu opłat, a przetwarzanie ich dokumentacji odbywa się z wyraźnym opóźnieniem. Oznacza to postawienie osób niewyrażających zgody w wyraźnie niekorzystnej sytuacji w celu objęcia wszystkich obywateli systemem e-zdrowia w zaplanowanym terminie. W związku z tym zgoda nie jest w wystarczającym stopniu dobrowolna. Dlatego też należy zbadać, czy istnieją inne uzasadnione podstawy przetwarzania danych osobowych, lub też rozważyć zastosowanie art. 8 ust. 3 dyrektywy 95/46/WE.

Przykład: urządzenia do prześwietlania osób

Urządzenia do prześwietlania osób są coraz powszechniej wykorzystywane w niektórych miejscach publicznych, w szczególności na lotniskach przed wejściem do strefy, w której oczekuje się na wejścia na pokład. Ze względu na fakt, że w chwili skanowania dane pasażerów są przetwarzane[20], przetwarzanie to musi następować zgodnie z jedną z podstaw prawnych określonych w art. 7. Poddanie się prześwietleniu jest czasem przedstawiane pasażerom jako opcjonalne, co sugeruje, że przetwarzanie może być uzasadnione przez ich zgodę. Odmowa poddania się prześwietleniu może jednak wzbudzić podejrzenia lub poskutkować dodatkową kontrolą, na przykład kontrolą osobistą. Wielu pasażerów zgadza się na prześwietlenie, gdyż w ten sposób unikają potencjalnych problemów lub opóźnień, podczas gdy ich podstawowym priorytetem jest punktualne wejście na pokład samolotu. Taka zgoda nie jest w wystarczającym stopniu dobrowolna. Jako że trzeba dowieść niezbędności przetwarzania (ze względów bezpieczeństwa publicznego), uzasadnionej podstawy nie należy szukać w art. 7 lit. a), ale w akcie prawnym – art. 7 lit. c) lub e) – skutkującym obowiązkiem współpracy ze strony pasażerów. Podstawą kontroli przy użyciu urządzeń do prześwietlania osób powinno zatem być prawodawstwo: można byłoby w nim nadal umożliwić wybór między prześwietleniem a przeszukaniem ręcznym, ale wybór ten byłby oferowany osobom fizycznym jedynie jako uzupełnienie, element działań dodatkowych.

[20] Zob. list przewodniczącego Grupy Roboczej Art. 29 do Daniela Calleja Crespo, dyrektora w DG ds. Energii i Transportu z dnia 11 lutego 2009 r. w sprawie urządzeń do prześwietlania osób w odpowiedzi na konsultacje Komisji w sprawie „skutków wykorzystania urządzeń do prześwietlania osób w dziedzinie ochrony lotnictwa z punktu widzenia praw człowieka, prywatności, godności osobistej, zdrowia i ochrony danych". Dokument ten jest dostępny pod adresem http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009-others_en.htm.

O wyborze podstawy prawnej przetwarzania danych osobowych może też decydować charakter administratora danych. Jest tak zwłaszcza w przypadku administratorów danych w sektorze publicznym, gdzie przetwarzanie danych wiąże się zazwyczaj z wykonaniem zobowiązania prawnego, o którym mowa jest w art. 7 lit. c), lub z realizacją zadania wykonywanego w interesie publicznym, o którym mowa jest w art. 7 lit. e). W związku z tym wykorzystanie zgody zainteresowanej osoby w celu zapewnienia legalności przetwarzania danych nie jest odpowiednią podstawą prawną. Jest to szczególnie oczywiste w przypadku przetwarzania danych osobowych przez organy publiczne wyposażone w uprawnienia władcze – na przykład organy ścigania wykonujące swoje zadania w dziedzinie policji i sądownictwa. Organy policyjne nie mogą polegać na zgodzie osoby fizycznej w przypadku środków, które nie zostały przewidziane w prawie lub nie byłyby w przeciwnym razie dozwolone prawem.

Należy niemniej uznać, że nawet jeżeli państwo ma obowiązek prawny przetwarzania danych osobowych, osoba fizyczna nie zawsze ma obowiązek współpracować. Mogą zaistnieć przypadki, gdy osobom, których dane dotyczą, oferowane są „usługi o wartości dodanej", z których można skorzystać lub nie. W większości przypadków przetwarzanie jest jednak w rzeczywistości obowiązkowe. Często nie jest łatwo stwierdzić, czy przetwarzanie danych osobowych przez organy publiczne opiera się w zgodny z prawem sposób na zgodzie osoby fizycznej. Dlatego też przetwarzanie danych osobowych w sektorze publicznym często bazuje na systemach hybrydowych, co może prowadzić do niepewności i nadużyć, gdy jest ono w niewłaściwy sposób uzasadniane zgodą.

Chociaż zgoda może w wyjątkowych przypadkach stanowić prawomocną podstawę przetwarzania danych osobowych przez państwo, w każdym indywidualnym przypadku należy dokładnie sprawdzić, czy zgoda ta jest w istocie wystarczająco dobrowolna. Jak pokazują poniższe przykłady, gdy administratorem danych jest organ publiczny, podstawą prawną legalności przetwarzania jest zazwyczaj nie zgoda, lecz wykonanie zobowiązania prawnego, o którym mowa w art. 7 lit. c), lub realizacja zadania wykonywanego w interesie publicznym, o którym mowa w art. 7 lit. e).

Przykład: administracja elektroniczna
W państwach członkowskich opracowywane są nowe dowody tożsamości w formie kart z układami elektronicznymi realizującymi pewne funkcje. Aktywacja elektronicznych usług karty może nie być obowiązkowa, jednak bez aktywacji użytkownik może nie mieć dostępu do pewnych usług administracyjnych, skorzystanie z których w inny sposób staje się bardzo trudne (przeniesienie części usług do Internetu, skrócenie godzin otwarcia urzędów). Nie można twierdzić, że zgoda jest uzasadnioną podstawą przetwarzania. Podstawą w tym przypadku powinna być ustawa regulująca rozwój usług elektronicznych wraz ze wszelkimi stosownymi zabezpieczeniami.

Przykład: dane dotyczące przelotu pasażera
Trwa dyskusja dotycząca tego, czy zgodę pasażerów można prawomocnie wykorzystać jako podstawę legalności przekazywania przez europejskie linie lotnicze danych związanych z rezerwacjami („danych PNR") władzom USA. Zdaniem Grupy Roboczej zgoda pasażerów nie może być dobrowolna, gdyż linie lotnicze mają obowiązek

przesłać powyższe dane przed odlotem, w związku z czym pasażerowie nie mają realnego wyboru, jeżeli chcą odbyć podróż[21]. Podstawą prawną nie jest tu zgoda pasażerów, lecz zgodnie z art. 7 lit. c) zobowiązania określone w międzynarodowej umowie między UE a USA w sprawie przetwarzania i przekazywania danych PNR.

Przykład: spis powszechny
Podczas spisu powszechnego obywatelom zadawane są różne pytania na temat ich sytuacji osobistej i zawodowej. Udzielenie odpowiedzi na te pytania jest obowiązkowe. Ponadto w spisie znajduje się pytanie dotyczące wykorzystywanych środków transportu, przy czym wyraźnie zaznaczono, że odpowiedź na jest nieobowiązkowa. Choć w przypadku głównej części spisu nie ma oczywiście dobrowolnej zgody, pozostawia się swobodę wyboru w przypadku ostatniego, nieobowiązkowego pytania. Nie powinno to jednak przesłaniać faktu, że głównym celem państwa publikującego kwestionariusz spisowy jest uzyskanie odpowiedzi. Ogólnie rzecz biorąc, zgoda nie stanowi w tym kontekście prawomocnej podstawy.

„[…] konkretne […]"

Aby zgoda była ważna, musi być konkretna. Innymi słowy, niedopuszczalna jest ogólna zgoda bez określenia dokładnego celu przetwarzania.

Aby zgoda była konkretna, musi być zrozumiała: powinna wyraźnie i precyzyjnie odnosić się do zakresu oraz konsekwencji przetwarzania danych. Nie może ona odnosić się do otwartego zbioru czynności przetwarzania. Innymi słowy, oznacza to, że kontekst, w jakim ma zastosowanie zgoda, jest ograniczony.

Zgoda musi zostać udzielona w odniesieniu do poszczególnych, jasno wskazanych aspektów przetwarzania. Chodzi zwłaszcza o to, jakie dane są przetwarzane i w jakich celach. Kwestia ta powinna być interpretowana w oparciu o racjonalne oczekiwania stron. „Konkretna zgoda" wiąże się więc nierozłącznie z faktem, że zgoda musi być świadoma. Wymaga się szczegółowości zgody w odniesieniu do poszczególnych elementów, które składają się na przetwarzanie danych: nie można uznać, że obejmuje ona „wszystkie uzasadnione cele" administratora danych. Zgoda powinna odnosić się do przetwarzania racjonalnego i niezbędnego z punktu widzenia celu.

Co do zasady powinno wystarczyć, aby administrator danych uzyskał zgodę dotyczącą różnych czynności tylko raz, jeżeli wchodzą one w zakres racjonalnych oczekiwań osoby, której dane dotyczą.

Trybunał Sprawiedliwości wydał niedawno orzeczenie w trybie prejudycjalnym[22] w sprawie art. 12 ust. 2 dyrektywy o prywatności i łączności elektronicznej dotyczące potrzeby ponownego wyrażenia zgody przez abonentów, którzy zgodzili się już na publikację ich danych osobowych w jednej książce telefonicznej, na przekazanie ich

[21] Zob. Opinię 6/2002 Grupy Roboczej Art. 29 w sprawie przekazywania informacji na temat listy pasażerów i innych danych przez linie lotnicze Stanom Zjednoczonym.

[22] Wyrok Trybunału z dnia 5 maja 2011 r. w sprawie Deutsche Telekom AG (sprawa C-543/09). Sprawie tej dał początek wniosek złożony przez niemiecki Federalny Sąd Administracyjny w sprawie książek telefonicznych, a w szczególności interpretacji art. 25 ust. 2 dyrektywy o usłudze powszechnej (2002/22/WE) oraz art. 12 ust. 2 dyrektywy o prywatności i łączności elektronicznej (2002/58/WE). Zagadnienie ma wyraźny związek ze szczególną rolą książek telefonicznych w dyrektywie o usłudze powszechnej.

danych w celu publikacji w innych wykazach. Trybunał uznał, że w sytuacji, gdy abonent został prawidłowo poinformowany o możliwości przekazania jego danych osobowych osobie trzeciej i zgodził się już na publikację tych danych w książce telefonicznej, ponowna zgoda abonenta na przekazanie tych samych danych nie jest już konieczna „pod warunkiem, że dane, o których mowa, nie zostaną wykorzystane do celów innych niż te, dla których zostały zebrane w związku z ich pierwszym opublikowaniem" (pkt 65).

