



01197/11/EN
WP187

Opinia 15/2011 w sprawie definicji zgody

Przyjęta w dniu 13 lipca 2011 r.

Grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określa art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro nr MO-59 06/036.

Strona internetowa: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Streszczenie

Opinia przedstawia dogłębną analizę pojęcia zgody obecnie stosowanego w dyrektywie o ochronie danych oraz dyrektywie o prywatności i łączności elektronicznej. Korzystając z doświadczenia członków Grupy Roboczej Artykułu 29, Opinia przedstawia liczne przykłady ważnej i nieważnej zgody, skupiając się na jej kluczowych elementach, takich jak znaczenie sformułowań: „wskazanie”, „dobrowolna”, „konkretna”, „jednoznaczna”, „wyraźna”, „świadoma”, etc. Opinia wyjaśnia bardziej szczegółowo niektóre aspekty związane z pojęciem zgody, na przykład kwestię terminu, w jakim należy uzyskać zgodę, czym różni się prawo do wyrażenia sprzeciwu od zgody, etc.

Zgoda jest jedną z kilku podstaw prawnych przetwarzania danych osobowych. Odgrywa ważną rolę, ale nie wyłącza możliwości, w zależności od kontekstu, aby inne podstawy prawne były bardziej odpowiednie, zarówno z punktu widzenia administratora, jak i osoby, której dane dotyczą. Jeżeli jest właściwie wykorzystywana, zgoda jest narzędziem dającym osobie, której dane dotyczą, możliwość kontroli nad przetwarzaniem jej danych osobowych. Jeśli jest niewłaściwie wykorzystywana, kontrola przez osobę, której dane dotyczą, staje się iluzją, a zgoda stanowi nieodpowiednią podstawę przetwarzania.

Opinię tę wydaje się częściowo w odpowiedzi na prośbę Komisji w kontekście trwającego przeglądu dyrektywy o ochronie danych. W związku z tym zawiera ona zalecenia, które powinny być uwzględnione w przeglądzie, obejmujące:

- (i) wyjaśnienie znaczenia pojęcia „jednoznacznej” zgody oraz wyjaśnienie, że tylko zgoda, która jest oparta na oświadczeniach lub działaniach oznaczających przyzwolenie, stanowi ważną zgodę;
- (ii) wymaganie od administratorów danych wprowadzenia mechanizmów wyrażania zgody (w ramach ogólnego obowiązku rozliczalności);
- (iii) dodanie wyraźnego wymogu dotyczącego jakości i dostępności informacji stanowiących podstawę zgody, oraz
- (iv) szereg sugestii dotyczących nieletnich oraz innych osób fizycznych nie posiadających 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 i 30 ust. 1 lit. a) i ust. 3 wspomnianej dyrektywy,

uwzględniając swój regulamin,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. Wprowadzenie

Zgoda osoby, której dane dotyczą, od zawsze była kluczowym pojęciem w dziedzinie ochrony danych, ale nie zawsze było jasne, czy zgoda jest potrzebna, oraz jakie warunki muszą być spełnione, aby zgoda była ważna. Może to prowadzić do różnych podejść oraz rozbieżnych poglądów w zakresie dobrych praktyk pomiędzy państwami członkowskimi. Może to osłabić pozycję (warunki) osób, których dane dotyczą. Problem ten staje się bardziej poważny, jako że przetwarzanie danych osobowych staje się coraz ważniejszą cechą nowoczesnego społeczeństwa, zarówno w środowisku *on-line*, jak i *off-line*, często dotycząc różnych państw członkowskich. Z tego względu Grupa Robocza Artykułu 29, w ramach swojego Programu prac na lata 2010-2011, postanowiła dokładnie przyjrzeć się temu tematowi.

Zgoda jest również jednym z tematów, na jaki Komisja poprosiła o wkład w kontekście przeglądu dyrektywy 95/46/WE. Komunikat Komisji „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”¹ mówi, że: „Komisja zbada możliwości wyjaśnienia i udoskonalenia przepisów dotyczących zgody”. W Komunikacie zostało to wyjaśnione² 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 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.”

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

² Pierwszy raport Komisji z wdrożenia dyrektywy o ochronie danych ((95/46/WE) (KOM(2003)265 wersja ostateczna, już wspomniany na stronie 17: „Pojęcie 'jednoznacznej zgody' (artykuł 7(a)) w szczególności w porównaniu z pojęciem 'wyraźnej zgody' w artykule 8, wymaga dalszych wyjaśnień oraz bardziej jednolitej interpretacji. Konieczne jest, aby operatorzy wiedzieli, co stanowi ważną zgodę, w szczególności w sytuacjach *on-line*.”

„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.”

W celu spełnienia prośbę Komisji o wkład oraz realizacji swojego Programu prac na lata 2010-2011, Grupa Robocza Artykułu 29 zobowiązała się do opracowania Opinii. Celem niniejszej Opinii jest wyjaśnienie zagadnień w celu zapewnienia jednolitej interpretacji istniejących ram prawnych. Jednocześnie w działaniu tym kieruje się logiką z wcześniejszych opinii w sprawie innych kluczowych przepisów dyrektywy³. Dokonanie ewentualnych zmian w istniejących ramach zajmie jakiś czas, zatem wyjaśnienie obecnego pojęcia „zgody” oraz jego głównych elementów ma swoje zalety. Wyjaśnienie istniejących przepisów pomoże również wskazać obszary, które wymagają poprawienia. Zatem, opierając się na przedmiotowej analizie, Opinia będzie starała się sformułować zalecenia dotyczące polityki (ang. *policy*), aby pomóc Komisji oraz twórcom polityk (ang. *policy makers*) przy rozważaniu zmian w stosowanych ramach prawnych ochrony danych.

Podstawowa treść Opinii kształtuje się następująco. Po przedstawieniu przeglądu historii legislacji oraz roli zgody w ustawodawstwie w zakresie ochrony danych, badane są różne elementy i wymogi dotyczące zgody, aby była ważna w świetle obowiązującego prawa, w tym niektórych istotnych części dyrektywy o prywatności i łączności elektronicznej 2002/58/WE. Analizie towarzyszą praktyczne przykłady oparte na doświadczeniach krajowych. Analiza ta potwierdza zalecenia, w ostatniej części tej Opinii, które mówią, że muszą istnieć określone elementy, aby uzyskać ważną zgodę w rozumieniu dyrektywy. Przedstawia także zalecenia w zakresie polityki dla twórców polityk do rozważenia w kontekście przeglądu dyrektywy 95/46/WE.

II. Ogólne spostrzeżenia i kwestie dotyczące polityki (ang. *policy issues*)

II.1. Historia w skrócie

Podczas gdy niektóre krajowe ustawy o ochronie danych/prywatności przyjęte w latach siedemdziesiątych przewidywały zgodę jako jedną z podstaw prawnych przetwarzania danych osobowych⁴, nie znalazło to odzwierciedlenia w Konwencji 108 Rady Europy⁵. Istnieją ewidentne powody, dla których zgoda nie odgrywa większej roli w Konwencji⁶.

Na poziomie UE poleganie na zgodzie jako kryterium legalności czynności przetwarzania danych osobowych przewidziano od samego początku procesu

³ Np. Opinia 8/2010 w sprawie prawa właściwego, przyjęta w dniu 16 lutego 2010 r. (WP 179) oraz Opinia 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający”, przyjęta w dniu 16 lutego 2010 r. (WP 169).

⁴ Patrz np. Artykuł francuskiej ustawy 78-17 z 6 stycznia 1978 - Loi n 78-17 "relative a l'informatique, aux fichiers et aux libertés".

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

⁶ Konwencja 108 wprowadziła pojęcia: „zgodne z prawem przetwarzanie” oraz „prawnie uzasadniony cel” (artykuł 5), ale w przeciwieństwie do dyrektywy 95/46/WE nie przewidziała listy kryteriów prawnie uzasadnionego przetwarzania. Zgoda osoby, której dane dotyczą, odgrywała rolę tylko w kontekście wzajemnej pomocy (artykuł 15). Jednak wymóg „zgody” był później wielokrotnie wspomniany w różnych rekomendacjach Komitetu Ministrów .

legislacyjnego, który zakończył się przyjęciem dyrektywy 95/46/WE. Artykuł 12 wniosku Komisji⁷ w 1990 r. określił cechy, jakie musiała posiadać zgoda, aby przesądzać o legalności czynności przetwarzania danych: musiała być „wyraźna” i „konkretna”. Art. 17, dotyczący danych szczególnie chronionych, wymagał, aby zgoda była „wyraźna i pisemna”. Zmieniony wniosek Komisji⁸ w 1992 r. wprowadził tekst bliski definicji „zgody osoby, której dane dotyczą” w dzisiejszym artykule 2 lit. g), zastępującym art. 12. Według niego zgoda musiała być „dobrowolna i konkretna”. Określenie „wyraźna” zastąpiono, określając zgodę jako „wyraźne wskazanie przez nią (osobę, której dane dotyczą) na to, że...”. W Memorandum wyjaśniającym towarzyszącym wnioskowi zmienionemu w 1992 r.⁹ stwierdzono, że zgodę można udzielić ustnie bądź na piśmie. W przypadku danych szczególnie chronionych zachowano wymóg „pisemnej” zgody. W 1992 r. zmieniony wniosek Komisji wprowadził zmiany w poprzednim wniosku i wprowadził art. 7 dotyczący podstaw prawnych przetwarzania. Art. 7 lit. a) przewidywał, że przetwarzanie mogłoby być prowadzone, jeżeli „osoba, której dane dotyczą, wyraziła na to zgodę”; pierwotna lista przesłanek obejmowała, tak jak dziś, pięć dodatkowych podstaw prawnych (poza zgodą), które można wykorzystać jako podstawy legalności przetwarzania danych.

Wspólne Stanowisko Rady¹⁰ w 1995 r. wprowadziło ostateczną (dzisiejszą) definicję zgody. Zgodę określono 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 odniesieniu do stanowiska Komisji z 1992 r. dotyczyła usunięcia słowa „wyraźne” (ang. *express*) poprzedzającego słowo „wskazanie”. Jednocześnie dodano słowo „jednoznacznie” do art. 7 lit. a), który brzmi następująco: „gdy osoba, której dane dotyczą, jednoznacznie wyraziła na to zgodę”. Wymóg pisemnej zgody w przypadku danych szczególnie chronionych zastąpiono „wyraźną zgodą”.

Wskazane przez Radę powody¹¹ nie wyjaśniły konkretnie tych zmian. Jednakże na stronie 4 stwierdzono, że „... dokonano... szeregu zmian... w celu wprowadzenia środka elastyczności, który gwarantuje równoważną ochronę... ale nie prowadzi do obniżenia poziomu ochrony; pozwalają one na stosowanie ogólnych zasad w skuteczny i niebiurokratyczny sposób, w zgodzie z szeregiem sposobów, przy zastosowaniu których... przetwarzane są dane.”

Rolę zgody wyraźnie uznano w Karcie Praw Podstawowych UE w części dotyczącej ochrony danych osobowych. W art. 8 ust. 2 wskazano, że dane osobowe mogą być przetwarzane „na podstawie zgody osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą”. W związku z tym zgoda jest uznawana za niezbędny aspekt podstawowego prawa do ochrony danych osobowych. Jednocześnie, zgodnie z Kartą zgoda nie jest jedyną podstawą pozwalającą na przetwarzanie danych osobowych;

⁷ Wniosek dotyczący dyrektywy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych, KOM (90), 314 wersja ostateczna, SYN 287 i 288, Bruksela, dnia 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, KOM (92) 422 FINAL- SYN 287, Bruksela, dnia 15 października 1992 r.