Odrębna zgoda może niemniej być niezbędna, jeżeli administrator danych zamierza przetwarzać dane w innych celach. Na przykład mogłaby zostać udzielona zgoda obejmująca zarówno informacje o nowych produktach dla osoby fizycznej, jak i konkretne akcje promocyjne, gdyż można uznać, że wchodzi to w zakres racjonalnych oczekiwań osoby, której dane dotyczą. Aby jednak umożliwić przesyłanie jej danych osobom trzecim, należy zwrócić się o odrębną, dodatkową zgodę. Potrzeba szczegółowości w odniesieniu do uzyskiwania zgody powinna być oceniana osobno w każdym przypadku zależnie od celu (celów) lub odbiorców danych.

Należy pamiętać, że przetwarzanie może mieć kilka różnych podstaw prawnych: niektóre dane mogą być przetwarzane, ponieważ są niezbędne w związku z umową z osobą, której dane dotyczą, na przykład o dostarczenie produktu i zarządzanie usługami, natomiast konkretna zgoda może być konieczna w przypadku przetwarzania wykraczającego poza zakres niezbędny dla realizacji umowy, na przykład służącego ocenie zdolności kredytowej osoby, której dane dotyczą.

Grupa Robocza wyjaśniła ten aspekt zgody w dokumencie WP 131 w sprawie elektronicznej dokumentacji zdrowotnej: „konkretna" zgoda musi dotyczyć precyzyjnie określonej, konkretnej sytuacji, w której przewidziane jest przetwarzanie danych medycznych. W związku z tym „ogólne przyzwolenie" osoby, której dane dotyczą, przykładowo na gromadzenie danych medycznych tej osoby na potrzeby elektronicznej dokumentacji zdrowotnej oraz dalsze przekazywanie tych danych medycznych w przyszłości pracownikom medycznym uczestniczącym w leczeniu, nie stanowi zgody w rozumieniu art. 2 lit. h) dyrektywy.

Takie samo rozumowanie przedstawiono w dokumencie WP 115 w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną: „definicja wyraźnie wyklucza sytuację, w której udzielenie zgody jest częścią akceptacji ogólnych zasad i warunków oferowanych usług łączności elektronicznej. […] w zależności od rodzaju oferowanych usług zgoda może odnosić się do specjalnych operacji lub może stanowić przyzwolenie zainteresowanej osoby na jej ciągłą lokalizację".

Chociaż w przywołanym powyżej we fragmencie Rozdziału II dotyczącym roli zgody orzeczeniu Trybunału nie użyto wyraźnie terminu „konkretna", również podkreśla się w nim potrzebę, aby zgoda była konkretna, stwierdzając: „nie wystarczy, aby umowa o pracę pracownika odnosiła się jedynie do układu zbiorowego zezwalającego na takie przekroczenie".

Przykład: serwisy społecznościowe
Dostęp do usług serwisów społecznościowych jest często uwarunkowany wyrażeniem zgody na różnego rodzaju przetwarzanie danych osobowych.

Przy rejestracji w serwisie społecznościowym od użytkownika może być wymagana zgoda na otrzymywanie reklamy behawioralnej, bez udostępnienia dodatkowych informacji ani możliwości wyboru opcji alternatywnych. Ze względu na znaczenie, jakie zyskały niektóre serwisy społecznościowe, niektóre kategorie użytkowników (na przykład młodzież) zgadzają się otrzymywać reklamę behawioralną, aby uniknąć ryzyka częściowego wykluczenia z interakcji społecznych. Użytkownik powinien mieć możliwość wyrażenia dobrowolnej i konkretnej zgody na otrzymywanie reklamy behawioralnej niezależnie od dostępu do serwisu społecznościowego. Możliwość taką można byłoby mu zaoferować za pośrednictwem wyskakującego okna.

Serwis społecznościowy oferuje możliwość korzystania z aplikacji zewnętrznych. W praktyce użytkownik często nie może skorzystać z aplikacji, jeżeli nie wyrazi zgody na przekazanie swoich danych jej twórcy do wykorzystania w różnych celach, w tym reklamy behawioralnej i odsprzedaży osobom trzecim. Biorąc pod uwagę fakt, że aplikacja może funkcjonować bez potrzeby przekazywania jakichkolwiek danych jej twórcy, Grupa Robocza zachęca do kierowania się zasadą szczegółowości przy uzyskiwaniu zgody użytkownika, tj. uzyskiwania odrębnej zgody od użytkownika na przekazywanie jego danych twórcy aplikacji do wspomnianych celów. Aby zaoferować użytkownikowi możliwość wyboru sposobów wykorzystania danych, na które wyraża zgodę (przekazanie twórcy; usługi o wartości dodanej; reklama behawioralna; przekazanie osobom trzecim itp.), można zastosować różne mechanizmy, jak na przykład wyskakujące okna.

Konkretność zgody oznacza również, że jeżeli cele, dla których administrator danych przetwarza dane, ulegną w pewnym momencie zmianie, użytkownika trzeba poinformować i umożliwić mu wyrażenie zgody na nowe rodzaje przetwarzania danych. Przedstawione informacje muszą w szczególności dotyczyć konsekwencji odmowy zaakceptowania proponowanych zmian.

„[…] świadome […]"

Ostatnim elementem definicji zgody – ale nie ostatnim wymaganiem, jak zostanie wskazane poniżej – jest jej świadomy charakter.

W art. 10 i 11 dyrektywy określono obowiązek przedstawiania informacji osobom, których dane dotyczą. Obowiązek informowania jest więc zagadnieniem odrębnym, ale w wielu przypadkach w oczywisty sposób powiązanym ze zgodą. Chociaż po przedstawieniu informacji nie zawsze następuje zgoda (można wykorzystać inną podstawę wskazaną w art. 7), przed udzieleniem zgody zawsze muszą zostać dostarczone informacje.

Oznacza to w praktyce, że „zgoda osoby, której dotyczą dane, (musi zostać) podjęta po rozpoznaniu i zrozumieniu faktów oraz następstw. Danej osobie należy jasno i zrozumiale przekazać dokładne i pełne informacje dotyczące wszystkich stosownych kwestii, w szczególności tych wymienionych w art. 10 i 11 dyrektywy, m.in. odnoszących się do charakteru przetwarzanych danych, celów przetwarzania, odbiorców możliwych transferów danych, oraz dotyczące praw osoby, której dane dotyczą. Dana

osoba musi także być świadoma skutków nieudzielenia zgody na to konkretne przetwarzanie"[23].

W wielu sytuacjach zgoda uzyskiwana jest w momencie gromadzenia danych osobowych, gdy rozpoczyna się przetwarzanie. W takim przypadku informacje, które należy przedstawić, pokrywają się z wymienionymi w art. 10 dyrektywy. O zgodę można jednak również zwracać się na etapie późniejszym, gdy cel przetwarzania ulegnie zmianie. W tym przypadku przedstawiane informacje muszą skupić się na tym, co jest niezbędne w konkretnych okolicznościach, w odniesieniu do celu przetwarzania.

Świadoma zgoda ma szczególnie duże znaczenie w kontekście przekazywania danych osobowych państwom trzecim: „wymagane jest, aby osoba, której dane dotyczą, (została) odpowiednio poinformowana o szczególnym ryzyku przekazania jej danych do kraju niezapewniającego odpowiedniego poziomu ochrony"[24].

Można wyróżnić dwa rodzaje wymagań służących zapewnieniu odpowiednich informacji:

- Jakość informacji – sposób przedstawienia informacji (w postaci zwykłego, zrozumiałego, widocznego tekstu, bez żargonu) jest decydujący z punktu widzenia oceny, czy zgoda jest „świadoma". Sposób, w jaki należy przedstawić informacje, zależy od kontekstu: powinien je zrozumieć zwykły/przeciętny użytkownik.

- Dostępność i widoczność informacji – informacje trzeba przedstawić bezpośrednio osobom fizycznym. Nie wystarcza, aby były one gdzieś „dostępne". Trybunał Sprawiedliwości podkreślił to w wyroku z 2004 r.[25], odnosząc się do umowy o pracę zawierającej warunki, których nie wymieniono w umowie, lecz odniesiono się do nich. Informacje muszą być wyraźnie widoczne (rodzaj i wielkość czcionki), rzucające się w oczy i wyczerpujące. W chwili zwracania się o zgodę konkretne informacje można przedstawić w oknach dialogowych. Jak wspomniano powyżej w odniesieniu do „konkretnej zgody", w przypadku serwisów społecznościowych szczególnie przydatne są internetowe narzędzia informacyjne służące zapewnieniu wystarczającej szczegółowości i jasności ustawień prywatności. Użytecznym narzędziem mogą w tym przypadku okazać się też warstwowe noty informacyjne, gdyż ułatwiają one przystępne przedstawienie odpowiednich informacji.

W miarę upływu czasu mogą pojawić się wątpliwości, czy zgoda udzielona pierwotnie w oparciu o właściwe i wystarczające informacje pozostaje ważna. Ludzie często zmieniają poglądy z różnych powodów – ich pierwotna decyzja mogła być nieprzemyślana lub sytuacja mogła się zmienić (np. dziecko osiąga większy stopień dojrzałości)[26]. Dlatego też dobrą praktyką jest, aby administratorzy danych dokonywali po pewnym czasie przeglądu decyzji podjętych przez poszczególne osoby, na przykład

---

[23] WP 131 – Dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej (EHR).

[24] WP12 – Dokument roboczy o przekazywaniu danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych. Zob. też WP114 – Dokument roboczy Grupy Roboczej Art. 29 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.

[25] Zob. przypis 12 (Rozdział II.2).

[26] Dokument roboczy 1/2008 w sprawie ochrony danych osobowych dzieci, WP 147, 18 lutego 2008 r.

informując je o bieżącym wyborze i oferując możliwość jego potwierdzenia lub cofnięcia[27]. Stosowny okres zależałby oczywiście od kontekstu i okoliczności sprawy.

Przykład: mapy przestępczości
Niektóre formacje policyjne rozważają publikację map lub udostępnianie innych danych pokazujących, gdzie dochodziło do poszczególnych rodzajów przestępstw. Zazwyczaj procesowi temu towarzyszą zabezpieczenia, dzięki którym nie są publikowane dane osobowe ofiar, gdyż przestępstwa są przyporządkowywane do stosunkowo rozległych regionów geograficznych. Niektóre formacje policyjne chcą jednak dokładniej wskazywać miejsca przestępstw w przypadkach, gdy ofiary wyrażają na to zgodę. W takim przypadku możliwe staje się precyzyjniejsze powiązanie osoby, której dane dotyczą, z miejscem, w którym popełniono przestępstwo. Ofiarom nie mówi się jednak konkretnie, że umożliwiające ich identyfikację informacje zostaną opublikowane w Internecie, ani też w jaki sposób mogą one zostać wykorzystane. Tak więc zgoda w tym przypadku nie jest ważna, gdyż ofiary mogą nie być w pełni świadome zakresu informacji publikowanych na ich temat.

Wraz ze wzrostem złożoności przetwarzania danych rosną oczekiwania wobec administratora danych. Im trudniej przeciętnemu obywatelowi jest nadzorować i zrozumieć wszystkie elementy procesu przetwarzania danych, tym większy wysiłek powinien podjąć administrator danych w celu wykazania, że zgodę uzyskano w oparciu o konkretne i zrozumiałe informacje.