⁹ Patrz strona 11 zmienionego wniosku dotyczącego dyrektywy Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, KOM (92) 422 FINAL- SYN 287, Bruksela, dnia 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 Patrz strona 4 Wspólnego Stanowiska.

Karta wyraźnie uznaje, że prawo może przewidywać inne uzasadnione podstawy, co ma miejsce w przypadku dyrektywy 95/46/WE.

Podsumowując, historia legislacji, w szczególności w UE, pokazuje, że zgoda odgrywa ważną rolę w koncepcjach ochrony danych i prywatności. Jednocześnie wskazuje, że zgody nie uznawano za jedyną podstawę prawną upoważniającą do prowadzenia czynności przetwarzania danych. Historia legislacji dyrektywy 95/46/WE wskazuje na względny konsensus co do warunków ważnej zgody, a mianowicie ma ona być: *dobrowolna, konkretna i świadoma*. Jednakże wskazuje również na niepewność co do możliwych sposobów wyrażania zgody - czy musi być wyraźna, pisemna, etc. Poniżej kwestia ta poddana jest dalszej analizie.

II.2. Rola pojęcia: podstawa legalności

Ogólna/Szczególna podstawa:

Zgoda jest wykorzystywana w dyrektywie zarówno jako ogólna podstawa legalności (art. 7), jak i jako szczególna podstawa w określonych okolicznościach (art. 8 ust. 2 lit. a), art. 26 ust. 1 lit.a)). Art. 7 wymienia zgodę jako pierwszą z sześciu różnych podstaw legalności przetwarzania danych osobowych, podczas gdy art. 8 przewiduje możliwość wykorzystania zgody jako przesłanki legalności przetwarzania szczególnych kategorii danych (szczególnie chronionych), które w innym przypadku byłoby zabronione. W tym ostatnim przypadku standard dla uzyskania zgody jest wyższy, ponieważ zgoda ta musi przewyższać ogólny standard dla uzyskania zgody i być „wyraźna”.

Ponadto dyrektywa pozwala na interakcję z innymi przepisami, jak wspomniano 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”*. Sposób działania tego systemu w praktyce jest złożony: państwa członkowskie mają swoje własne podejścia i w niektórych przypadkach doprowadziło to do rozbieżności.

Pojęcie zgody nie zawsze było transponowane słowo w słowo na poziomie krajowym. Tytułem przykładu, zgoda jako ogólne pojęcie nie jest zdefiniowana we francuskim ustawodawstwie o ochronie danych, ale jej znaczenie zostało dokładnie i spójnie wyjaśnione w orzecznictwie organu ochrony danych (CNIL), w odniesieniu do definicji zawartej w dyrektywie o ochronie danych. W Zjednoczonym Królestwie pojęcie zgody zostało wypracowane w prawie zwyczajowym w odniesieniu do sformułowania zawartego w dyrektywie. Ponadto czasami zgodę wyraźnie definiowano w określonych sektorach, na przykład w kontekście e-prywatności, e-administracji czy e-zdrowia. W związku z tym pojęcie opracowane w przepisach szczególnych oraz pojęcie wypracowane w ogólnym ustawodawstwie o ochronie danych będą miały na siebie wzajemny wpływ.

Zgoda jest pojęciem stosowanym w innych dziedzinach prawa, szczególnie prawa zobowiązań umownych. W tym kontekście, w celu zapewnienia ważności umowy będą musiały zostać wzięte pod uwagę inne kryteria niż te wspomniane w dyrektywie, takie jak wiek, bezprawny nacisk, etc. Zakres prawa cywilnego oraz zakres dyrektywy nie są ze sobą w sprzeczności, tylko nakładają się na siebie: dyrektywa nie odnosi się do ogólnych warunków ważności zgody w kontekście prawa cywilnego, ale nie wyklucza

ich. Oznacza to na przykład, że w celu oszacowania ważności umowy w kontekście art. 7 lit. b) dyrektywy trzeba będzie wziąć pod uwagę wymogi prawa cywilnego. Poza zastosowaniem ogólnych warunków dla ważności zgody na mocy prawa cywilnego, zgodę wymaganą w art. 7 lit. a) należy również interpretować, biorąc pod uwagę art. 2 lit. h) dyrektywy.

To współdziałanie z innymi przepisami jest widoczne nie tylko na poziomie krajowym, ale również na poziomie europejskim. Podobne pojmowanie elementów dyrektywy wywnioskowano także z innych kontekstów, co pokazuje wyrok Trybunału Sprawiedliwości w obszarze prawa pracy¹²: wymagano zgody w kontekście rezygnacji z prawa społecznego. Trybunał zinterpretował pojęcie zgody w kontekście dyrektywy 93/104 dotyczącej niektórych aspektów organizacji czasu pracy. Trybunał stwierdził, że 'zgoda pracownika' wymagała zgody od pracownika (nie zgody związku w imieniu pracownika), i uznał, że „zgoda” (...) oznacza świadomą, dobrowolną zgodę. Stwierdził również, że pracownik podpisujący umowę zatrudnienia w odniesieniu do układu zbiorowego upoważniającego do przedłużenia czasu pracy nie spełnił wymogów, aby zgoda była wyrażona dobrowolnie i wyraźnie, przy pełnej znajomości wszystkich faktów. Ta interpretacja zgody w konkretnym kontekście jest bardzo bliska brzmieniu dyrektywy 95/46/WE.

Zgoda nie jest jedyną podstawą legalności

Dyrektywa wyraźnie przedstawia zgodę jako podstawę legalności. Jednakże niektóre państwa członkowskie postrzegają ją jako preferowaną podstawę, czasami bliską zasadzie konstytucyjnej, związanej ze statusem ochrony danych jako prawem podstawowym. Inne państwa członkowskie mogą postrzegać ją jako jedną z sześciu możliwości, jako wymóg operacyjny, który nie jest ważniejszy niż inne możliwości. Wyjaśnienie relacji zgody z innymi podstawami legalności – np. w odniesieniu do umów, zadań leżących w interesie publicznym czy też prawnie uzasadnionych interesów administratora danych, oraz prawa do wyrażenia sprzeciwu – pomoże podkreślić rolę zgody w określonych przypadkach.

Porządek, w jakim wymienione są podstawy prawne w art. 7, jest istotny, ale nie oznacza, że zgoda zawsze jest najbardziej odpowiednią podstawą legalności przetwarzania danych osobowych. Art. 7 rozpoczyna listę przesłanek od zgody, a następnie wymienia inne podstawy, w tym umowy i inne zobowiązania prawne, przechodząc stopniowo do zrównoważenia interesów. Należy zauważyć, że pięć pozostałych podstaw wymienionych po zgodzie wymaga przeprowadzenia testu „konieczności”, który ściśle ogranicza kontekst, w jakim mogą one mieć zastosowanie. Nie oznacza to, że wymóg zgody zostawia większy margines swobody działania niż inne podstawy wskazane w art. 7.

Ponadto, uzyskanie zgody nie neguje zobowiązań administratora danych wynikających z art. 6 dotyczących rzetelności, konieczności i proporcjonalności, jak również jakości danych. Na przykład, nawet jeżeli przetwarzanie danych osobowych oparte jest na zgodzie użytkownika, nie będzie to podstawą legalności gromadzenia danych, które są nadmierne w stosunku do określonego celu.

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

Uzyskanie zgody nie pozwoli również na ominięcie innych przepisów, takich jak art. 8 ust. 5. Tylko w nielicznych określonych okolicznościach zgoda może być podstawą legalności operacji przetwarzania danych, które w innym przypadku byłyby zakazane, szczególnie w odniesieniu do przetwarzania niektórych danych szczególnie chronionych (art. 8), bądź też pozwolić na wykorzystywanie danych osobowych w celu dalszego przetwarzania, niezależnie od tego, czy jest to zgodne z pierwotnym celem czy nie. Co do zasady, zgoda nie powinna być postrzegana jako wyjątek od pozostałych zasad ochrony danych, ale jako gwarancja. Jest to głównie podstawa legalności i nie oznacza odstępstwa od stosowania pozostałych zasad.

Wybór najbardziej odpowiedniej podstawy prawnej nie zawsze jest oczywisty, szczególnie między podstawą z art. 7 lit. a) a art. 7 lit. b). Zgodnie z art. 7 lit. b) przetwarzanie danych musi być konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą, 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 zawierania umowy nie może rozszerzyć jego zakresu tak, aby usprawiedliwić przetwarzanie danych, które będzie wykraczało poza konieczne przetwarzanie: będzie musiał wykazać legalność dodatkowego przetwarzania poprzez szczególną zgodę, do czego będą miały zastosowanie wymogi art. 7 lit. a). Wskazuje to na potrzebę szczególności warunków umowy. W praktyce oznacza to, że konieczne może być posiadanie zgody jako dodatkowego warunku dla określonej części przetwarzania. Zatem albo przetwarzanie jest konieczne dla realizacji umowy, albo należy uzyskać (dobrowolną, [ang. *free*]) zgodę.

W przypadku niektórych operacji może mieć zastosowanie szereg podstaw prawnych, w tym samym czasie. Innymi słowy, każda operacja przetwarzania danych musi cały czas być zgodna z jedną lub z większą liczbą podstaw prawnych. Nie wyklucza to jednoczesnego wykorzystania kilku podstaw, pod warunkiem, że są wykorzystywane w odpowiednim kontekście. Niektóre przypadki gromadzenia danych i dalszego przetwarzania mogą być konieczne na mocy umowy z osobą, której dane dotyczą – art. 7 lit. b); inne przypadki przetwarzania danych mogą być konieczne w wyniku zobowiązania prawnego – art. 7 lit. c); gromadzenie dodatkowych informacji może wymagać odrębnej zgody – art. 7 lit. a); zaś jeszcze inne przypadki przetwarzania mogą być zgodne z prawem dzięki zrównoważeniu interesów – art. 7 lit. f).

Przykład: zakup samochodu

Administrator danych może być uprawniony do przetwarzania danych zgodnie z różnymi celami i na podstawie różnych podstaw:

- dane konieczne do kupna samochodu: art. 7 lit. b),
- w celu przetwarzania dokumentów dotyczących samochodu: art. 7 lit. c),
- w celu zarządzania świadczeniem usług klientowi (np. w celu serwisowania samochodu w innych filiach firmy w UE): art. 7 lit. f),
- w celu przekazywania danych stronom trzecim dla ich własnych działań marketingowych: art. 7 lit. a).

II.3. Powiązane pojęcia

Kontrola

Pojęcie zgody tradycyjnie wiąże się z ideą, że osoba, której dane dotyczą, powinna mieć kontrolę nad wykorzystywaniem jej danych. Z punktu widzenia praw podstawowych, kontrola realizowana poprzez zgodę jest ważnym pojęciem. Jednocześnie oraz z tego samego punktu widzenia, decyzja osoby fizycznej, iż zgadza się na operację przetwarzania danych, powinna podlegać rygorystycznym wymogom, w szczególności przy uwzględnieniu faktu, że podjęcie takiej decyzji przez osobę fizyczną może oznaczać zrzeczenie się prawa podstawowego.