Zdefiniowaną w art. 2 lit. h) zgodę należy interpretować łącznie z dodatkowymi wymaganiami wymienionymi w dalszej części dyrektywy. W art. 7 do elementów definicji dodaje się słowo „jednoznacznie", a w art. 8 słowo „wyraźnej", gdy przetwarzanie dotyczy określonych kategorii danych.

III.A.2. Artykuł 7 lit. a)

Zgodnie z art. 7 lit. a) dyrektywy podstawę prawną przetwarzania danych osobowych stanowi jednoznaczna zgoda osoby, której dane dotyczą. Tak więc, aby zgoda była ważna, musi ona oprócz spełnienia kryteriów określonych w art. 2 lit. h) być również *jednoznaczna*.

Aby zgoda była jednoznaczna, procedura ubiegania się o zgodę i jej udzielania *nie może pozostawiać wątpliwości* co do zamiaru wyrażenia zgody przez osobę, której dane dotyczą. Innymi słowy, wskazanie przez osobę, której dane dotyczą, na to, że wyraża przyzwolenie, musi niedwuznacznie określać jej zamiar. Jeżeli istnieją uzasadnione wątpliwości co do intencji osoby fizycznej, występuje dwuznaczność.

Jak opisano bardziej szczegółowo poniżej, wymaganie to zmusza administratorów danych do tworzenia niezawodnych procedur pozwalających osobom fizycznym wyrazić zgodę; muszą oni mianowicie ubiegać się o jasną i wyraźną zgodę lub polegać na pewnych procedurach umożliwiających uzyskanie jasnej dorozumianej zgody osoby fizycznej. Administrator danych musi również posiadać wystarczającą pewność, że

[27] Grupa Robocza Art. 29 wydała podobne zalecenie w Opinii 2/2010 w sprawie internetowej reklamy behawioralnej przyjętej w dniu 22 czerwca 2010 r. (WP 171).

osoba udzielająca zgody jest w rzeczywistości osobą, której dane dotyczą. Jest to szczególnie istotne, gdy zgoda jest wyrażana przez telefon lub w Internecie.

Powiązanym zagadnieniem jest dowód uzyskania zgody. Administratorzy danych wykorzystujący zgodę mogą chcieć lub musieć wykazać, że uzyskali zgodę, na przykład w kontekście sporu z osobą, której dane dotyczą. W niektórych przypadkach wniosek o przedstawienie takich dowodów może wręcz wiązać się z działaniami mającymi na celu egzekwowanie przepisów. W związku z tym, a także w ramach dobrej praktyki, administratorzy danych powinni pozyskiwać i przechowywać dowody tego, że zgoda została w istocie udzielona, tj. zgoda powinna być możliwa do zweryfikowania.

Poniżej zamieszczono analizę pewnych metod udzielania zgody wraz z oceną, czy pozwalają one uzyskać jednoznaczną zgodę.

Procedurami lub mechanizmami dobrze nadającymi się do uzyskiwania jednoznacznej zgody są wyraźne oświadczenia wyrażające przyzwolenie, takie jak podpisana umowa lub pisemne oświadczenia o chęci wyrażenia przyzwolenia. Jednocześnie dostarczają one co do zasady administratorowi danych dowodu, że uzyskano zgodę.

Przykład: zgoda na otrzymywanie informacji promocyjnych drogą pocztową
Hotel prosi osoby fizyczne o podanie na papierowym formularzu adresu pocztowego, jeżeli życzą sobie otrzymywać informacje promocyjne drogą pocztową. Jeżeli dana osoba, po podaniu danych adresowych, podpisze formularz, wyrażając tym samym przyzwolenie, będzie to stanowić jednoznaczną zgodę. W takim przypadku będzie ona zarówno wyraźna, jak i pisemna. Procedura ta daje administratorowi danych wystarczający dowód uzyskania zgody wszystkich klientów pod warunkiem, że administrator danych zachowa wszystkie podpisane formularze.

Nie wszystkie jednak formy zgody, które mogą wydawać się wyraźne, skutkują uzyskaniem zgody. Kwestię tę poruszono w rozpatrywanej niedawno przez Trybunał Sprawiedliwości sprawie (Volker i Markus Schecke przeciwko krajowi związkowemu Hesji), która dotyczyła publikacji nazwisk beneficjentów różnych funduszy UE[28] oraz kwot otrzymanych przez poszczególnych beneficjentów. Rzecznik generalna zbadała, czy warunki jednoznacznej zgody zostały spełnione w przypadku, w którym osoby fizyczne podpisały oświadczenie stwierdzające: „Przyjmuję do wiadomości, że na podstawie art. 44a rozporządzenia […] nr 1290/2005 informacje o beneficjentach środków z EFRG i EFRROW i o kwotach przez nich otrzymanych podlegają publikacji". Rzecznik generalna stwierdziła: „Przyjęcie do wiadomości uprzedniego zawiadomienia, że nastąpi jakaś publikacja, nie jest tożsame z wyrażeniem »jednoznacznej« zgody na konkretny rodzaj szczegółowej publikacji. Nie można tego również określić jako »dobrowolne konkretne wskazanie« woli wnioskodawców zgodnie z definicją zgody osoby, których dane dotyczą, zawartą w art. 2 lit. h)". W związku z tym rzecznik generalna uznała, że skarżący nie wyrazili zgody na przetwarzanie (tj. publikację) ich danych osobowych w rozumieniu art. 7 lit. a) dyrektywy 95/46/WE[29].

[28] Europejskiego Funduszu Rolniczego Gwarancji (EFRG) i Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich (EFRROW).

[29] Opinia rzecznika generalnego Eleanor Sharpston przedstawiona w dniu 17 czerwca 2010 r., Volker und Markus Schecke GbR, w sprawach połączonych C-92/09 i C-93/09. Należy zauważyć, że w wyroku z dnia 9 listopada 2010 r. Trybunał Sprawiedliwości orzekł, że przetwarzanie danych nie opierało się na zgodzie: „63. Odnośna regulacja unijna, która

Wyraźnej zgody można udzielić również w środowisku internetowym. Podobnie jak w świecie rzeczywistym (*off-line*), istnieją tam środki odpowiednie do udzielenia jednoznacznej zgody, co ilustruje następujący przykład:

Przykład: zgoda za pośrednictwem Internetu na udział w programie lojalnościowym
Na stronie internetowej hotelu znajduje się formularz rezerwacyjny, za pośrednictwem którego osoby fizyczne mogą z wyprzedzeniem rezerwować pokoje drogą elektroniczną. W internetowym formularzu, w którym osoby fizyczne wprowadzają żądane daty i informacje związane z płatnością, znajduje się też widoczne pole wyboru, które powinny zaznaczyć osoby chcące, aby ich dane osobowe zostały wykorzystane w związku z zapisami do programu lojalnościowego. Zaznaczenie pola po otrzymaniu odpowiednich informacji stanowi wyraźną, jednoznaczną zgodę, gdyż działanie polegające na zaznaczeniu pola wyboru jest wystarczająco jasne, by nie pozostawiać wątpliwości co do woli uczestnictwa osoby fizycznej w programie lojalnościowym.

Wyraźnej zgody można udzielić również ustnie poprzez oświadczenie mające na celu wyrażenie przyzwolenia. Wyraźna zgoda ustna jest udzielana w następującej sytuacji:

Przykład: ustna zgoda na otrzymywanie informacji promocyjnych
Podczas dokonywania płatności za usługi hotelowe klienci są pytani przez recepcjonistę, czy chcieliby podać swój adres, aby hotel mógł im przesyłać informacje promocyjne. Osoby fizyczne, które po wysłuchaniu pytania pracownika i odpowiednich informacji odpowiadają, podając swój adres, udzielają wyraźnej zgody. Działanie polegające na podaniu adresu może stanowić jednoznaczne wskazanie woli osoby fizycznej. Administrator danych może jednak zdecydować się wprowadzić mechanizmy pozwalające dowieść w bardziej wiarygodny sposób, że zgoda została udzielona.

W pewnych okolicznościach jednoznaczna zgoda może zostać *dorozumiana* na podstawie pewnych działań; w szczególności ma to miejsce, gdy działania te prowadzą do niebudzącego wątpliwości wniosku, że udzielono zgody. Zależy to jednak od tego, czy przedstawiono odpowiednie informacje dotyczące przetwarzania danych, które umożliwiają osobie fizycznej podjęcie decyzji (kto jest administratorem danych, jakie są cele przetwarzania itp.).

ogranicza się do ustanowienia, że beneficjenci pomocy będą wcześniej informowani o publikacji dotyczących ich danych, nie zmierza więc do oparcia wprowadzonego przez nią przetwarzania danych osobowych na zgodzie zainteresowanych beneficjentów".

Przykład: zgoda na fotografowanie
Podczas meldowania się w hotelu klienci są informowani przez recepcjonistę, że w jednej z hotelowych kawiarni odbędzie się po południu sesja fotograficzna. Wybrane zdjęcia zostaną wykorzystane w materiałach marketingowych, w szczególności w drukowanych broszurach hotelu. Jeżeli goście hotelowi pragną znaleźć się na zdjęciach, zaprasza się ich do kawiarni w określonych godzinach. Dla osób, które nie chcą zostać sfotografowane, dostępna jest inna kawiarnia.

Można uznać, że ci goście hotelowi, którzy po uzyskaniu informacji zdecydują się udać do kawiarni podczas sesji, wyrazili zgodę na fotografowanie. Wniosek o ich zgodzie można wyciągnąć z działania polegającego na pójściu do kawiarni, w której odbywa się sesja, o danej porze. Pójście do kawiarni stanowi wskazanie woli osoby fizycznej, które co do zasady można uznać za jednoznaczne, gdyż nie ma większych wątpliwości co do tego, że osoba udająca się do kawiarni pragnęła zostać sfotografowana. Z punktu widzenia hotelu rozsądne byłoby jednak posiadanie dokumentów potwierdzających uzyskanie zgody na wypadek, gdyby jej ważność została w bliskiej przyszłości zakwestionowana.

Jak już stwierdzono, w Internecie i w środowisku *off-line* obowiązują te same wymagania, w tym wymóg jednoznacznej zgody. Grupa Robocza zauważa jednak, że ryzyko niejednoznaczności zgody może być większe w Internecie, co wymaga szczególnej uwagi. Następny przykład ilustruje przypadek, w którym zgoda wywnioskowana z pewnych działań (udziału w grze internetowej) nie spełnia wymogów ważnej zgody.

Przykład: gra internetowa
Podmiot oferujący grę internetową wymaga od graczy, by podali swój wiek, nazwisko oraz adres w celu uczestnictwa w grze (chodzi o rozkład graczy według wieku i lokalizacji). Na stronie internetowej znajduje się informacja dostępna za pośrednictwem łącza (chociaż uzyskanie dostępu do tej informacji nie jest niezbędne, aby wziąć udział w grze), w której stwierdza się, że korzystając ze strony internetowej (a więc podając informacje), gracze zgadzają się na przetwarzanie swoich danych do celów otrzymywania informacji marketingowych od podmiotu oferującego grę i osób trzecich.

Dostęp i udział w grze nie są równoznaczne z udzieleniem jednoznacznej zgody na dalsze przetwarzanie informacji osobowych do celów innych niż udział w grze. Udział w grze nie oznacza zamiaru udzielenia przez osobę fizyczną zgody na przetwarzanie w zakresie innym niż niezbędny do gry. Ten rodzaj zachowania nie stanowi jednoznacznego wskazania woli osoby fizycznej, aby jej dane były wykorzystywane w celach marketingowych.

Przykład: domyślne ustawienia prywatności
Domyślne ustawienia serwisu społecznościowego, do których użytkownicy nie muszą zaglądać, aby z niego korzystać, dają dostęp do informacji całej kategorii „znajomi znajomych", co oznacza, że komplet danych osobowych każdego użytkownika jest widoczny dla wszystkich „znajomych znajomych". Użytkownicy, którzy nie chcą, aby dotyczące ich informacje widzieli „znajomi znajomych", muszą kliknąć przycisk. Jeżeli pozostaną bierni lub nie podejmą działania polegającego na kliknięciu przycisku, administrator danych uzna to za zgodę na widoczność ich danych. Bardzo wątpliwe jest jednak, czy *brak* kliknięcia przycisku oznacza, że wszyscy *wyrazili zgodę*, aby ich dane były widoczne dla wszystkich „znajomych znajomych". Ze względu na niepewność co do tego, czy brak działania ma oznaczać zgodę, brak kliknięcia może nie zostać uznany za jednoznaczną zgodę.

Powyższy przykład ilustruje przypadek, w którym osoba fizyczna pozostaje bierna (np. nie podejmuje działania lub „milczy"). Jednoznaczna zgoda nie daje się łatwo pogodzić z procedurami uzyskiwania zgody na podstawie bezczynności lub milczenia: milczenie lub bezczynność są zawsze dwuznaczne (osoba, której dane dotyczą, mogła mieć na celu wyrażenie zgody lub mogła jedynie mieć na celu niewykonanie pewnej czynności). Ilustruje to przywołany poniżej przykład.

Sytuacja, w której uznaje się, że osoba fizyczna wyraziła zgodę, jeżeli nie odpowiedziała na list informujący ją, iż brak odpowiedzi oznacza zgodę, jest dwuznaczna. W tego rodzaju sytuacjach zachowanie osoby fizycznej (lub raczej jego brak) budzi poważne wątpliwości co do tego, czy miała ona na celu wyrażenie przyzwolenia. Fakt, że dana osoba nie podjęła żadnych konkretnych działań, nie pozwala wnioskować, iż wyraziła zgodę. Wymóg jednoznacznej zgody nie jest więc spełniony. Ponadto, jak wskazano bardziej szczegółowo poniżej, administrator danych będzie miał poważne trudności z przedstawieniem dowodów świadczących o wyrażeniu zgody przez osobę fizyczną.

Grupa Robocza wskazała nieodpowiedniość zgody opartej na milczeniu osób fizycznych w kontekście marketingu bezpośredniego prowadzonego za pośrednictwem poczty elektronicznej. „Dorozumiana zgoda na otrzymywanie takich wiadomości nie jest zgodna z definicją zgody zawartą w dyrektywie 95/46/WE […] Podobnie domyślnie zaznaczone pola wyboru, np. na stronach internetowych, również nie są zgodne z definicją w dyrektywie"[30]. Poniższy przykład potwierdza ten pogląd:

Przykład: nieważna zgoda na dalsze wykorzystanie danych klienta
Księgarnia internetowa rozsyła do uczestników swojego programu lojalnościowego wiadomości e-mail, informując ich, że ich dane zostaną przekazane firmie reklamowej, która planuje wykorzystać je do celów marketingowych. Użytkownicy mają dwa tygodnie, by odpowiedzieć na wiadomość e-mail. Informuje się ich, że brak odpowiedzi zostanie uznany za zgodę na przekazanie danych. Ten rodzaj mechanizmu, w którym o zgodzie wnioskuje się na podstawie braku reakcji osób fizycznych, nie skutkuje ważną, jednoznaczną zgodą. Nie można w niewątpliwy sposób ustalić, czy osoba fizyczna wyraziła przyzwolenie na przekazanie danych, na podstawie braku odpowiedzi.

[30] Opinia 5/2004 w sprawie niezamówionych komunikatów do celów marketingu zgodnie z art. 13 dyrektywy 2002/58/WE, przyjęta w dniu 27 lutego 2004 r. (WP 90).

Z powyższego wynika, że wymaganie, aby zgoda była *jednoznaczna*, skutkuje zachętą dla administratorów danych, aby wdrażać procedury i mechanizmy niepozostawiające wątpliwości co do tego, że zgoda została udzielona na podstawie wyraźnego działania osoby fizycznej lub na mocy jednoznacznego wniosku wyciągniętego z działania osoby fizycznej.

Jak wspomniano powyżej, w ramach dobrej praktyki administratorzy danych powinni rozważyć wdrożenie stosownych środków i procedur, aby wykazać, że zgoda została udzielona. Im bardziej skomplikowane jest środowisko, w którym działają, tym więcej środków będzie niezbędnych w celu zapewnienia możliwości weryfikacji zgody. Informacje te powinny być udostępniane na żądanie organowi ochrony danych.

III.A.3. Artykuł 8 ust. 2 lit. a)

W art. 8 dyrektywy zapewniono szczególną ochronę „szczególnych kategorii danych", które ze swojej natury są uważane za bardzo wrażliwe. Przetwarzanie takich danych jest zabronione, chyba że zachodzi co najmniej jeden z kilku wskazanych wyjątków. Zgodnie z art. 8 ust. 2 lit. a) zakaz ten nie obowiązuje, jeżeli osoba, której dane dotyczą, udzieliła *wyraźnej zgody* na ich przetwarzanie.

Z prawnego punktu widzenia dwa angielskie terminy (*explicit* i *express*) oznaczające „wyraźną" zgodę są równoważne. Zgoda taka ma miejsce we wszystkich sytuacjach, gdy osobie fizycznej przedstawia się propozycję wyrażenia przyzwolenia (lub nie) na konkretny sposób wykorzystania lub ujawnienia jej danych osobowych, a osoba ta aktywnie (ustnie lub pisemnie) odpowiada na zadane pytanie. Wyraźna zgoda udzielana jest zazwyczaj w formie pisemnej, z odręcznym podpisem. Wyraźna zgoda jest na przykład udzielana, gdy osoby, których dane dotyczą, podpisują formularz zgody jasno określający, dlaczego administrator danych pragnie gromadzić i dalej przetwarzać dane osobowe.

Chociaż wyraźnej zgody tradycyjnie udziela się w formie pisemnej (na papierze lub w formie elektronicznej), co opisano w Rozdziale III.A.2, nie jest to niezbędne, a więc może ona również zostać udzielona ustnie. Potwierdza to fakt usunięcia proponowanego wymogu, aby zgoda opisana w art. 8 została udzielona na piśmie, z ostatecznej wersji dyrektywy. Jak jednak wskazano w tym samym rozdziale, zgoda ustna może być trudna do udowodnienia, a więc w praktyce administratorom danych zaleca się uzyskiwanie zgody w formie pisemnej dla celów dowodowych.

Wymaganie wyraźnej zgody oznacza, że zgoda dorozumiana zazwyczaj nie spełnia wymogu art. 8 ust. 2. W tym kontekście warto przypomnieć opinię Grupy Roboczej Art. 29 w sprawie elektronicznej dokumentacji zdrowotnej[31], w której stwierdza się: „W odróżnieniu od przepisów art. 7 dyrektywy zgoda w przypadku szczególnie chronionych danych osobowych oraz, co za tym idzie, w przypadku EHR musi być **wyraźna**. Niezajęcie stanowiska nie spełnia wymogu »wyraźnej« zgody […]".

[31] WP 131 – Dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej (EHR).

Przykład: dane medyczne do potrzeb badań
Nie spełnia wymogu wyraźnej zgody poinformowanie pacjenta przez klinikę, że jego dokumentacja medyczna zostanie przekazana do potrzeb badań, chyba że wyrazi on sprzeciw (telefonując pod wskazany numer).

Jak wskazano w Rozdziale II.A.2, osoba fizyczna może udzielić wyraźnej zgody ustnie i na piśmie, podejmując konkretne działanie w celu wyrażenia swojego pragnienia, aby dać przyzwolenie na pewną formę przetwarzania danych. W środowisku internetowym wyraźnej zgody można udzielić, posługując się podpisem elektronicznym. Można jednak zależnie od kontekstu udzielić jej też klikając przycisk, wysyłając wiadomość e-mail z potwierdzeniem, klikając ikonę itp.[32]. Wyraźną akceptację procedur związanych z konkretnym działaniem osoby fizycznej zawiera motyw 17 dyrektywy o prywatności i łączności elektronicznej, w którym stwierdza się: „Zgoda może być udzielona w jakikolwiek sposób umożliwiający swobodne i świadome wyrażenie woli użytkownika, włączając zaznaczenie okna wyboru podczas przeglądania witryny internetowej".

Ważności zgody nie warunkuje możliwość jej zarejestrowania. Zachowanie dowodu leży jednak w interesie administratora danych. Oczywiście wiarygodność poszczególnych mechanizmów może się różnić, przez co dostarczają one w większym lub mniejszym stopniu dowodu udzielenia zgody. Zgoda uzyskana za pośrednictwem kliknięcia przycisku w sytuacji, gdy tożsamość danej osoby fizycznej potwierdza tylko adres poczty elektronicznej, będzie miała znacznie mniejszą wartość dowodową od zgody uzyskanej za pośrednictwem podobnego procesu umożliwiającego na przykład zarejestrowanie uzyskania zgody[33]. Potrzeba uzyskania silnych dowodów będzie również zależeć od rodzaju gromadzonych danych i celu tego procesu: podpis elektroniczny nie będzie konieczny w przypadku zgody na otrzymywanie ofert handlowych, ale może być niezbędny do wyrażenia zgody na przetwarzanie w Internecie pewnych rodzajów danych finansowych. Wyraźna zgoda udzielona w środowisku internetowym musi być możliwa do zarejestrowania, aby można było uzyskać do niej dostęp w przyszłości[34].

W świetle powyższego uznaje się, że internetowe formularze rejestracyjne, za pośrednictwem których osoby fizyczne wprowadzają identyfikujące je dane oraz wyrażają przyzwolenie na przetwarzanie danych, spełniają wymóg wyraźnej zgody pod warunkiem spełnienia wszystkich pozostałych wymogów. Na przykład otwierając osobistą internetową dokumentację medyczną pacjenci mogą udzielić zgody, podając dane kontaktowe i zaznaczając odpowiednie pole wyboru, aby wyrazić przyzwolenie.

---

32 Interpretacja ta jest zgodna z prawodawstwem UE, głównie dotyczącym handlu elektronicznego i szerszego wykorzystania podpisu elektronicznego, w którym wymaga się, aby państwa członkowskie zmieniły swoje przepisy zawierające formalne wymagania co do „pisemnej" i „odręcznej" postaci dokumentów, tak aby ich elektroniczne odpowiedniki były również akceptowane, jeżeli spełnione są określone warunki.