Mimo że zgoda odgrywa znaczenie w zapewnieniu możliwości kontroli osobom, których dane dotyczą, nie jest to jedyny sposób, aby to uczynić. Dyrektywa przewiduje inne sposoby kontroli, w szczególności prawo do wyrażenia sprzeciwu, ale jest to inny instrument, który może być wykorzystany na innym etapie przetwarzania, tj. po rozpoczęciu przetwarzania i na podstawie innej podstawy prawnej.

Zgoda jest związana z pojęciem informacyjnego samostanowienia. Niezależność osoby, której dane dotyczą, jest zarówno warunkiem wstępnym, jak i konsekwencją zgody: daje osobie, której dane dotyczą, możliwość wpływu na przetwarzanie danych. Jednakże, o czym będzie mowa w następnym rozdziale, zasada ta ma ograniczenia i istnieją przypadki, w których osoba, której dane dotyczą, nie jest w stanie podjąć rzeczywistej decyzji. Administrator danych może chcieć wykorzystać zgodę osoby, której dane dotyczą, jako sposób przeniesienia odpowiedzialności na osobę fizyczną. Na przykład, zgadzając się na publikację danych osobowych w Internecie lub na ich przekazanie do podejrzanego podmiotu w kraju trzecim, osoba może ponieść szkodę, a administrator może twierdzić, że jest to przecież tylko to, na co osoba, której dane dotyczą, wyraziła zgodę. W związku z tym ważne jest, aby pamiętać, że w pełni ważna zgoda nie zwalnia administratora danych z jego zobowiązań i nie stanowi podstawy legalności przetwarzania, które w innym przypadku byłoby nierzetelne (ang. *unfair*) zgodnie z art. 6 dyrektywy.

Pojęcie kontroli jest również związane z faktem, że osoba, której dane dotyczą, powinna mieć możliwość wycofania zgody. Wycofanie zgody nie działa wstecz, ale powinno, co do zasady, zapobiegać dalszemu przetwarzaniu danych osoby fizycznej przez administratora danych. Zostanie to szczegółowo omówione poniżej (Rozdział III).

Przejrzystość

Drugi wymiar zgody dotyczy informacji: przejrzystości dla osoby, której dane dotyczą. Przejrzystość jest warunkiem posiadania kontroli oraz przyczynienia się do ważności zgody. Przejrzystość jako taka nie jest wystarczającą podstawą legalności przetwarzania danych osobowych, ale jest niezbędnym warunkiem do zapewnienia ważności zgody.

Aby zgoda była ważna, musi być świadoma. Oznacza to, że wszystkie konieczne informacje muszą być podane w momencie pozyskiwania zgody oraz że informacje te powinny dotyczyć istotnych aspektów przetwarzania, którego podstawą legalności ma być zgoda. Zazwyczaj informacje te powinny obejmować elementy wskazane w art. 10 dyrektywy, ale będą także zależeć od tego, kiedy i w jakich okolicznościach zgoda od osoby jest pozyskiwana.

Niezależnie od tego, czy zgoda zostanie udzielona czy też nie, przejrzystość przetwarzania danych również jest warunkiem rzetelności, co ma swoją wartość także po tym, jak zapewniono wstępne informacje.

Moment i sposoby wyrażenia zgody

Ten trzeci wymiar dotyczy sposobu realizacji kontroli: w jaki sposób można wyrazić zgodę oraz kiedy należy się o nią zwrócić, aby zapewnić, że będzie to zgoda ważna? Pytania te mają decydujący wpływ na sposób realizacji i interpretacji zgody.

Mimo że termin, w jakim należy zwrócić się o wyrażenie zgody, nie jest określony w dyrektywie, jasno wynika z treści różnych przepisów, które wskazują, że, co do zasady, zgoda musi być wyrażona przed rozpoczęciem przetwarzania¹³. Uzyskanie zgody przed rozpoczęciem przetwarzania danych jest niezbędnym warunkiem legalności przetwarzania danych. Szczegółowe omówienie tej kwestii znajduje się poniżej w Rozdziale III.B dotyczącym dyrektywy o prywatności i łączności elektronicznej.

Zgoda, uznawana jako upoważnienie przez osobę fizyczną pozwalające na przetwarzanie dotyczących jej danych, może być wyrażona na różne sposoby: art. 2 lit. h) odnosi się do „wskazania”; musi być ona jednoznaczna (art. 7 lit.a)) oraz wyraźna w odniesieniu do danych szczególnie chronionych (art. 8). Jednakże jest to niezbędne do podkreślenia faktu, że zgoda różni się od prawa do wyrażenia sprzeciwu przewidzianego w art. 14. Podczas gdy zgodnie z art. 7 lit. a) administrator danych nie może przetwarzać danych dopóki nie uzyska zgody; zgodnie z art. 7 lit. f) administrator danych może przetwarzać dane, pod warunkiem spełnienia warunków i zapewnienia zabezpieczeń, dopóki osoba, której dane dotyczą, nie wyrazi sprzeciwu. Jak stwierdzono w Dokumencie roboczym 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.

Z tych powodów prawo do wyrażenia sprzeciwu, o którym mowa w art. 8 dyrektywy, nie powinno być mylone ze zgodą. Ta ostatnia jest podstawą prawną przetwarzania danych, o czym mowa w art. 7 lit. a), 8 ust. 2 lit. a), art. 26 lit. 1 lub jak przewidziano w różnych przepisach dyrektywy 2002/58/WE.

II.4. Właściwe wykorzystywanie zgody jako podstawy prawnej

Konieczne jest podkreślenie, że zgoda nie zawsze jest podstawowym czy też najbardziej pożądanym środkiem przesadzającym o legalności przetwarzania danych osobowych.

Zgoda czasami jest słabą podstawą uzasadniającą przetwarzanie danych osobowych i traci swoją wartość, gdy jej zakres jest zwiększany czy też ograniczany, aby dopasować ją do sytuacji, w których nigdy nie miała być wykorzystana. Wykorzystanie zgody „we właściwym kontekście” jest decydującą kwestią. Jeżeli jest wykorzystywana w okolicznościach, w których nie jest to właściwe, ponieważ jest mało prawdopodobna

¹³ Tytułem przykładu, niemiecka wersja dyrektywy (oraz niemiecka federalna ustawa o ochronie danych) stosuje termin „Einwilligung” [zgoda, zezwolenie, przystanie – przypis tłumacza]. Pojęcie to jest określone w niemieckim kodeksie cywilnym jako „wstępna zgoda” („prior acceptance”).

¹⁴ WP 114 – Dokument roboczy Grupy Roboczej Artykułu 29 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE, przyjęty w dniu 24 października 1995 r..

obecność elementów składających się na ważną zgodę, doprowadzi to do dużego osłabienia i w praktyce *osłabi* pozycję osoby, której dane dotyczą.

Grupa Robocza i EIOD już poparły to podejście w swoich wkładach do dyskusji na temat nowych ram prawnych ochrony danych. W szczególności stwierdzono, że: „*nie zawsze jest jasne, co stanowi prawdziwą, jednoznaczną zgodę. Niektórzy administratorzy danych wykorzystują tę niepewność, polegając na metodach nieodpowiednich do zapewnienia prawdziwej, jednoznacznej zgody*”¹⁵, z naruszeniem warunków artykułu 6 dyrektywy. Podobnie GR Art. 29 zauważyła, że „*złożony charakter praktyk zbierania danych, modeli biznesowych, modeli sprzedaży i aplikacji technologicznych w wielu przypadkach uniemożliwia obywatelom podejmowanie decyzji pozwalających kontrolować wykorzystanie i przekazywanie ich danych opartych na aktywnym wyborze*”¹⁶.

W związku z tym ważne jest, aby wyjaśnić granice zgody oraz zapewnić, że tylko zgoda, która jest skonstruowana w sposób zgodny z prawem, jest za taką uważana.¹⁷

III. Analiza przepisów

W analizie tej w rozdziale III.A skupimy się na dyrektywie 95/46/WE. W rozdziale III.B dokonamy analizy określonych istotnych części dyrektywy o prywatności i łączności elektronicznej 2002/58/WE. Należy zauważyć, że dyrektywy nie wykluczają się wzajemnie. Ogólne warunki ważności zgody, przewidziane w dyrektywie 95/46/WE, mają zastosowanie zarówno w środowisku *off-line*, jak i *on-line*. Dyrektywa 2002/58/WE określa te warunki dla niektórych wyraźnie wskazanych usług *on-line*, zawsze w świetle ogólnych warunków dyrektywy o ochronie danych.

III.A Dyrektywa 95/46/WE

Pojęcie „zgody osoby, której dane dotyczą” jest określone w art. 2 lit. h) i następnie wykorzystywane w art. 7, 8 oraz art. 26. Rola zgody wspomniana jest również w motywach 30 oraz 45. Przepisy te i wszystkie istotne szczegóły zostaną omówione odrębnie i w tym rozdziale.

III.A.1. Artykuł 2(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*” [tłumaczenie oficjalne z *EUR-lexu – przypis tłumacza*]. Definicja ta zawiera różne kluczowe elementy, które zostaną omówione poniżej.

„*wskazanie... na to, że... wyraża...*” (ang. “... any... indication of his wishes... signifying...”, dosłownie: “...każde... wskazanie woli.... oznaczające...”)

¹⁵ Opinia Europejskiego Inspektora Ochrony Danych z 14 stycznia 2011 r. w sprawie Komunikatu Komisji „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”.

¹⁶ „Przyszłość Prywatności: Wspólny wkład do Konsultacji Komisji Europejskiej w sprawie ram prawnych dla podstawowego prawa do ochrony danych osobowych”, 1 grudnia 2009 r., WP 168.

¹⁷ Opinia Europejskiego Inspektora Ochrony Danych z 14 stycznia 2011 r., op.cit.

W zasadzie nie ma ograniczeń co do formy, jaką może przyjąć zgoda. Jednakże, aby zgoda była ważna, zgodnie z dyrektywą, powinna być wskazaniem. Nawet jeżeli może to być „każda” (ang. *any*) forma wskazania, powinno być jasne, co dokładnie mieści się w definicji wskazania.

Forma wskazania (tj. sposób, w jaki wola jest wyrażona) nie jest określona w dyrektywie. Ze względu na elastyczność, „pisemna” zgoda została usunięta z ostatecznego tekstu. Należy podkreślić, że dyrektywa zawiera „każde” wskazanie woli (ang. *any indication of a wish*). Daje to możliwość szerokiego rozumienia zakresu takiego wskazania. Minimalnym wyrażeniem wskazania może być każdy rodzaj sygnału, wystarczająco jasnego, aby mógł wskazać wolę osoby, której dane dotyczą, oraz aby był zrozumiały dla administratora danych. Słowa „wskazanie” (ang. *indication*) oraz „wyraża” (ang. *signifying*) wskazują w kierunku działania naprawdę potrzebnego (w przeciwieństwie do sytuacji, gdy zgodę można by wywnioskować z braku działania).