33 W związku z tą kwestią zob. na przykład ustawy grecką i niemiecką w sprawie wymagań wobec zgody udzielanej drogą elektroniczną, w których wymaga się, aby zgoda była rejestrowana w bezpieczny sposób, aby użytkownik lub abonent miał do niej dostęp w każdej chwili i aby istniała możliwość jej odwołania w dowolnym momencie (art. 5 ust. 3 greckiej ustawy nr 3471/2006 o ochronie danych osobowych w sektorze łączności elektronicznej; art. 13 ust. 2 niemieckiej ustawy o usługach świadczonych zdalnie, art. 94 niemieckiej ustawy o telekomunikacji oraz art. 28 ust. 3a niemieckiej ustawy federalnej o ochronie danych).

34 Analiza warunków technicznych, jakie muszą spełniać dokumenty elektroniczne i podpisy elektroniczne, aby ich wartość dowodową uznawano za równoważną odręcznym odpowiednikom, wykracza poza zakres niniejszej opinii. Kwestia ta nie wchodzi w zakres prawodawstwa o ochronie danych i została uregulowana na szczeblu UE.

Wykorzystanie silniejszych metod uwierzytelnienia – na przykład podpisu elektronicznego – poskutkuje oczywiście tym samym wynikiem, dając mocniejszy dowód[35].

W niektórych przypadkach państwa członkowskie mogą zdecydować, że podstawą legalności danej czynności przetwarzania danych musi być zgoda, oraz określić rodzaj zgody. Na przykład w przypadku ubiegania się o kartę umożliwiającą dostęp do dokumentacji medycznej państwa członkowskie mogą postanowić, że osoby fizyczne rejestrujące się za pośrednictwem Internetu muszą korzystać z konkretnego rodzaju podpisu elektronicznego. Wybór taki zagwarantuje wyraźną zgodę, dając również administratorowi danych większą pewność, że będzie w stanie wykazać, iż osoba fizyczna udzieliła zgody.

III.A.4. Artykuł 26 ust. 1

W art. 26 ust. 1 lit. a) wskazano jednoznaczną zgodę osoby, której dane dotyczą, jako wyjątek od zakazu przekazywania danych do państw trzecich, które nie zapewniają odpowiedniego stopnia ochrony. Wcześniejsze rozważania dotyczące art. 7 lit. a) mają zastosowanie również w tym przypadku. Oznacza to, że oprócz spełnienia wymogów dotyczących ważnej zgody, o których mowa w art. 2 lit. h), zgoda musi być także jednoznaczna.

Grupa Robocza Art. 29 poświęciła wiele wysiłku, aby opracować wskazówki dotyczące stosowania art. 25 i 26 dyrektywy, w tym wyjątku związanego ze zgodą. W tym kontekście warto przypomnieć fragment dokumentu WP 12[36] Grupy Roboczej dotyczący znaczenia jednoznacznej zgody: „Ponieważ zgoda musi być jednoznaczna, wszelkie wątpliwości co do tego, czy zgoda została udzielona, uniemożliwiają zastosowanie tego wyjątku. Może to ze znacznym prawdopodobieństwem oznaczać, że w wielu sytuacjach, w których zgoda jest dorozumiana (na przykład dlatego, że osoba fizyczna została poinformowana o przekazaniu danych i nie wyraziła sprzeciwu), wyjątek ten nie ma zastosowania".

W świetle powyższego uzyskanie jednoznacznej zgody jest bardziej prawdopodobne, gdy dana osoba podejmuje konkretne działanie wyrażające przyzwolenie na przekazanie danych, na przykład podpisując formularz zgody lub podejmując inne działania, które w niebudzący wątpliwości sposób potwierdzają wniosek, że zgody udzielono.

W dokumencie WP 114[37] dotyczącym wykorzystania zgody w odniesieniu do przekazywania danych Grupa Robocza stwierdziła: „zgoda […] raczej nie zapewni administratorom odpowiedniej i trwałej podstawy działania w przypadku powtarzających się lub strukturalnych przekazów danych przeznaczonych do przetwarzania. W praktyce, zwłaszcza jeśli przekaz stanowi nierozerwalną część

---

35 Jest tak, ponieważ w przypadku pewnych rodzajów podpisu elektronicznego (zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie i utworzonego przy użyciu bezpiecznego urządzenia służącego do składania podpisu elektronicznego) istnieje automatyczne domniemanie takiej samej wartości dowodowej, jak w przypadku podpisu odręcznego.

36 WP12 – Dokument roboczy o przekazywaniu danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych, przyjęty w dniu 24 lipca 1998 r.

37 Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r., przyjęty w dniu 25 listopada 2005 r.

głównej operacji przetwarzania (np. centralizacja światowej bazy danych o zasobach ludzkich, która aby funkcjonować właściwie, musi być stale i systematycznie zasilana danymi), administratorzy mogą znaleźć się w sytuacji bez wyjścia, jeśli choćby jeden podmiot danych postanowi po jakimś czasie wycofać swoją zgodę. Mówiąc ściślej, nie będzie można już przekazywać danych dotyczących osoby, która wycofała swoją zgodę. W takiej sytuacji przekazywanie danych dalej odbywałoby się częściowo na podstawie zgody podmiotu danych, ale w odniesieniu do tych osób, które swoją zgodę wycofały, należałoby znaleźć rozwiązanie alternatywne (umowa, wiążące zasady korporacyjne itp.). Opieranie się na zgodzie może zatem okazać się rozwiązaniem tylko pozornie dobrym: na pierwszy rzut oka prostym, ale w rzeczywistości złożonym i kłopotliwym".

III.A.5. Zgoda udzielana przez osoby fizyczne nieposiadające pełnej zdolności do czynności prawnych

W dyrektywie 95/46/WE nie określono konkretnych zasad dotyczących uzyskiwania zgody osób fizycznych nieposiadających pełnej zdolności do czynności prawnych, w tym dzieci. Ten fakt należy wziąć pod uwagę przy przeglądzie dyrektywy o ochronie danych. Oprócz kwestii poruszonych powyżej zgoda ze strony tych osób wiąże się z dodatkowymi, specyficznymi problemami.

W przypadku dzieci warunki udzielenia ważnej zgody różnią się w poszczególnych państwach członkowskich. Grupa Robocza Art. 29 rozważała kilkakrotnie zagadnienie zgody udzielanej przez dzieci, badając krajowe praktyki w tym zakresie[38].

Z dotychczasowych prac wynika, że w przypadku ubiegania się o zgodę dziecka, przepisy prawa mogą wymagać uzyskania zgody dziecka i jego przedstawiciela ustawowego, lub też wyłącznie zgody dziecka, jeżeli jest ono już dojrzałe. Istnieją różne granice wiekowe dla stosowania tych zasad. Brak jest zharmonizowanych procedur weryfikacji wieku dziecka.

W związku z brakiem ogólnych zasad w tym zakresie podejście do problemu jest fragmentaryczne i nie dostrzega się potrzeby szczególnej ochrony dzieci w pewnych okolicznościach ze względu na ich bezbronność oraz pojawianie się niepewności prawnej, zwłaszcza jeżeli chodzi o sposób uzyskiwania zgody dzieci.

Zdaniem Grupy Roboczej taki brak harmonizacji pociąga za sobą konsekwencje z punktu widzenia pewności prawnej. Harmonizacja warunków umożliwiających osobom fizycznym nieposiadającym pełnej zdolności do czynności prawnych korzystanie ze swoich praw na szczeblu UE, zwłaszcza w odniesieniu do progu wiekowego, z pewnością zaowocowałaby dodatkowymi gwarancjami. Grupa Robocza zdaje sobie jednak sprawę, że zagadnienia te mogą wykraczać dalece poza zakres ochrony danych, dotycząc ogólniej kwestii prawa cywilnego. Grupa Robocza zwraca uwagę Komisji na trudności wskazane w tym obszarze.

Ponadto zdaniem Grupy Roboczej Art. 29 interesy dzieci i innych osób fizycznych nieposiadających pełnej zdolności do czynności prawnych byłyby lepiej chronione,

[38] WP 147 – Dokument roboczy 1/2008 w sprawie ochrony danych osobowych dzieci (ogólne wytyczne i szczególny przypadek szkół); WP 160 – Opinia 2/2009 w sprawie ochrony danych osobowych dzieci (ogólne wytyczne i szczególny przypadek szkół).

gdyby dyrektywa zawierała dodatkowe przepisy dotyczące konkretnie gromadzenia i dalszego przetwarzania ich danych. W przepisach tych można byłoby określić okoliczności, w których niezbędna byłaby zgoda przedstawiciela ustawowego wraz ze zgodą osoby fizycznej nieposiadającej pełnej zdolności do czynności prawnych lub w miejsce tej zgody, jak też okoliczności, w których nie powinno być możliwe wykorzystanie zgody jako podstawy legalności przetwarzania danych osobowych. Należałoby też uwzględnić wymóg stosowania mechanizmów weryfikacji wieku w środowisku internetowym. Możliwe są różne mechanizmy i progi wiekowe. Na przykład weryfikacja wieku nie musiałaby podlegać jednej regule, ale mogłaby opierać się na ruchomej skali, przy czym wykorzystywany mechanizm byłby uzależniony od okoliczności takich jak rodzaj (cele) przetwarzania, podwyższone ryzyko, rodzaj gromadzonych danych, sposoby wykorzystania danych (czy mają one zostać ujawnione) itp.

III.B. Dyrektywa 2002/58/WE

Zmieniona niedawno dyrektywa o prywatności i łączności elektronicznej (dyrektywa 2002/58/WE)[39] stanowi *lex specialis* w stosunku do dyrektywy 95/46/WE, gdyż ustanawia zasady sektorowe w odniesieniu do prywatności i łączności elektronicznej. Większość jej przepisów dotyczy wyłącznie dostawców publicznie dostępnych usług łączności elektronicznej (np. dostawców usług telefonicznych, internetowych itp.).

Niektóre przepisy dyrektywy o prywatności i łączności elektronicznej bazują na zgodzie jako podstawie prawnej pozwalającej przetwarzać dane dostawcom publicznie dostępnych usług łączności elektronicznej[40]. Tak jest na przykład w przypadku wykorzystywania danych o ruchu lub lokalizacji.

Zdaniem Grupy Roboczej Art. 29 warto skomentować wybrane, szczególnie interesujące aspekty związane z wykorzystaniem zgody na mocy dyrektywy o prywatności i łączności elektronicznej. Omówionych zostanie w tym celu następujących pięć zagadnień:

a) Związek między dyrektywą 95/46/WE a dyrektywą o prywatności i łączności elektronicznej w odniesieniu do definicji i ogólnego znaczenia zgody. Kwestii tej dotyczy art. 2 lit. f) dyrektywy o prywatności i łączności elektronicznej.

b) Pytanie, czy w celu naruszenia poufności komunikacji (na przykład monitorowania lub przejęcia łączności telefonicznej) niezbędne jest uzyskanie zgody jednej czy też obydwu stron komunikacji. Kwestię tę regulują art. 6 ust. 3 i art. 5 ust. 1.