Zgodę powinno oznaczać każde wskazanie woli, za pomocą którego osoba *wyraża* swoje przyzwolenie: może na nią składać się odręczny podpis na dokumencie papierowym, ale również ustne oświadczenia o wyrażeniu przyzwolenia, czy też zachowanie, z którego racjonalnie można wywnioskować zgodę. W związku z tym, poza klasycznymi przykładami podpisu, wrzucenie wizytówki do szklanej kuli mogłoby być objęte tą definicją. To samo dotyczy sytuacji, gdy osoba fizyczna wysłała swoje imię i nazwisko oraz adres do organizacji w celu uzyskania od niej informacji. W tym przypadku jej działanie należy rozumieć jako przyzwolenie na przetwarzanie takich danych, o ile jest to konieczne do rozpatrzenia i odpowiedzi na wniosek/prośbę.

W swojej opinii w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną (WP115) Grupa Robocza oceniła, w jaki sposób osoby fizyczne powinny być stawiane w sytuacji, w której mają wyrazić zgodę na usługi wymagające ich automatycznej lokalizacji (np. możliwość zatelefonowania pod określony numer telefonu w celu uzyskania informacji na temat warunków pogodowych w swojej lokalizacji). W tym przypadku uznano, że pod warunkiem, że użytkownicy uzyskują wcześniej pełne informacje na temat przetwarzania ich danych o lokalizacji, zatelefonowanie pod dany numer telefonu będzie równoznaczne z wyrażeniem zgody na określenie ich lokalizacji.

Przykład: billboardy reklamowe z nadajnikami Bluetooth

Istnieje rozwijająca się forma reklamy polegająca na tym, że billboardy wysyłają wiadomości, prosząc o ustanowienie połączenia w celu wysyłania reklam ludziom przechodzącym obok tych billboardów. Wiadomości wysyłane są do osób, które aktywowały funkcję Bluetooth w swoich telefonach komórkowych. Sama aktywacja funkcji Bluetooth nie stanowi ważnej zgody (tj. funkcja Bluetooth mogłaby być aktywowana w innych celach). Z drugiej strony, gdy ktoś jest informowany o usłudze i zbliża się do billboardu na odległość kilku centymetrów ze swoim telefonem komórkowym, wówczas, zwyczajnie mówiąc, ma miejsce wskazanie woli: pokazuje to, które osoby naprawdę są zainteresowane otrzymaniem reklam. Tylko te osoby powinny być uważane za te, które wyraziły zgodę; tylko one powinny otrzymywać wiadomości na swoje telefony.

Wątpliwe jest, czy brak jakiegokolwiek zachowania – czy też raczej: pasywne zachowanie – może być interpretowane jako wskazanie w ściśle określonych okolicznościach (tj. w całkowicie jednoznacznym kontekście). Pojęcie „wskazanie” jest szerokie, ale wydaje się oznaczać potrzebę działania. Inne elementy definicji zgody oraz dodatkowy wymóg z art. 7 lit. a), aby zgoda była jednoznaczna, wspierają tę interpretację. Wymóg, iż osoba, której dane dotyczą, musi wyrazić zgodę, wydaje się wskazywać, że zwykły brak działania jest niewystarczający oraz że jakiś rodzaj działania jest wymagany, aby stanowiło to o zgodzie, mimo że możliwe są różne rodzaje działań, które mają być ocenione „w kontekście”.

W praktyce, przy braku aktywnego zachowania osoby, której dane dotyczą, dla administratora danych problematyczne będzie zweryfikowanie, czy milczenie miało w zamierzeniu oznaczać akceptację lub zgodę. Na przykład, administrator danych mógł nie mieć pewności potrzebnej do założenia istnienia zgody w następującym przypadku: wyobraźmy sobie sytuację, w której po wysłaniu klientom listu informującego ich o planowanym przekazaniu ich danych, o ile nie wyrażą sprzeciwu w ciągu 2 tygodni, tylko 10% spośród klientów udzieli odpowiedzi. W tym przykładzie dyskusyjne jest, że 90% osób, które nie odpowiedziały, w rzeczywistości zgodziły się na przekazanie danych. W takich przypadkach administrator danych nie posiada jasnego wskazania intencji osób, których dane dotyczą. Poza tym nie ma dowodów i w związku z tym nie będzie mógł udowodnić, że uzyskał zgodę. W praktyce niejednoznaczność pasywnej odpowiedzi utrudni wypełnienie wymogów dyrektywy.

“... *dobrowolne*...” (“... *freely given* ...”)

Zgoda może być ważna tylko wówczas, gdy osoba, której dane dotyczą, może dokonać rzeczywistego wyboru oraz nie istnieje ryzyko oszukania, zastraszenia, nacisku czy istotnych negatywnych konsekwencji, jeżeli osoba nie wyrazi zgody. Jeżeli konsekwencje wyrażenia zgody naruszają wolność wyboru osoby fizycznej, zgoda nie jest dobrowolna. Sama dyrektywa przewiduje w art. 8 ust. 2 lit. a), że w niektórych przypadkach, które mają być określone przez państwa członkowskie, zakaz przetwarzania szczególnych kategorii danych osobowych nie może być zniesiony poprzez zgodę osoby, której dane dotyczą.

Przykładem powyższego jest przypadek, w którym osoba, której dane dotyczą, jest pod wpływem administratora danych, np. ze względu na stosunek pracy. W tym przykładzie, mimo że niekoniecznie zawsze, osoba, której dane dotyczą może być w sytuacji zależności od administratora danych – ze względu na charakter relacji lub na szczególne okoliczności – i może się obawiać, że będzie potraktowana inaczej, jeżeli nie wyrazi zgody na przetwarzanie danych.

Grupa Robocza odniosła się do ograniczeń zgody w sytuacjach, gdy nie może być dobrowolna, w kilku opiniach, w szczególności w swojej opinii w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej (EHR) (WP 131), opinii w sprawie przetwarzania danych w kontekście zatrudnienia (WP 48), oraz opinii dotyczącej przetwarzania danych przez Światową Organizację Antydopingową (WP 162).

W dokumencie WP 131, Grupa Robocza wspomniała, że „*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 wycofaniu zgody, przetwarzanie danych jest kontynuowane na innej podstawie prawnej, mogą zostać podniesione wątpliwości co do oryginalnego wykorzystania zgody jako wstępnej podstawy prawnej: jeżeli przetwarzanie mogło mieć miejsce od początku przy użyciu innej podstawy, stawianie osoby fizycznej w sytuacji, w której jest proszona o zgodę na przetwarzanie, mogłoby być uznane za wprowadzające w błąd lub z natury nierzetelne. Inaczej byłoby, gdyby nastąpiła zmiana okoliczności, jak np. nowa ustawa regulująca kwestie dotyczące przedmiotowej bazy danych. Jeżeli taka nowa podstawa może mieć zastosowanie do przetwarzania danych, może ono być prowadzone. Jednakże, w praktyce takie okoliczności nie występują często. W zasadzie, zgoda może być uznana za niewystarczającą, jeżeli nie jest dozwolone skuteczne jej wycofanie.

Grupa Robocza przyjęła wspólne stanowisko w sprawie interpretacji dobrowolnej zgody w kontekście zatrudnienia¹⁹: „gdy od pracownika wymagana jest zgoda i z nieudzieleniem zgody wiąże się rzeczywista lub potencjalna istotna szkoda, zgoda nie jest ważna, ze względu na niespełnienie postanowień art. 7 lub 8, jako że nie jest dobrowolna. Jeżeli pracownik nie ma możliwości odmowy wyrażenia zgody, nie jest to zgoda... Problematiczna jest sytuacja, w której wyrażenie zgody jest warunkiem zatrudnienia. Pracownik w teorii może odmówić udzielenia zgody, ale konsekwencją może być utrata możliwości podjęcia pracy. W takich okolicznościach zgoda nie jest dobrowolna i w związku z tym nie jest ważna. Sytuacja jest jeszcze jaśniejsza, gdy, co często ma miejsce, wszyscy pracodawcy nakładają taki sam lub podobny warunek zatrudnienia.”

Przykład: zdjęcia w intranecie

Zgoda w kontekście zatrudnienia może być ważna, co pokazuje następujący przykład: firma postanawia utworzyć intranet, w którym będą podane nazwiska pracowników i ich podstawowe funkcje. Każdy z pracowników pytany jest, czy chciałby, aby obok jego nazwiska znalazło się jego zdjęcie. Osoby, które chcą, aby umieszczono ich zdjęcie, są proszone o przesłanie zdjęcia na podany adres. Po otrzymaniu odpowiednich informacji, działanie osoby polegające na wysłaniu zdjęcia będzie uważane za zgodę. Jeżeli firma posiada zdjęcia cyfrowe wszystkich pracowników i prosi każdego z nich o zgodę na umieszczenie zdjęć w powyższych celach, każdy pracownik, który kliknie w przycisk oznaczający zgodę, również będzie uznany za osobę, która wyraziła ważną zgodę. W każdym przypadku w pełni respektowana jest możliwość wyboru przez pracowników,

¹⁸ WP 162 w sprawie WADA przedstawia takie same wnioski: "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 WP 48 w sprawie przetwarzania danych osobowych w kontekście zatrudnienia. WP114 – Dokument roboczy Grupy Roboczej Artykułu 29 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.- jest również tu istotny.

czy chcą, aby ich zdjęcia pojawiły się w intranecie.

Kontekst zatrudnienia wymaga szczegółowego omówienia: kulturowe i społeczne aspekty stosunku zatrudnienia odgrywają tutaj rolę, podobnie jak sposób, w jaki zasady ochrony danych i inne przepisy wzajemnie na siebie oddziałują. W kontekście zatrudnienia dane osobowe można przetwarzać do różnych celów:

- o dane konieczne dla realizacji zadań przez pracownika: zastosowanie art. 7 lit. b) – konieczne dla umowy,
- o określenie prawa (opcji) pracowników do nabycia akcji: albo na podstawie zgody - art. 7 lit. a), albo jako możliwość wynikająca z administracyjnych aspektów umownego stosunku pracy – art. 7 lit. b),
- o przetwarzanie numeru ubezpieczenia społecznego do celów ubezpieczenia społecznego: art. 7 lit. c) – zobowiązanie prawne, lub ewentualnie art. 8 lit. b) – zobowiązanie w obszarze prawa w zakresie zatrudnienia,
- o przetwarzanie danych ujawniających pochodzenie etniczne: w niektórych krajach może to być również obowiązkiem ze względu postanowienia prawa w zakresie zatrudnienia – art. 8 lit. b), podczas gdy w innych krajach jest to ściśle zabronione.

Mimo że może istnieć silne domniemanie, że zgoda ma osłabione znaczenie w takich kontekstach, nie wyklucza to całkowicie jej wykorzystania, pod warunkiem, że istnieją wystarczające gwarancje, że zgoda jest rzeczywiście dobrowolna.

Podczas gdy stosunek zależności często jest główną przyczyną, dla której zgoda nie jest dobrowolna, inne elementy kontekstowe mogą wpływać na decyzję osoby, której dane dotyczą. Mogą mieć na przykład wymiar finansowy, emocjonalny lub praktyczny. Fakt, że gromadzenie danych jest dokonywane przez organ publiczny również może mieć jakiś wpływ na osobę, której dane dotyczą. Jednakże odróżnienie zwykłej zachęty od czegoś, co ma faktyczny wpływ na wolność realizacji wyboru przez osobę, której dane dotyczą, może być trudne. Poniższe przykłady są próbą zilustrowania różnego charakteru wysiłków bądź kosztów dla osób fizycznych, mogących wpłynąć na ich decyzję.

Przykład – Elektroniczna dokumentacja zdrowotna

W wielu państwach członkowskich podejmowane są kroki w kierunku utworzenia elektronicznego podsumowania dokumentacji zdrowotnej pacjentów. Pozwoli to świadczącym usługi opieki zdrowotnej na dostęp do kluczowych informacji, gdziekolwiek pacjent wymaga leczenia.

- W pierwszym scenariuszu, utworzenie akt podsumowujących jest całkowicie dobrowolne, a pacjent nadal będzie leczony, niezależnie od tego, czy zgodził się na stworzenie akt podsumowujących czy też nie. W tym przypadku zgoda na stworzenie akt podsumowujących jest dobrowolna, ponieważ pacjent nie poniesie szkody, jeżeli zgoda nie będzie udzielona czy też zostanie wycofana.
- W drugim scenariuszu, istnieje umiarkowana zachęta finansowa do wybrania elektronicznej dokumentacji zdrowotnej. Pacjenci nie zgadzający się na jej utworzenie nie poniosą szkody w takim sensie, że koszty się dla nich nie zmieniają. Można tutaj również uznać, że pacjenci mają wolność wyboru, co do wyrażenia zgody na nowy system czy też nie wyrażenia zgody.
- W trzecim scenariuszu pacjenci nie zgadzający się na system elektronicznej dokumentacji zdrowotnej i muszą uiścić znaczną dodatkową opłatę na rzecz

poprzedniego systemu taryfowego, a przetwarzanie ich akt jest znacznie opóźnione. Oznacza to widoczną niekorzyść dla osób nie wyrażających zgody, w celu doprowadzenia do przeniesienia do systemu elektronicznej dokumentacji zdrowotnej wszystkich obywateli w zaplanowanym terminie. Zatem zgoda nie jest wystarczająco dobrowolna. Toteż należy także zbadać istnienie innych prawnie uzasadnionych podstaw przetwarzania danych osobowych lub przeanalizować stosowanie art. 8 ust. 3 dyrektywy 95/46/WE.

Przykład: skanery ciała

Następuje rozwój wykorzystywania skanerów ciała w niektórych publicznych miejscach, w szczególności na lotniskach w celu dostania się do strefy, w której oczekuje się na wejście na pokład samolotu. Uwzględniając fakt, że dane pasażerów są przetwarzane w momencie, gdy ma miejsce skanowanie²⁰, przetwarzanie musi być zgodne z jedną z podstaw prawnych z art. 7. Czasami przejście przez skanery ciała jest przedstawiane pasażerom jako możliwość, przez co daje się do zrozumienia, że przetwarzanie może być uzasadnione przez ich zgodę. Jednakże odmowa przejścia przez skaner ciała może wzbudzić podejrzenia bądź przyczynić się do dodatkowych kontroli, takich jak kontrola osobista. Wielu pasażerów zgadza się na dokonanie przeskanowania, ponieważ czyniąc to, uniknie potencjalnych problemów lub opóźnień, podczas gdy ich najważniejszym priorytetem jest dostanie się na pokład samolotu na czas. Taka zgoda nie jest wystarczająco dobrowolna. Jako że trzeba wykazać konieczność przetwarzania (ze względów bezpieczeństwa publicznego), podstawy prawnej nie należy szukać w art. 7 lit. a), lecz w akcie prawnym – art. 7 lit. c) lub lit. e) – czego skutkiem jest zobowiązanie pasażerów do współpracy. Podstawą przeskanowania ciała powinno być zatem ustawodawstwo: prawo to może nadal przewidywać możliwość wyboru między skanowaniem a kontrolą osobistą, jednakże taki wybór nie będzie proponowany osobie fizycznej jako uzupełnienie, jako część dodatkowych środków.

Charakter administratora danych może również być decydujący przy wyborze podstawy prawnej przetwarzania danych osobowych. Ma to szczególnie miejsce w przypadku administratorów danych w sektorze publicznym, gdzie przetwarzanie danych jest zazwyczaj związane z wykonaniem zobowiązania prawnego, o czym mowa w art. 7 lit. c) lub z realizacją zadania wykonywanego w interesie publicznym, o którym mowa w art. 7 lit. e). W związku z tym wykorzystanie zgody osoby, której dane dotyczą, w celu zapewnienia legalności przetwarzania danych nie jest odpowiednią podstawą prawną. Jest to szczególnie widoczne w przypadku przetwarzania danych osobowych przez organy publiczne posiadające uprawnienia władcze – jak np. organy egzekwowania prawa w zakresie swoich zadań w obszarze działalności policyjnej i sądowej. Organy policji nie mogą polegać na zgodzie osoby fizycznej w przypadku środków, które nie zostały przewidziane lub w przeciwnym razie nie byłyby dozwolone przez prawo.

Należy jednak uznać, że nawet jeżeli państwa mogą mieć prawny obowiązek przetwarzania danych osobowych, osoba fizyczna nie zawsze ma obowiązek współpracy. Mogą zdarzyć się przypadki, w których osobom, których dane dotyczą, świadczone są „usługi o wartości dodanej”, z których mogą skorzystać bądź nie. Jednak w większości przypadków przetwarzanie jest w rzeczywistości obowiązkowe. Często

²⁰ Patrz pismo z 11 lutego 2009 r. od Przewodniczącego Grupy Roboczej Artykułu 29 do pana Daniela CALLEJA CRESPO, Dyrektora DG TREN (Dyrekcji Generalnej ds. Energii i Transportu) w sprawie skanerów ciała, w odpowiedzi na Konsultacje Komisji dotyczące „wpływu wykorzystywania skanerów ciała w dziedzinie bezpieczeństwa lotniczego na prawa człowieka, prywatność, godność osobistą, zdrowie i ochronę danych” Dostępne na stronie http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009-others_en.htm.

nie tak łatwo jest określić, czy przetwarzanie danych osobowych przez organy publiczne prawowicie oparte jest na zgodzie osoby fizycznej. Toteż przy przetwarzaniu danych osobowych w sektorze publicznym często stosuje się systemy łączące różne przesłanki przetwarzania (tzw. *hybrid schemes*), co może prowadzić do niepewności lub nadużyć, gdy przetwarzanie jest niewłaściwie uzasadnione zgodą.

Podczas gdy w wyjątkowych przypadkach zgoda może być dla państw ważną podstawą przetwarzania danych osobowych, należy dokonać dokładnej kontroli konkretnych przypadków w celu oceny, czy zgoda jest w istocie wystarczająco dobrowolna. Jak pokazują poniższe przykłady, gdy organ publiczny jest administratorem danych, podstawą prawną legalności przetwarzania będzie raczej spełnienie prawnego zobowiązania wynikającego z art. 7 lit. c), lub realizacja zadania w interesie publicznym z art. 7 lit. e), a nie zgoda.

Przykład: e-administracja

W państwach członkowskich tworzone są nowe dokumenty tożsamości z elektronicznymi funkcjami wbudowanymi w chipie. Aktywacja elektronicznych usług karty (dokumentu) może nie być obowiązkowa. Jednakże bez aktywacji użytkownik może nie mieć dostępu do określonych usług administracyjnych, które w przeciwnym razie byłyby niezwykle trudno osiągalne (zapewnianie niektórych usług *on-line*, skrócenie godzin otwarcia urzędu). Nie można uznać zgody za prawną podstawę uzasadniającą przetwarzanie. W tym przypadku właściwą podstawą powinna być ustawa regulująca rozwijanie e-usług, wraz ze wszystkimi odpowiednimi zabezpieczeniami.

Przykład: dane PNR (dotyczące pasażera)

Przedmiotem dyskusji była kwestia, czy zgoda pasażerów może być wykorzystana jako ważna podstawa legalności przekazywania informacji związanych z rezerwacją (danych PNR) przez europejskie linie lotnicze do władz USA. Grupa Robocza uważa, że zgoda pasażerów nie może być dobrowolna, ponieważ linie lotnicze są zobowiązane do przesłania danych przed odlotem, i w związku z tym pasażerowie nie mają rzeczywistego wyboru, jeżeli chcą lecieć²¹. Podstawą prawną nie jest tutaj zgoda pasażera, tylko raczej, zgodnie z art. 7 lit. c), zobowiązania przewidziane w międzynarodowej umowie między UE a USA w sprawie przetwarzania i przekazywania danych PNR.

Przykład: spis powszechny

Podczas spisu powszechnego ludność proszona jest o udzielenie odpowiedzi na różne pytania dotyczące ich sytuacji osobistej i zawodowej. Udzielenie odpowiedzi na te pytania jest obowiązkowe. Ponadto spis powszechny zawiera pytanie, na które odpowiedź jest wyraźnie określona jako nieobowiązkowa, dotyczące środków transportu wykorzystywanych przez osobę fizyczną. Mimo że oczywiście nie ma dobrowolnej zgody w przypadku głównej części spisu, istnieje wolny wybór co do odpowiedzi na ostatnie pytanie nieobowiązkowe. Nie powinno to jednak ukryć faktu, że głównym celem, o jaki chodzi państwu w związku z tym kwestionariuszem, jest uzyskanie

²¹ Patrz Opinia 6/2002 Grupy Roboczej Artykułu 29 w sprawie przekazywania informacji na temat listy pasażerów i innych danych przez linie lotnicze Stanom Zjednoczonym.

odpowiedzi. Ogólnie mówiąc, zgoda nie stanowi ważnej podstawy w tym kontekście.

“... konkretne ...” (“... specific...”)

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

Ściśle mówiąc, zgoda musi być zrozumiała: powinna wyraźnie i dokładnie odnosić się do zakresu i konsekwencji przetwarzania danych. Nie może dotyczyć otwartego zestawu operacji przetwarzania. Innymi słowy, oznacza to, że kontekst, w jakim zgoda ma zastosowanie, jest ograniczony.

Zgoda musi być udzielona w odniesieniu do różnych aspektów przetwarzania, jasno określonych. Szczególnie chodzi o to, jakie dane są przetwarzane i w jakich celach. To rozumowanie powinno być oparte na racjonalnych oczekiwaniach stron. „Konkretna zgoda” jest w związku z tym nierozłącznie związana z faktem, że zgoda musi być świadoma. Istnieje wymóg szczegółowości zgody w odniesieniu do różnych elementów, które stanowią przetwarzanie danych: nie może ona obejmować „wszystkich prawnie uzasadnionych celów”, do których dąży administrator danych. Zgoda powinna odnosić się do przetwarzania, które jest racjonalne i konieczne w odniesieniu do celu.

W zasadzie powinno być wystarczającym wymogiem, aby administratorzy danych uzyskali zgodę tylko raz dla różnych operacji, jeżeli odpowiadają one racjonalnym oczekiwaniom osoby, której dane dotyczą.