---

[39] Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE 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, 18 grudnia 2009 r.

[40] Dane o ruchu oznaczają wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi, w tym dane dotyczące wyznaczania trasy, długości lub czasu komunikatu.

c) Pytanie o moment, w którym należy uzyskać zgodę. Kwestii tej dotyczą liczne przepisy dyrektywy o prywatności i łączności elektronicznej, w tym art. 5 ust. 3, art. 6 i 13.

d) Zakres zastosowania prawa sprzeciwu i rozróżnienie między nim a zgodą. Rozróżnienie to można analizować na podstawie art. 13 dyrektywy o prywatności i łączności elektronicznej.

e) Możliwość odwołania zgody określona wyraźnie w art. 6 ust. 3 oraz art. 9 ust. 3 i 4 dyrektywy o prywatności i łączności elektronicznej.

III.B.1. Artykuł 2 lit. f) – Zgoda i związek z dyrektywą 95/46/WE

„zgoda użytkownika lub abonenta"

W art. 2 dyrektywy o prywatności i łączności elektronicznej wyraźnie stwierdza się, że definicje zawarte w dyrektywie 95/46/WE mają zastosowanie do dyrektywy 2002/58/WE. W art. 2 lit. f) stanowi się: „»zgoda« użytkownika lub abonenta odpowiada zgodzie podmiotu danych określonej w dyrektywie 95/46/WE".

Oznacza to, że w każdej sytuacji, gdy na mocy dyrektywy o prywatności i łączności elektronicznej wymagana jest zgoda, kryteria służące ustaleniu, czy zgoda jest ważna, są takie same, jak określone w dyrektywie 95/46/WE, a mianowicie zgodne z definicją w art. 2 lit. h) oraz szczegółowymi warunkami określonymi w art. 7 lit. a). Pogląd, że zgoda na mocy dyrektywy o prywatności i łączności elektronicznej musi być interpretowana w powiązaniu z art. 2 lit. h) oraz art. 7 lit. a) łącznie, potwierdza treść motywu 17[41].

III.B.2. Artykuł 5 ust. 1 – Czy jest niezbędna zgoda jednej czy też dwóch stron

„[…] zgody zainteresowanych użytkowników […]"

Artykuł 5 ust. 1 dyrektywy o prywatności i łączności elektronicznej chroni poufność komunikacji, zabraniając wszelkiego przejęcia lub nadzoru komunikatu bez zgody wszystkich zainteresowanych użytkowników.

W tym przypadku w art. 5 ust. 1 wymagana jest zgoda „wszystkich zainteresowanych użytkowników", a więc innymi słowy obydwu stron komunikacji. Zgoda jednej ze stron nie wystarcza.

Opracowując Opinię 2/2006[42], Grupa Robocza Art. 29 przeanalizowała kilka usług związanych ze skanowaniem treści wiadomości e-mail oraz w niektórych przypadkach śledzeniem otwierania wiadomości e-mail. Grupa Robocza wyraziła zaniepokojenie faktem, że w przypadku takich usług jedna ze stron komunikacji nie jest informowana.

---

41 Stwierdza się w nim: „Do celów niniejszej dyrektywy, zgoda […] powinna mieć to samo znaczenie co zgoda podmiotu danych opisana i szerzej określona w dyrektywie 95/46/WE".

42 Opinia 2/2006 dotycząca kwestii prywatności w związku ze świadczeniem usług skanowania wiadomości elektronicznych, przyjęta w dniu 21 lutego 2006 r. (WP 118).

Aby zapewnić zgodność takich usług z przepisem art. 5 ust. 1, niezbędna jest zgoda obydwu stron komunikacji.

III.B.3. Artykuł 6 ust. 3, art. 9, art. 13 i art. 5 ust. 3 – Moment, w którym należy uzyskać zgodę

„[…] po otrzymaniu jasnych i wyczerpujących informacji […]"

Pewne przepisy dyrektywy o prywatności i łączności elektronicznej zawierają wyraźne lub dorozumiane sformułowania wskazujące, że zgodę należy uzyskać przed przetwarzaniem. Jest to zgodne z dyrektywą 95/46/WE.

W art. 6 ust. 3 dyrektywy o prywatności i łączności elektronicznej zawarto wyraźne odniesienie do uprzedniej zgody abonenta lub użytkownika, ustanawiając obowiązek przedstawienia informacji i uzyskania uprzedniej zgody przed przetwarzaniem danych o ruchu do celów wprowadzania na rynek usług łączności elektronicznej lub usług tworzących wartość wzbogaconą. W przypadku pewnych rodzajów usług zgodę można uzyskać od abonenta w chwili dokonywania subskrypcji usług. W innych przypadkach może być możliwe uzyskanie zgody bezpośrednio od użytkownika. Podobne podejście przyjęto w art. 9 w odniesieniu do przetwarzania danych dotyczących lokalizacji innych niż dane o ruchu. Dostawca usług musi poinformować użytkowników lub abonentów – *przed uzyskaniem ich zgody* – o rodzaju danych dotyczących lokalizacji innych niż dane o ruchu, które *będą* przetwarzane. W art. 13 ustanawia się wymóg uzyskania uprzedniej zgody abonentów w celu wykorzystywania automatycznych systemów wywołujących bez ludzkiej ingerencji, faksów lub poczty elektronicznej do celów marketingu bezpośredniego.

W art. 5 ust. 3 określono szczegółowe zasady dotyczące przechowywania informacji lub uzyskania dostępu do informacji przechowywanych w urządzeniu końcowym użytkownika, w tym do celów śledzenia aktywności internetowej użytkownika. Chociaż w art. 5 ust. 3 nie pojawia się słowo „uprzednia", w jasny i oczywisty sposób wynika to z brzmienia przepisu.

Rozsądne jest uzyskanie zgody *przed* rozpoczęciem przetwarzania danych. W przeciwnym wypadku przetwarzanie odbywające się w okresie od chwili jego rozpoczęcia do chwili uzyskania zgody byłoby niezgodne z prawem ze względu na brak podstawy prawnej. Ponadto w takich przypadkach, jeżeli osoba fizyczna nie wyraziłaby zgody, wszelkie przetwarzanie danych, do którego już doszło, byłoby niezgodne z prawem z tego samego powodu.

Z powyższego wynika, że we wszystkich sytuacjach, w których *wymagana* jest zgoda, trzeba ją uzyskać przed rozpoczęciem przetwarzania danych. Możliwość rozpoczęcia przetwarzania bez uzyskania uprzednio zgody jest zgodna z prawem tylko wtedy, gdy dyrektywa o ochronie danych lub dyrektywa o prywatności i łączności elektronicznej nie wymaga zgody, ale określa alternatywną podstawę i odnosi się do prawa sprzeciwu lub odmowy przetwarzania. Mechanizmy te są wyraźnie odróżniane od zgody. W takich przypadkach przetwarzanie danych mogło się już rozpocząć, a osoba fizyczna ma prawo do sprzeciwu lub odmowy.

Stosowny przykład można znaleźć w art. 5 ust. 3 poprzedniej dyrektywy o prywatności i łączności elektronicznej, w której stwierdza się (podkreślenie własne): „korzystanie z sieci łączności elektronicznej w celu przechowywania informacji lub uzyskania dostępu do informacji przechowanej na terminalu abonenta lub użytkownika jest dozwolone wyłącznie pod warunkiem że abonent lub użytkownik otrzyma jasną i wyczerpującą informację zgodnie z dyrektywą 95/46/WE, między innymi o celach przetwarzania, oraz zostanie zaoferowane mu prawo do odmówienia zgody na takie przetwarzanie przez kontrolera danych". To sformułowanie należy porównać z nowym brzmieniem art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej zmienionej dyrektywą 2009/136/WE[43], w którym stwierdza się: „(…) przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika było dozwolone wyłącznie pod warunkiem że dany abonent lub użytkownik wyraził zgodę (…)". Konsekwencje tej zmiany w brzmieniu art. 5 ust. 3 Grupa Robocza Art. 29 wyjaśniła w Opinii 2/2010 w sprawie internetowej reklamy behawioralnej[44]. Różnicę między odmową a zgodą szerzej omawia się również w następnym rozdziale.

W wielu przypadkach, w których w dyrektywie o prywatności i łączności elektronicznej lub w dyrektywie o ochronie danych przewidziano możliwość odmowy przyzwolenia na przetwarzanie danych osobowych, jest tak, gdyż podstawa prawna początkowego przetwarzania danych jest *inna* niż zgoda – może być nią np. istniejąca umowa. Zostało to dokładniej zilustrowane w kolejnym podrozdziale, który dotyczy art. 13 dyrektywy o prywatności i łączności elektronicznej.

III.B.4. Artykuł 13 ust. 2 i 3 – prawo sprzeciwu oraz jego odróżnienie od zgody

„(…) klienci zostali jasno i wyraźnie poinformowani o możliwości sprzeciwienia się […]"

W art. 13 dyrektywy o prywatności i łączności elektronicznej umożliwiono posłużenie się zgodą w celu legalnego przesyłania komunikatów elektronicznych do celów marketingu bezpośredniego. Wykorzystano w tym celu standardową zasadę i przepis szczególny.

W przypadku użycia automatycznych systemów wywołujących, faksów i poczty elektronicznej niezbędne jest uzyskanie uprzedniej zgody osoby, której dane dotyczą.

Jeżeli adresat komunikatu handlowego jest istniejącym klientem, a celem komunikatu jest promocja własnych produktów lub usług usługodawcy bądź podobnych produktów lub usług, nie jest wymagana zgoda, ale zapewnienie, aby osoby fizyczne „zostały (…) poinformowane o możliwości sprzeciwienia się" (art. 13 ust. 2). W motywie 41

[43] Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE 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, tekst mający znaczenie dla EOG, Dz.U. L 337 z 18.12.2009, s. 11–36.

[44] Opinia z dnia 22 czerwca 2010 r., WP 171: kwestię, czy zgodę można wyrazić „przez zastosowanie odpowiednich ustawień w przeglądarce lub innej aplikacji" (motyw 66 dyrektywy 2009/136/WE), omówiono wyraźnie w pkt. 4.1.1. dokumentu WP 171.

wyjaśnia się, dlaczego prawodawca nie wymaga zgody w tym przypadku: „W kontekście istniejącej relacji z klientem, uzasadnione staje się zezwolenie wykorzystywania szczegółowych elektronicznych danych kontaktowych w celu oferowania podobnych produktów lub usług". Tak więc co do zasady podstawą prawną umożliwiającą pierwszy kontakt za pośrednictwem poczty elektronicznej jest stosunek umowny pomiędzy osobą fizyczną a usługodawcą. Osoby fizyczne powinny jednak mieć możliwość wyrażenia sprzeciwu wobec dalszych kontaktów. Jak Grupa Robocza wskazała już wcześniej: „Możliwość tę należy nadal oferować w każdej kolejnej wiadomości służącej marketingowi bezpośredniemu i powinna ona być bezpłatna, za wyjątkiem kosztów przesłania odmowy"[45].