Ostatnio Europejski Trybunał Sprawiedliwości wydał wstępne orzeczenie²² w sprawie art. 12 ust. 2) dyrektywy o prywatności i łączności elektronicznej dotyczące potrzeby ponownego wyrażenia zgody przez abonentów, którzy już zgodzili się na opublikowanie swoich danych osobowych w jednej książce telefonicznej, na przeniesienie ich danych i opublikowanie w innych tego typu usługach. Trybunał uznał, że w sytuacji, gdy abonenta odpowiednio poinformowano o możliwości przekazania jego danych osobowych stronie trzeciej i już się zgodził na publikację tych danych w takiej książce, ponowne wyrażenie zgody przez abonenta na przekazanie tych samych danych nie jest potrzebne, *jeżeli jest zagwarantowane, że przedmiotowe dane nie zostaną wykorzystane do celów innych niż te, dla których zostały zebrane w celu ich pierwszej publikacji (para. 65).*

Niemniej odrębna zgoda może być potrzebna, gdy administrator zamierza przetwarzać dane w innych celach. Na przykład zgoda mogłaby być udzielona w odniesieniu zarówno do informacji na temat nowych produktów dla osoby fizycznej, jak i określonych działań promocyjnych, jako że mogłoby to być uznane za wchodzące w zakres racjonalnych oczekiwań osoby, której dane dotyczą. Jednak odrębna, dodatkowa zgoda powinna być wymagana na przesłanie danych osoby stronom trzecim. Potrzeba szczegółowości w przypadku uzyskiwania zgody powinna być oceniana dla konkretnych przypadków, w zależności od celu (celów) lub odbiorców danych.

²² Orzeczenie Trybunału z dnia 5 maja 2011, Deutsche Telekom AG (Case C-543/09). Sprawa ta zaczęła się od wskazania przez niemiecki Federalny Sąd Administracyjny dotyczącego książek telefonicznych, a w szczególności interpretacji art. 25 ust. 2 dyrektywy w sprawie usługi powszechnej (2002/22/WE) oraz art. 12 ust. 2 dyrektywy o prywatności i łączności elektronicznej (2002/58/WE). Jest to wyraźnie związane ze szczególną rolą książek telefonicznych w dyrektywie w sprawie usługi powszechnej.

Należy pamiętać, że przetwarzanie może mieć kilka różnych podstaw prawnych: niektóre dane mogą być przetwarzane, ponieważ są potrzebne w ramach umowy z osobą, której dane dotyczą, np. dotyczącej dostarczenia produktu i zarządzania usługami, a szczególna zgoda może być konieczna na przetwarzanie wykraczające ponad to, co jest konieczne dla realizacji umowy, na przykład w celu oceny wiarygodności i zdolności kredytowej.

Grupa Robocza wyjaśniła ten aspekt zgody w dokumencie WP 131 w sprawie elektronicznej dokumentacji zdrowotnej EHR): „konkretna” zgoda dotyczy precyzyjnie określonej, konkretnej sytuacji, w której przewidziane jest przetwarzanie danych medycznych. W związku z tym „ogólne przyzwolenie” osoby, której dotyczą dane, przykładowo na gromadzenie danych medycznych tej osoby na potrzeby EHR oraz dalsze przekazywanie tych danych medycznych, odnoszące się do przeszłości lub przyszłości, udzielone pracownikowi medycznemu uczestniczącemu w leczeniu, nie stanowi zgody w rozumieniu art. 2 lit. h) dyrektywy”.

Taki sam tok rozumowania jest przedstawiony w dokumencie WP 115 w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną: *„(Ta) 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.”*

W orzeczeniu Trybunału wspomnianym powyżej w Rozdziale II w części „rola zgody”, nawet jeżeli termin „konkretna” nie jest wyraźnie użyty, tok rozumowania również wskazuje na potrzebę, aby zgoda była konkretna, o czym świadczy stwierdzenie: *„nie wystarczy, że określona umowa zatrudnienia pracownika będzie odnosić się do układu zbiorowego, który pozwala na takie przedłużenie”*.

Przykład: portale społecznościowe

Dostęp do usług portali społecznościowych często uwarunkowany jest udzieleniem zgody na różnego rodzaju przetwarzanie danych osobowych.

Użytkownik może być zobowiązany do udzielenia zgody na otrzymywanie reklamy behawioralnej, aby zarejestrować się w portalu społecznościowym, nie uzyskawszy bardziej szczegółowej informacji lub możliwości skorzystania z opcji alternatywnych. Biorąc pod uwagę znaczenie, jakie portale społecznościowe zyskały, niektóre kategorie użytkowników (np. młodzież) zaakceptują odbiór reklamy behawioralnej w celu uniknięcia ryzyka częściowego wyłączenia z interakcji społecznych. Użytkownik powinien być w stanie udzielić dobrowolnej i wyraźnej zgody na otrzymywanie reklamy behawioralnej, niezależnie od jego dostępu do portalu społecznościowego. Wyskakujące okienko mogłoby zostać wykorzystane do zaoferowania użytkownikowi takiej możliwości.

Portal społecznościowy oferuje możliwość korzystania z zewnętrznych aplikacji. Użytkownikowi w praktyce często uniemożliwia się korzystanie z danej aplikacji, jeśli nie wyrazi zgody na przekazanie swoich danych do autora aplikacji do różnych celów, w tym reklamy behawioralnej i odsprzedaży osobom trzecim. Biorąc pod uwagę, że

aplikację można uruchamiać bez potrzeby przekazywania jakichkolwiek danych autorowi aplikacji, Grupa Robocza zachęca do zachowania szczególności przy uzyskiwaniu zgody użytkownika, czyli uzyskiwaniu odrębnej zgody od użytkownika na przekazanie jego danych do autora aplikacji dla tych innych celów. Różne mechanizmy, takie jak wyskakujące okienka, mogłyby zostać wykorzystane, aby umożliwić użytkownikowi wybór celów przetwarzania, na które wyraża zgodę (przekazanie do autora aplikacji; usługi o wartości dodanej; reklama behawioralna; przekazywanie do osób trzecich; itp.).

Specyfika zgody oznacza również, że jeśli cele, dla których dane są przetwarzane przez administratora danych, po pewnym czasie ulegną zmianie, użytkownik musi zostać poinformowany o tym i być w stanie wyrazić zgodę na nowe cele przetwarzania danych. Dostarczone informacje muszą w szczególności wyjaśniać skutki odmowy zgody na proponowane zmiany.

“... świadoma...” (ang. *informed*)

Ostatnim elementem definicji zgody - ale nie ostatnim wymogiem, jak zobaczymy poniżej - jest jej świadomy charakter.

Art. 10 i 11 dyrektywy określają obowiązek przekazywania informacji osobom, których dane dotyczą. Obowiązek informacyjny jest więc czymś odrębnym, lecz w wielu przypadkach jest oczywiście powiązany ze zgodą. Mimo, że zgoda nie zawsze następuje po przedstawieniu informacji (inna podstawa z art. 7 może być wykorzystana), informacja musi być zawsze (przekazana), przed udzieleniem zgody.

W praktyce oznacza to, że: „zgoda osoby, której dotyczą dane, 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

Zgoda w wielu przypadkach będzie uzyskana w momencie zebrania danych osobowych, gdy przetwarzanie się rozpocznie. W tym przypadku, informacje, które mają być podane, są zbieżne z tym, co jest wymienione w art. 10 dyrektywy. Jednak zgoda może być wymagana „na późniejszym etapie”, kiedy cel przetwarzania ulegnie zmianie. W takim przypadku podawane informacje będą musiały dotyczyć tego, co jest istotne w danym kontekście, w odniesieniu do celu przetwarzania.

Świadoma zgoda jest szczególnie znacząca w kontekście przekazywania danych osobowych do państw trzecich: „wymaga, aby osoba, której dane dotyczą, była odpowiednio poinformowana o szczególnych zagrożeniach dla jej danych, gdy są one przekazywane do państwa nie zapewniającego odpowiedniego poziomu ochrony”²⁴.

²³ WP 131 - Dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej.

²⁴ WP 12 - Dokument roboczy w sprawie przekazywania danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych. Patrz także WP114 - Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.

Dwa wymagania mogą być określone w celu zapewnienia, że został spełniony obowiązek informacyjny:

- Jakość informacji - sposób w jaki informacje są udzielane (w postaci zrozumiałego, dobrze widocznego tekstu niezawierającego żargonu) ma kluczowe znaczenie dla oceny, czy zgoda jest „świadoma”. Sposób, w jaki informacje te powinny być udzielone, zależy od kontekstu: przeciętny użytkownik powinien być w stanie je zrozumieć.
- Dostępność i widoczność informacji - informacje muszą być podane bezpośrednio osobom fizycznym. Nie wystarczy, aby informacje były gdzieś „dostępne”. Trybunał Sprawiedliwości zwracał na to uwagę w wyroku z 2004 r.²⁵, odnosząc się do umowy o pracę, w szczególności do warunków umowy, które nie zostały zapisane w umowie, ale o których była w niej mowa. Informacje muszą być dobrze widoczne (rodzaj i wielkość czcionki), a także wystarczające i wyczerpujące. Okna dialogowe mogą być wykorzystane do przedstawienia konkretnej informacji w momencie, gdy zgoda jest wymagana. Jak wspomniano powyżej, w odniesieniu do „konkretnej zgody”, narzędzia informacyjne *on-line* są szczególnie użyteczne w odniesieniu do portali społecznościowych, w celu zapewnienia wystarczającej szczegółowości i jasności w ustawieniach prywatności. Zagnieżdżone ostrzeżenia mogą być również przydatnym narzędziem w tym zakresie, ponieważ umożliwiają udzielenie odpowiednich informacji w łatwo dostępny sposób.

W miarę upływu czasu, mogą pojawić się wątpliwości, czy zgoda, pierwotnie udzielona w oparciu o aktualne i wyczerpujące informacje, pozostaje w mocy. Z różnych powodów ludzie często zmieniają swoje poglądy, ponieważ ich początkowe wybory były źle dokonane, albo ze względu na zmianę okoliczności, takich jak w przypadku dorastającego dziecka²⁶. Dlatego dobrą praktyką jest, aby administratorzy danych dokonywali okresowych przeglądów indywidualnych wyborów na przykład przez informowanie danej osoby fizycznej o bieżącym wyborze i zaproponowanie jej ewentualnego potwierdzenia danego wyboru lub jego cofnięcia²⁷. Stosowny okres czasu pomiędzy przeglądami będzie oczywiście zależeć od kontekstu i okoliczności sprawy.

Przykład: mapy przestępczości

Niektóre służby policyjne rozważają publikowanie map przestępczości, lub udzielanie innych informacji, pokazujących, gdzie poszczególne rodzaje przestępstw miały miejsce. Zwykle zabezpieczenia wbudowane w proces publikacji zapewniają, że dane osobowe ofiar przestępstw nie są publikowane, ponieważ przestępstwo jest związane jedynie ze stosunkowo szerokim regionem geograficznym. Jednak niektóre służby policyjne chcą wskazywać miejsca przestępstw z większą dokładnością, w przypadku, gdy ofiara przestępstwa wyrazi na to zgodę. W takim przypadku możliwe staje się bardziej precyzyjne połączenie osoby, której dane dotyczą, z miejscem, gdzie przestępstwo zostało popełnione. Niemniej ofiara nie jest wyraźnie informowana o tym, że informacje umożliwiające jej identyfikację będą publikowane w Internecie oraz w jaki sposób informacje te mogą być wykorzystane. Zatem zgoda w tym przypadku nie

²⁵ Patrz przypis 12 (Rozdział II.2).

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

²⁷ Grupa Robocza Art. 29 przedstawiła podobne zalecenia w swojej Opinii 2/2010 w sprawie internetowej reklamy behawioralnej, przyjętej w dniu 22 czerwca 2010 r.

jest ważna, ponieważ ofiara może nie być w pełni świadoma, w jakim zakresie informacje na jej temat zostaną opublikowane.

Im bardziej złożony jest proces przetwarzania danych, tym więcej można oczekiwać od administratora danych. Im trudniejsze staje się dla przeciętnego obywatela nadzorowanie i zrozumienie wszystkich elementów przetwarzania danych, tym większy wysiłek powinien podjąć administrator danych, aby wykazać, że zgoda została uzyskana w oparciu o konkretne i zrozumiałe informacje.

Zgodę, w rozumieniu art. 2 lit. h), należy interpretować łącznie z wymogami wymienionymi w dalszej części tekstu dyrektywy. W art. 7 do elementów definicji dodaje się słowo „jednoznacznej”, a w art. 8 dodaje się wyraz „wyraźnej”, gdy przetwarzanie dotyczy przetwarzania określonych kategorii danych.

III.A.2. Art. 7 lit. a)

Zgodnie z art. 7 lit. a) dyrektywy jednoznaczna zgoda osoby, której dane dotyczą, stanowi podstawę prawną przetwarzania danych osobowych. Tak więc, aby zgoda była ważna, poza kryteriami określonymi w art. 2 lit. h), zgoda musi być *jednoznaczna*.

Aby zgoda była jednoznaczna procedura pozyskiwania i wyrażania zgody *nie może budzić wątpliwości*, co do zamiaru wyrażenia zgody przez osobę, której dane dotyczą. Innymi słowy, wskazanie przez osobę, której dane dotyczą, na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych nie może pozostawiać wątpliwości co do jej zamiaru. Jeżeli istnieją uzasadnione wątpliwości co do zamiaru osoby fizycznej, wówczas występuje dwuznaczność.

Jak opisano poniżej, wymóg ten wymusza na administratorach danych utworzenie wydajnych procedur umożliwiających osobom fizycznym udzielenie zgody; mianowicie, albo uzyskanie jasnej wyraźnej zgody albo poleganie na pewnego rodzaju procedurach, które zapewniają uzyskanie jednoznacznej dorozumianej zgody osoby fizycznej. Administrator danych musi być również wystarczająco pewny, że osoba fizyczna udzielająca zgodę jest w rzeczywistości osobą, której dane dotyczą. Jest to szczególnie istotne wtedy, gdy zgoda została udzielona podczas rozmowy telefonicznej bądź *on-line*.

Podobny problem dotyczy dowodu udzielenia zgody. Administratorzy danych, opierający się na zgodzie, mogą chcieć lub potrzebować wykazać, że uzyskali zgodę na przykład w kontekście sporu z osobą, której dane dotyczą. Rzeczywiście, w niektórych przypadkach mogą oni zostać poproszeni o takie dowody w kontekście działań związanych z egzekwowaniem prawa. W związku z tym, i jako dobrą praktykę, administratorzy danych winni utworzyć i przechowywać dowody wykazujące, że zgoda została rzeczywiście udzielona, tj. zgoda powinna być możliwa do zweryfikowania.

Rozważmy teraz następujące metody udzielania zgody i oceńmy, czy zgoda została udzielona jednoznacznie.

Wyraźne oświadczenie o wyrażeniu przyzwolenia, jak na przykład pisemne przyzwolenie lub pisemne oświadczenie o chęci wyrażenia zgody, są procedurami i mechanizmami, które dobrze nadają się do wyrażenia jednoznacznej zgody. A tym

samym, co do zasady, umożliwiając administratorowi danych wykazanie, że zgoda została udzielona.

Przykład: zgoda na otrzymywanie informacji promocyjnych drogą pocztową

Hotel prosi osoby fizyczne o podanie swoich adresów pocztowych w formie papierowej, jeśli chcą otrzymywać informacje promocyjne drogą pocztową. Jeśli dana osoba fizyczna, po wpisaniu danych teleadresowych, podpisze formularz, wyrażając tym samym swoje przyzwolenie, będzie to stanowić jednoznaczną zgodę. W tym przypadku zgoda będzie zarówno wyraźna, jak i na piśmie. Procedura ta zapewnia administratorowi danych odpowiednie dowody uzyskania zgody od wszystkich klientów, o ile administrator danych zachowa wszystkie podpisane formularze.

Jednak nie wszystkie formy wyrażania zgody, które mogą wydawać się wyraźne, świadczyć będą o wyrażeniu zgody. Kwestia ta została omówiona w niedawnej sprawie ETS (Volker und Markus Schecke v. Land Hessen), która dotyczyła publikacji imion i nazwisk osób korzystających z różnych funduszy UE²⁸ oraz kwot otrzymanych przez każdego beneficjenta. Rzecznik Generalny zbadał, czy warunki jednoznacznej zgody zostały spełnione w przypadku, gdy osoby fizyczne podpisały następujące oświadczenie: „Mam świadomość, że art. 44a rozporządzenia Nr 1290/2005... wymaga publikacji informacji na temat beneficjentów [funduszy z]EFRG i EFRROW oraz kwot otrzymanych przez każdego beneficjenta.” Rzecznik Generalny stwierdził: „*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, której dane dotyczą, zawartą w art. 2 lit. h.*” Uznała zatem, że skarżący nie wyrazili swojej zgody na przetwarzanie (tj. publikacji) ich danych osobowych w rozumieniu art. 7 lit. a) dyrektywy 95/46/WE.²⁹

Wyraźna zgoda może być również udzielona w środowisku *on-line*. Tak jak w świecie rzeczywistym (ang. *off-line*), istnieją odpowiednie środki umożliwiające udzielenie jednoznacznej zgody, co ilustruje następujący przykład.

Przykład: zgoda *on-line* na uczestnictwo w programie lojalnościowym

Na stronie internetowej hotelu znajduje się formularz rezerwacji, dzięki któremu osoby fizyczne mogą rezerwować pokoje drogą elektroniczną z wyprzedzeniem. Formularz *on-line*, w którym osoby fizyczne wprowadzają żądane daty i informacje dotyczące płatności, również posiada widoczne pole wyboru, które osoba fizyczna może zaznaczyć, jeżeli chce, aby jej dane były wykorzystywane do celów związanych z programem lojalnościowym. Zaznaczenie tego pola po otrzymaniu stosownych informacji stanowiłoby wyraźną jednoznaczną zgodę, gdyż działanie polegające na zaznaczeniu pola wyboru jest wystarczająco jasne, aby nie pozostawić wątpliwość, co do woli osoby fizycznej do wzięcia udziału w programie lojalnościowym.

²⁸ Europejski Fundusz Rolniczy Gwarancji (EFRG) oraz Europejski Fundusz Rolny 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 połączonych sprawach C-92/09 i C-93/09. Należy zauważyć, że ETS orzekł w wyroku z dnia 9 listopada 2010, że przetwarzanie danych nie było oparte o zgodę: „63. Odnośna regulacja unijna, która 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.”

Wyrażna zgoda może być również udzielona ustnie poprzez oświadczenia o wyrażeniu przyzwolenia. Wyrażna ustna zgoda byłaby udzielona w następującej sytuacji.

Przykład: ustna zgoda na otrzymywanie informacji promocyjnych

Podczas płacenia w kasie hotelu pracownik pyta klientów, czy chcieliby podać swój adres, aby hotel mógł im przysyłać informacje handlowe. Osoby fizyczne, które odpowiedzą poprzez podanie swojego adresu, po wysłuchaniu prośby pracownika oraz odpowiednich informacji, udzieliliby wyraźnej zgody. Działanie polegające na podaniu swojego adresu może stanowić jednoznaczne wskazanie woli osoby fizycznej. Niemniej, administrator danych może zdecydować się na wprowadzenie mechanizmów umożliwiających bardziej wiarygodną weryfikację, czy zgoda faktycznie została udzielona.

W niektórych przypadkach jednoznaczna zgoda może wynikać z pewnych działań, w szczególności będzie miało to miejsce w przypadku, gdy działania prowadzą do wniosku nie budzącego wątpliwości, że zgoda została udzielona. Jednak to zależy od tego, czy były udzielone istotne informacje o przetwarzaniu danych, umożliwiające osobie fizycznej podjęcie decyzji (m.in. kto jest administratorem danych, jakie są cele przetwarzania danych, itp.).

Przykład: zgoda na fotografowanie

Podczas przyjmowania gości do hotelu, pracownik przy ładzie informuje ich, że po południu będą robione zdjęcia w jednej z hotelowych kawiarenek. Wybrane zdjęcia zostaną wykorzystane do materiałów marketingowych, w szczególności w broszurach hotelu w formie papierowej. Jeśli goście chcieliby zostać ujęci na zdjęciach, zapraszani są do kawiarenki w określonych godzinach. Inna kawiarenka jest wskazywana gościom, którzy nie chcą być fotografowani.

Goście hotelowi, którzy – po otrzymaniu informacji – decydują się pójść do kawiarenki podczas robienia zdjęć mogą być uznani za osoby fizyczne, które wyraziły zgodę na fotografowanie. Ich zgoda wynika z działania polegającego na tym, że poszli do kawiarenki o określonej godzinie, gdzie odbywa się sesja zdjęciowa. Pójście do kawiarenki stanowi wyrażenie woli osoby fizycznej, która, co do zasady, może być uznana za jednoznaczną, świadcząca o tym, że osoba fizyczna idąca do kawiarni chce być sfotografowana. Jednakże, właściciele hotelu mogą uznać to za uzasadnione, aby posiadać dokument potwierdzający uzyskanie zgody w przypadku, gdyby ważność takiej zgody była zakwestionowana w najbliższej przyszłości.

Jak już wspomniano, te same wymagania, w tym jednoznacznej zgody, stosuje się zarówno w środowisku *off-line* jak i *on-line*. Jednak Grupa Robocza zauważa, że ryzyko związane z udzielaniem niejednoznacznej zgody może być większe w środowisku *on-line*, co wymaga szczególnej ostrożności. Następny przykład ilustruje przypadek, w którym zgoda wynikająca z pewnych działań (udział w grze *on-line*) nie spełnia wymagań ważnej zgody.

Przykład: gry on-line

Dostawca gier on-line wymaga od graczy, aby podali swój wiek, imię i nazwisko oraz adres w celu uczestnictwa w grze on-line (rozkład wieku i lokalizacji [adresów] wśród

graczy). Strona zawiera informację, dostępną poprzez link (choć zapoznanie się z takim rodzajem informacji nie jest konieczne do udziału w grze), co oznacza, że poprzez korzystanie ze strony internetowej (a tym samym dostarczanie informacji) gracze wyrażają zgodę na przetwarzanie swoich danych w celu przesyłania informacji marketingowych przez dostawcę gier on-line oraz podmioty trzecie.