Potrzebę uzyskania zgody należy odróżnić od prawa sprzeciwu. Jak wskazano powyżej w Rozdziale III.A.2, zgoda oparta na braku działania osoby fizycznej, na przykład poprzez domyślnie zaznaczone pola wyboru, nie spełnia wymagań ważnej zgody na mocy dyrektywy 95/46/WE. Ten sam wniosek dotyczy ustawień przeglądarki, przy których domyślnie akceptowane byłyby działania skierowane do użytkownika (za pośrednictwem plików *cookie*). Wyraźnie wynika to z nowego brzmienia art. 5 ust. 3 cytowanego powyżej w Rozdziale III.B.3. W tych dwóch przykładach nie są w szczególności spełnione wymogi jednoznacznego wskazania woli. Osoba, której dane dotyczą, musi mieć możliwość podjęcia decyzji i jej wyrażenia, na przykład przez samodzielne zaznaczenie pola wyboru, w obliczu celu przetwarzania danych.

W swojej opinii w sprawie reklamy behawioralnej Grupa Robocza stwierdziła: „wydaje się, że zasadnicze znaczenie ma wprowadzenie w przeglądarkach domyślnych ustawień chroniących prywatność. Innymi słowy, powinny mieć skonfigurowaną opcję »nieprzyjmowania plików *cookie* osób trzecich i nieprzekazywania pochodzących z nich informacji«. W celu uzupełnienia i zwiększenia skuteczności tego środka, przeglądarki powinny wymagać od użytkowników zastosowania kreatora ustawień prywatności, kiedy po raz pierwszy instalują bądź aktualizują przeglądarkę oraz zapewnienia możliwości łatwego dokonywania wyboru podczas użytkowania"[46].

III.B.5. Artykuł 6 ust. 3, art. 9 ust. 3 i 4 – możliwość odwołania zgody

„[…] w każdej chwili możliwość odwołania swojej zgody […]"

Możliwość odwołania zgody, która jest dorozumiana w dyrektywie 95/46/WE, zapisano w przepisach dyrektywy o prywatności i łączności elektronicznej. Wyraźnie wskazano to w Opinii Grupy Roboczej w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną[47]:

Na mocy art. 9 dyrektywy 2002/58/WE osoby, które wyraziły zgodę na przetwarzanie danych dotyczących lokalizacji innych niż dane o ruchu, mogą w dowolnym czasie wycofać tę zgodę i muszą mieć możliwość prostego i nieodpłatnego czasowego wycofania zgody na przetwarzanie tych danych. Grupa robocza uważa te prawa – które można traktować jako wykonanie prawa do wyrażenia sprzeciwu wobec przetwarzania danych dotyczących lokalizacji – jako mające zasadnicze znaczenie z punktu widzenia

[45] Opinia 5/2004 w sprawie niezamówionych komunikatów do celów marketingu zgodnie z art. 13 dyrektywy 2002/58/WE, przyjęta w dniu 27 lutego 2004 r.

[46] Opinia z dnia 22 czerwca 2010 r., WP 171, *op. cit.*

[47] Opinia 5/2005 w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną przyjęta w dniu 25 listopada 2005 r. (WP 115).

delikatnej natury danych dotyczących lokalizacji. Grupa robocza wyraża przekonanie, że warunkiem koniecznym dla wykonania tych praw jest stałe informowanie osób, i to nie tylko wówczas, gdy składają zapotrzebowanie na usługę, lecz także w czasie, gdy z niej korzystają. W odniesieniu do usług wymagających ciągłego przetwarzania danych dotyczących lokalizacji grupa robocza reprezentuje pogląd, że ich dostawca powinien regularnie przypominać zainteresowanej osobie, że jej urządzenie końcowe zostało, będzie lub może być zlokalizowane. Umożliwi to tej osobie wykonanie prawa do wycofania zgody na mocy art. 9 dyrektywy 2002/58/WE, jeżeli będzie chciała z niego skorzystać.

Jak wspomniano już powyżej, oznacza to, że odwołanie zgody dotyczy przyszłości, nie zaś przetwarzania danych, które miało miejsce w przeszłości, w okresie, w którym dane gromadzono w sposób legalny. Dlatego też uprzednio podjętych decyzji ani procesów wdrożonych na podstawie tych informacji nie można po prostu anulować. Jeżeli jednak nie istnieje inna podstawa prawna uzasadniająca dalsze przechowywanie danych, administrator danych powinien je usunąć.

IV. Wnioski

W niniejszej opinii przeanalizowano ramy prawne wykorzystania zgody na mocy dyrektywy 95/46/WE i dyrektywy 2002/58/WE. Cel opinii jest dwojaki: po pierwsze, jest nim wyjaśnienie istniejących wymogów prawnych i zilustrowanie tego, jak funkcjonują one w praktyce. Po drugie, w opinii przedstawiono przemyślenia dotyczące dalszej przydatności istniejących ram prawnych w świetle licznych nowych sposobów przetwarzania danych osobowych oraz ewentualnej potrzeby zmiany tych ram.

IV.1. Wyjaśnienie najważniejszych aspektów obecnych ram

W art. 2 lit. h) dyrektywy 95/46/WE zdefiniowano zgodę jako „konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych". W art. 7 dyrektywy, która określa podstawę prawną przetwarzania danych osobowych, jako jedną z podstaw prawnych określa się *jednoznaczną* zgodę. W art. 8 wymaga się *wyraźnej* zgody jako podstawy prawnej przetwarzania danych szczególnie chronionych. W art. 26 ust. 1 dyrektywy 95/46/WE i niektórych przepisach dyrektywy o prywatności i łączności elektronicznej wymaga się zgody w celu prowadzenia określonych czynności przetwarzania danych w zakresie stosowania tych przepisów. Celem rozwinięcia w tej opinii pewnych zagadnień jest wyjaśnienie poszczególnych elementów ram prawnych, aby generalnie ułatwić ich stosowanie przez zainteresowane strony.

Elementy/spostrzeżenia o charakterze ogólnym

- Zgoda jest jedną z sześciu podstaw prawnych przetwarzania danych osobowych (jedną z pięciu w przypadku danych szczególnie chronionych); jest ona podstawą ważną, gdyż daje osobie, której dane dotyczą, pewną kontrolę nad przetwarzaniem jej danych. Znaczenie zgody jako elementu autonomii i samostanowienia osoby fizycznej zależy od jej wykorzystania we właściwym kontekście i wraz z niezbędnymi elementami.

- Ogólnie rzecz biorąc, ramy prawne określone w dyrektywie 95/46/WE mają zastosowanie, gdy tylko jakikolwiek podmiot ubiega się o zgodę, niezależnie od tego, czy dzieje się to w środowisku *off-line*, czy też *on-line*. Na przykład jeżeli tradycyjny (niedziałający w Internecie) detalista prowadzi zapisy do programu lojalnościowego przy wykorzystaniu papierowego formularza, zastosowanie mają te same reguły, jak w przypadku podmiotu czyniącego to samo za pośrednictwem strony internetowej. Ponadto w dyrektywie o prywatności i łączności elektronicznej wskazano pewne czynności przetwarzania danych, w przypadku których wymagana jest zgoda: dotyczą one głównie przetwarzania danych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej. Wymagania warunkujące ważność zgody w dyrektywie 2002/58/WE są takie same, jak w dyrektywie 95/46/WE.

- Sytuacji, w których administratorzy danych korzystają ze zgody jako podstawy prawnej przetwarzania danych osobowych, nie należy mylić z sytuacjami, w których administrator danych opiera przetwarzanie na innych podstawach prawnych, które wiążą się z prawem sprzeciwu osoby fizycznej. Może tak być na przykład, gdy przetwarzanie odbywa się w związku z „uzasadnionymi interesami" administratora danych (art. 7 lit. f) dyrektywy 95/46/WE), ale osobie fizycznej przysługuje prawo sprzeciwu (art. 14 lit. a) dyrektywy 95/46/WE). Kolejny przykład dotyczy sytuacji, w której administrator danych wysyła komunikaty przy użyciu poczty elektronicznej do istniejących klientów w celu promowania swoich własnych bądź podobnych produktów lub usług; osobom fizycznym przysługuje jednak prawo sprzeciwu na mocy art. 13 ust. 2 dyrektywy 2002/58/WE. W obydwu przypadkach osoba, której dane dotyczą, ma prawo sprzeciwić się przetwarzaniu, co nie jest tożsame ze zgodą.

- Poleganie na zgodzie przy przetwarzaniu danych osobowych nie zwalnia administratora danych z obowiązku spełnienia pozostałych wymogów określonych w ramach prawnych ochrony danych, jak na przykład przestrzegania zasady proporcjonalności na mocy art. 6 ust. 1 lit. c), bezpieczeństwa przetwarzania, o którym mowa w art. 17 itp.

- Ważna zgoda opiera się na założeniu zdolności osoby fizycznej do jej wyrażenia. Zasady dotyczące zdolności do wyrażenia zgody nie są zharmonizowane, w związku z czym mogą się różnić w poszczególnych państwach członkowskich.

- Osoby, które wyraziły zgodę, powinny mieć możliwość jej odwołania, co zapobiegnie dalszemu przetwarzaniu ich danych. Potwierdzono to również w dyrektywie o prywatności i łączności elektronicznej w odniesieniu do konkretnych czynności przetwarzania danych na podstawie zgody, jak na przykład przetwarzania danych dotyczących lokalizacji innych niż dane o ruchu.

- Zgoda musi zostać udzielona przed rozpoczęciem przetwarzania danych osobowych, ale może być też wymagana w trakcie przetwarzania, jeżeli pojawia się nowy cel. Podkreśla się to w różnych przepisach dyrektywy 2002/58/WE poprzez wymóg „uprzedniej" zgody (np. w art. 6 ust. 3) lub też wynika to z brzmienia tych przepisów (np. art. 5 ust. 3).

Poszczególne elementy ram prawnych związanych ze zgodą

- Aby zgoda była ważna, musi być *dobrowolna*. Oznacza to, że nie może zachodzić ryzyko wprowadzenia w błąd, zastraszenia lub znaczących negatywnych

konsekwencji dla osoby, której dane dotyczą, jeżeli nie wyrazi ona zgody. W przypadku czynności przetwarzania danych w środowisku pracy, w którym występuje element podległości, jak też w kontekście usług publicznych takich jak opieka zdrowotna, może być wymagana wnikliwa ocena, czy zgoda osób fizycznych jest dobrowolna.

- Zgoda musi być *konkretna*. Wymogu tego nie spełnia ogólna zgoda bez określenia dokładnych celów przetwarzania. W związku z tym zamiast zamieszczenia informacji w ogólnych warunkach umowy wymagane jest zastosowanie specjalnych klauzul zgody odrębnych od ogólnych warunków.

- Zgoda musi być *świadoma*. W art. 10 i 11 dyrektywy wymieniono rodzaj informacji, które trzeba przedstawić osobom fizycznym. Podane informacje muszą być w każdym przypadku wystarczające w celu zagwarantowania, że osoby fizyczne mogą podjąć świadome decyzje dotyczące przetwarzania ich danych osobowych. Potrzeba „świadomej" zgody przekłada się na dwa dodatkowe wymagania. Po pierwsze, informacje trzeba przedstawić z wykorzystaniem odpowiedniego języka, aby osoby, których dane dotyczą, rozumiały, na co się zgadzają, i do jakich celów. Jest to kwestią kontekstu. Wykorzystanie zbyt skomplikowanego żargonu prawnego lub technicznego nie spełnia wymogów prawnych. Po drugie, informacje przedstawione użytkownikom powinny być jasne i wystarczająco widoczne, aby użytkownicy nie mogli ich przeoczyć. Informacje trzeba dostarczyć bezpośrednio osobom fizycznym. Nie wystarcza, aby były tylko gdzieś dostępne.

- Jeżeli chodzi o sposób wyrażenia zgody, w art. 8 ust. 2 lit. a) wymaga się na przetwarzanie danych szczególnie chronionych *wyraźnej* zgody, co oznacza aktywną reakcję ustną lub na piśmie, za pośrednictwem której osoba fizyczna wyraża swoją wolę, aby jej dane były przetwarzane w określonych celach. W związku z tym wyraźnej zgody nie można uzyskać, zamieszczając domyślnie zaznaczone pole wyboru. Osoba, której dane dotyczą, musi podjąć konkretne działanie oznaczające zgodę i musi mieć możliwość jej nieudzielenia.

- W przypadku danych nienależących do szczególnie chronionych wymagana jest (art. 7 lit. a)) zgoda *jednoznaczna*. „Jednoznaczność" wymaga posłużenia się w celu uzyskania zgody mechanizmami niepozostawiającymi wątpliwości co do zamiaru wyrażenia zgody przez osobę fizyczną. W praktyce wymaganie to pozwala administratorom danych wykorzystać w celu uzyskania zgody różne rodzaje mechanizmów od oświadczeń wyrażających przyzwolenie (wyraźna zgoda) po mechanizmy oparte na działaniach, których celem jest wyrażenie przyzwolenia.

- Zgoda bazująca na bezczynności lub milczeniu nie stanowi zazwyczaj ważnej zgody, zwłaszcza w kontekście internetowym. To zagadnienie pojawia się w szczególności w odniesieniu do wykorzystania domyślnych ustawień, które osoba, której dane dotyczą, musi zmodyfikować, aby odmówić przetwarzania. Tak jest na przykład w przypadku domyślnie zaznaczonych pól wyboru lub ustawień przeglądarki internetowej, która domyślnie gromadzi dane.

IV.2 Ocena obecnych ram i ewentualnych potrzeb zmian

Ocena ogólna

Zdaniem Grupy Roboczej obecne ramy ochrony danych zawierają przemyślany zestaw zasad ustanawiających warunki ważności zgody jako podstawy legalności czynności przetwarzania danych. Zasady te mają zastosowanie zarówno w środowisku *off-line*, jak i *on-line*. W szczególności:

Ramy prawne udało się w pewnych aspektach należycie zrównoważyć. Z jednej strony gwarantują one, że za zgodę uznawana jest tylko zgoda rzeczywista i świadoma. Pod tym względem wyraźne wymagania art. 2 lit. h), aby zgoda była dobrowolna, konkretna i świadoma, są istotne i zadowalające. Z drugiej strony wymóg ten nie ma charakteru sztywnego, ale zapewnia wystarczającą elastyczność, unikając reguł odnoszących się do konkretnych technologii. Ilustruje to ten sam art. 2 lit. h), gdzie zgodę definiuje się jako dowolne wskazanie woli osoby fizycznej. Zapewnia to wystarczające pole manewru co do sposobu, w jaki wskazanie to może zostać dokonane. W art. 7 i 8, w których wymaga się odpowiednio zgody jednoznacznej oraz wyraźnej, uchwycono we właściwy sposób konieczność zachowania równowagi między tymi dwoma aspektami, a więc zapewnienia elastyczności i unikania zbyt sztywnych struktur, a zarazem zagwarantowania ochrony.

Wynikiem są ramy, których prawidłowe zastosowanie i wdrożenie umożliwi dotrzymanie kroku szerokiej gamie czynności przetwarzania danych, które są często wynikiem rozwoju technicznego.

W praktyce jednak ustalenie, kiedy niezbędna jest zgoda, a w szczególności jakie są wymogi dotyczące ważnej zgody i jak należy stosować je w praktyce, nie zawsze jest łatwe ze względu na niejednolite regulacje w państwach członkowskich. Wdrożenie na szczeblu krajowym poskutkowało różniącymi się podejściami. Konkretne niedociągnięcia wskazano podczas dyskusji prowadzonych w Grupie Roboczej Art. 29 w związku z opracowywaniem niniejszej opinii. Przedstawiono je bardziej szczegółowo poniżej.

Możliwe zmiany

- Pojęcie jednoznacznej zgody jest przydatnym składnikiem systemu nie nazbyt sztywnego, ale zapewniającego dobrą ochronę. Choć może ono prowadzić do stworzenia racjonalnego systemu, bywa ono niestety często niewłaściwie rozumiane lub po prostu ignorowane. Chociaż powyższe wskazania i przykłady powinny przyczynić się do zwiększenia pewności prawnej i poprawy ochrony praw osób fizycznych w przypadkach, gdy zgoda jest wykorzystywana jako podstawa prawna, sytuacja ta wydaje się wymagać pewnych zmian.
- W szczególności zdaniem Grupy Roboczej Art. 29 samo sformułowanie („jednoznaczna") należałoby uczynić jaśniejszym podczas rewizji ogólnych ram ochrony danych. Celem wyjaśnienia powinno być podkreślenie, że jednoznaczna zgoda wymaga użycia mechanizmów niepozostawiających wątpliwości co do zamiaru wyrażenia zgody przez osobę, której dane dotyczą. Jednocześnie należy jasno wskazać, że wykorzystanie domyślnych ustawień, które osoba, której dane dotyczą, musi zmodyfikować, aby odmówić przetwarzania (zgoda oparta na milczeniu), nie stanowi samo w sobie jednoznacznej zgody. Jest tak zwłaszcza w środowisku internetowym.

- Oprócz opisanych powyżej wyjaśnień Grupa Robocza Art. 29 przedstawia następujące sugestie:

    i) *Po pierwsze*, w definicji zgody w art. 2 lit. h) powinno znaleźć się słowo „jednoznaczne" (lub równoważne) w celu podkreślenia, że ważna jest wyłącznie zgoda oparta na oświadczeniach lub działaniach wyrażających przyzwolenie. Oprócz zwiększenia przejrzystości skutkowałoby to dostosowaniem definicji zgody w art. 2 lit. h) do wymagań dotyczących ważnej zgody na mocy art. 7. Ponadto znaczenie słowa „jednoznaczny" można byłoby bardziej szczegółowo objaśnić w jednym z motywów przyszłego aktu prawnego.

    ii) *Po drugie*, w kontekście ogólnego obowiązku rozliczalności administratorzy danych powinni być w stanie wykazać, że uzyskali zgodę. W samej rzeczy, jeżeli zostanie wzmocniona zasada ciężaru dowodu, co nałoży na administratorów danych obowiązek wykazania, że skutecznie uzyskali zgodę osoby, której dane dotyczą, będą oni zmuszeni wdrożyć standardowe praktyki i mechanizmy uzyskiwania oraz dowodzenia jednoznacznej zgody. Rodzaj tych mechanizmów będzie zależny od kontekstu i powinien uwzględniać charakterystykę oraz okoliczności przetwarzania, a w szczególności ryzyko z nim związane.

- Grupa Robocza Art. 29 nie jest przekonana, czy ramy prawne powinny co do zasady zawierać wymaganie wyraźnej zgody w odniesieniu do wszystkich rodzajów czynności przetwarzania, w tym również objętych obecnie art. 7 dyrektywy. Zdaniem Grupy obowiązującą normą powinna pozostać jednoznaczna zgoda, która obejmuje wyraźną zgodę, ale też zgodę wynikającą z jednoznacznych *działań*. Umożliwia to administratorom danych większą elastyczność w uzyskiwaniu zgody, a cała procedura może być szybsza i przyjaźniejsza dla użytkownika.

- Niektóre aspekty ram prawnych dotyczące zgody wywnioskowano z brzmienia przepisów i historii uregulowań prawnych lub też zostały one wypracowane w orzecznictwie oraz opiniach Grupy Roboczej Art. 29. Większą pewność prawną zapewniłoby wyraźne zamieszczenie tych aspektów w nowych ramach legislacyjnych ochrony danych. Pod uwagę można byłoby wziąć następujące kwestie:

    i) Uwzględnienie wyraźnej klauzuli ustanawiającej prawo osoby fizycznej do odwołania zgody.

    ii) Podkreślenie faktu, że zgoda musi zostać udzielona przed rozpoczęciem przetwarzania lub przed jakimkolwiek dalszym wykorzystaniem danych do celów nieobjętych pierwotną zgodą w przypadkach, gdy nie istnieje inna podstawa prawna przetwarzania.

    iii) Uwzględnienie wyraźnych wymogów dotyczących jakości (obowiązek przedstawienia informacji na temat przetwarzania danych w łatwo zrozumiały sposób, jasnym i prostym językiem) oraz dostępności informacji (obowiązek zadbania, aby informacje były widoczne, rzucały się w oczy i były bezpośrednio dostępne). Jest to niezbędne,

aby umożliwić osobom fizycznym podejmowanie świadomych decyzji.

- Wreszcie, w odniesieniu do osób fizycznych nieposiadających pełnej zdolności do czynności prawnych można byłoby wprowadzić przepisy zapewniające lepszą ochronę, w tym:

  i) Wyjaśnienia dotyczące okoliczności, w których wymagana jest zgoda rodziców lub przedstawicieli ustawowych osoby fizycznej nieposiadającej pełnej zdolności do czynności prawnych, w tym określenie granicy wieku, poniżej której taka zgoda byłaby obowiązkowa.

  ii) Ustanowienie obowiązku wykorzystywania mechanizmów weryfikacji wieku, które mogą być uzależnione od okoliczności takich jak wiek dziecka, rodzaj przetwarzania danych, podwyższone ryzyko, oraz to, czy informacje będą przechowywane przez administratora danych, czy też udostępniane osobom trzecim.

  iii) Obowiązek dostosowania informacji skierowanych do dzieci w sposób ułatwiający im zrozumienie, co oznacza gromadzenie danych pochodzących od nich, a tym samym wyrażenie zgody.

  iv) Konkretne zabezpieczenia wskazujące czynności przetwarzania danych, jak na przykład reklama behawioralna, w przypadku których zgoda nie powinna być możliwą podstawą legalnego przetwarzania danych osobowych.

Grupa Robocza Art. 29 powróci w przyszłości do zagadnienia zgody. Krajowe organy ochrony danych oraz Grupa Robocza mogą w szczególności podjąć na późniejszym etapie decyzję o opracowaniu wytycznych rozwijających niniejszą opinię, w których zawarte zostaną dodatkowe przykłady praktyczne odnoszące się do wykorzystania zgody.

Sporządzono w Brukseli dnia 13 lipca 2011 r.

W imieniu Grupy Roboczej

Przewodniczący
Jacob KOHNSTAMM