Dostęp i udział w grze nie jest równoznaczny z udzieleniem jednoznacznej zgody na dalsze przetwarzanie danych osobowych w celach innych niż udział w grze. Udział w grze nie oznacza, że zgoda osoby fizycznej dotyczy również przetwarzania jej danych w celach innych niż te, które są niezbędne do udziału w grze. Tego typu zachowanie (działanie) nie stanowi jednoznacznego wskazania woli przez osobę fizyczną, aby jej dane były przetwarzane w celach marketingowych

Przykład: domyślne ustawienia prywatności

Domyślne ustawienia portalu społecznościowego, które użytkownicy nie koniecznie muszą otwierać, aby skorzystać z portalu, ustawione są na dostęp dla osób z kategorii „znajomi znajomych”, co oznacza, że wszystkie dane osobowe danego użytkownika widoczne są dla wszystkich osób z kategorii „znajomi znajomych”. Użytkownicy, którzy nie chcą, aby ich dane wyświetlane były osobom z kategorii „znajomi znajomych”, muszą wybrać odpowiednią opcję poprzez kliknięcie przycisku. Jeśli użytkownicy ci pozostaną bierni, lub też nie zaangażują się w działanie polegające na wybraniu odpowiedniej opcji, zostanie to uznane przez administratora danych za wyrażenie zgody na udostępnienie danych. Jest to jednak bardzo wątpliwe, czy *nie* kliknięcie na daną opcję oznacza, że ogół użytkowników wyraził *zgodę*, aby ich dane widoczne były dla wszystkich ‘znajomych znajomych’. Ze względu na niepewność co do tego, czy brak działania może oznaczać zgodę, brak kliknięcia nie może być uznany za jednoznaczny zgodę.

Powyższy przykład ilustruje przypadek, w którym osoba fizyczna pozostaje bierna (np. poprzez brak działania lub przez „milczenie”). Jednoznaczna zgoda nie współgra dobrze z procedurami uzyskania zgody na podstawie braku działania lub milczenia osoby fizycznej: milczenie danej strony lub jej bezczynność związane jest nieodłącznie z niejednoznacznością (osoba, której dane dotyczą, mogła mieć na celu zgodę lub mogła mieć na celu jedynie nie wykonanie czynności). Poniższy przykład to ilustruje.

Okoliczności można uznać za niejednoznaczne, w przypadku, gdy uważa się, że osoba fizyczna udzieliła zgodę, jeśli nie odpowiedziała na list, w którym jest informowana, że brak odpowiedzi oznaczać będzie wyrażenie zgody. W tego typu sytuacjach, zachowania osoby (lub raczej ich brak) mogą budzić poważne wątpliwości co do tego, czy osoba fizyczna ma na celu wyrażenie przyzwolenia. Sam fakt, że osoba fizyczna nie podjęła żadnych działań nie daje podstaw do stwierdzenia, że wyraziła swoją zgodę. Tak więc, nie będzie spełniony wymóg jednoznacznej zgody. Poza tym, jak zilustrowano poniżej, zapewnienie dowodów wskazujących, że osoba fizyczna wyraziła zgodę będzie również bardzo trudne dla administratora danych.

Grupa Robocza stwierdziła niemożność stosowania zgody opartej o milczenie osoby fizycznej w kontekście marketingu bezpośredniego wysyłanego za pośrednictwem poczty elektronicznej. *„Dorozumiana zgoda na otrzymywanie takich wiadomości nie jest zgodna z definicją zgody w dyrektywie 95/46/WE... Podobnie domyślnie wybrane*

*pola, np. na stronach internetowych, także nie są zgodne z definicją w dyrektywie*³⁰.
Poniższy przykład potwierdza ten pogląd:

Przykład: nieważna zgoda na dalsze przetwarzanie danych klienta

Księgarnia *on-line* rozsyła do swoich klientów programu lojalnościowego e-mail informujący klientów, że ich dane zostaną przekazane firmie reklamowej, która zamierza wykorzystać je do celów marketingowych. Użytkownicy mają dwa tygodnie na przesłanie swojej odpowiedzi na e-mail. Są oni informowani, że brak odpowiedzi będzie uznany za wyrażenie zgody na przekazanie danych. Tego rodzaju mechanizm, w którym zgoda jest pochodną braku reakcji ze strony osoby fizycznej, nie umożliwia udzielenia ważnej, jednoznacznej zgody. Nie jest możliwe ustalenie bez żadnych wątpliwości na podstawie braku odpowiedzi, że osoba fizyczna wyraziła zgodę na przekazanie danych.

Z powyższego wynika, że konsekwencją wymogu *jednoznaczności* zgody jest to, że administratorzy danych są *de facto* zachęceni do tworzenia procedur i mechanizmów, które nie pozostawiają wątpliwości, że zgoda została udzielona na podstawie wyraźnego działania osoby fizycznej albo, gdy jednoznacznie wynika z wyraźnego działania osoby fizycznej.

Jak wspomniano powyżej, jako element dobrej praktyki administratorzy danych powinni rozważyć wprowadzenie odpowiednich środków i procedur, aby wykazać, że zgoda została udzielona. Im bardziej skomplikowane jest środowisko, w którym działają, tym więcej środków będzie niezbędnych do zapewnienia, że zgoda jest możliwa do zweryfikowania. Informacje te powinny być do dyspozycji organu ochrony danych na żądanie.

III.A.3. Art. 8 ust. 2 lit. a)

Art. 8 dyrektywy przewiduje szczególną ochronę „*szczególnych kategorii danych*”, które ze swej natury są uważane za bardzo wrażliwe. Przetwarzanie takich danych jest zabronione, chyba że co najmniej jeden z kilku określonych wyjątków ma zastosowanie. Art. 8 ust. 2 lit. a) stanowi, że zakaz nie ma zastosowania, jeżeli osoba, której dane dotyczą, udzieliła *wyraźnej zgody* na ich przetwarzanie.

Z prawnego punktu widzenia „*wyraźną zgodę*” należy rozumieć tak samo jak *wyraźną zgodę*. Obejmuje ona wszystkie sytuacje, w której osobie fizycznej przedstawiona jest propozycja udzielenia zgody bądź nie co do konkretnego wykorzystania lub ujawnienia jej danych osobowych, zaś osoba fizyczna aktywnie odpowiada na pytanie, ustnie lub na piśmie. Zazwyczaj *wyraźna zgoda* udzielana jest na piśmie i potwierdzana podpisem odrębnym. Na przykład *wyraźna zgoda* zostanie udzielona, w przypadku, gdy osoba fizyczna podpisze formularz zgody, który jasno określa, dlaczego administrator danych zamierza zbierać i dalej przetwarzać jej dane osobowe.

Mimo, że *wyraźna zgoda* jest tradycyjnie udzielana w formie pisemnej, czy to w formie papierowej lub w formie elektronicznej, jak przedstawiono wcześniej w rozdziale

³⁰ Opinia 5/2004 w sprawie niezamówionych komunikatów do celów marketingowych zgodnie z art. 13 dyrektywy 2002/58/WE, przyjętej w dniu 27 lutego 2004 r. (WP90).

III.A.2, nie jest to konieczne; zatem, zgoda może być udzielona ustnie. Potwierdza to fakt, że wymóg pisemnej zgody zaproponowany w art. 8 został usunięty z ostatecznej wersji dyrektywy. Jednak, jak wskazano w tym rozdziale, ustna zgoda może być trudna do udowodnienia, a więc w praktyce administratorom danych zaleca się stosowanie pisemnej zgody ze względów dowodowych.

Wymóg udzielenia wyraźnej zgody oznacza, że zgoda, która jest dorozumiana zazwyczaj nie spełnia wymogu art. 8 ust. 2. W związku z tym warto przypomnieć dokument roboczy Grupy Roboczej Art. 29 w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej (EHR)³¹, który stwierdza, że „*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’ ...*”.

Przykład: dane medyczne (przekazane) na potrzeby badań

Nie zostanie spełniony wymóg wyraźnej zgody w sytuacji, gdy pacjent zostanie poinformowany przez klinikę, że jego dokumentacja medyczna zostanie przekazana na potrzeby badań, chyba że wyrazi sprzeciw (poprzez zatelefonowanie pod wskazany numer).

Jak wspomniano w rozdziale II.A.2, jednostki mogą udzielić jednoznacznej zgody, zarówno ustnie jak i na piśmie, poprzez zaangażowanie w działanie wyrażające pragnienie, aby zgodzić się na jakąś formę przetwarzania danych. W środowisku *on-line* udzielenie wyraźnej zgody może być dokonane za pomocą elektronicznego lub cyfrowego podpisu. Jednakże można ją również wyrazić, w zależności od kontekstu, za pomocą aktywnych przycisków, e-maili potwierdzających, klikając na ikony, itp.³². Zatwierdzenie procedur, które pociągają za sobą pozytywne działanie osoby fizycznej jest wyraźnie wskazane w motywie 17 dyrektywy o prywatności i łączności elektronicznej, który stwierdza, że „*Zgoda może być udzielona w jakikolwiek sposób umożliwiający swobodne i świadome wyrażenie woli użytkownika, włączając zaznaczenie okna wyboru podczas przeglądania witryny internetowej*”.

Zgoda nie musi być możliwa do zarejestrowania, aby była ważna. Jednak jest to w interesie administratora danych, aby zachować dowód (udzielenia zgody). Oczywiście siła dowodu uzyskanego za pomocą danego mechanizmu może się różnić, dostarczając mniej lub bardziej wiarygodnego potwierdzenia udzielenia zgody. Zgoda, która została uzyskana przy pomocy kliknięcia przycisku w przypadku, gdy tożsamość osoby fizycznej została potwierdzona na podstawie adresu poczty elektronicznej, będzie miała o wiele mniejszą wartość dowodową niżeli zgoda uzyskana przy pomocy mechanizmu, na przykład, umożliwiającego zarejestrowanie udzielenia zgody³³. Potrzeba uzyskania

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

³² Interpretacja ta jest zgodna z prawodawstwem UE, głównie w sprawie handlu elektronicznego oraz szerszego wykorzystania podpisu cyfrowego, które zobowiązywało państwa członkowskie do zmiany przepisów zawierających wymogi formalne dotyczące dokumentów, aby były „na piśmie” i „odręczne”, tak aby ich elektroniczne odpowiedniki były powszechnie przyjęte, jeśli spełnione są określone warunki.

³³ W związku z tym, warto przyjrzeć się na przykład greckiemu i niemieckiemu prawu dotyczącemu wymogów udzielenia zgody w formie elektronicznej, które zobowiązują, by zgoda była rejestrowana w sposób bezpieczny, dostępna dla użytkownika lub abonenta w każdej chwili i odwołalna w każdym czasie (art. 5 ust. 3 greckiej ustawy 3471/2006 w sprawie ochrony danych osobowych w sektorze łączności elektronicznej; art. 13 ust. 2 niemieckiej ustawy o usługach telekomunikacyjnych (ang. *teleservices*), art. 94 niemieckiej ustawy o telekomunikacji, oraz art. 28 ust. 3a niemieckiej ustawy federalnej o ochronie danych).

silnych dowodów zależeć będzie także od rodzaju gromadzonych danych oraz celów (przetwarzania): podpis elektroniczny nie będzie potrzebny do wyrażenia zgody na otrzymywanie ofert handlowych, ale może być konieczny do wyrażenia zgody na przetwarzanie niektórych typów danych finansowych *on-line*. Wyrażna zgoda udzielona w środowisku *on-line* powinna być możliwa do zarejestrowania w taki sposób, aby była możliwa do wykorzystania w kolejnych odniesieniach.³⁴

W świetle powyższego, formularze rejestracji *on-line*, w których osoby fizyczne podadzą dane ich identyfikujące wraz z wyrażeniem swojego przyzwolenia na przetwarzanie, będą uznane za spełniające wymóg wyrażnej zgody, pod warunkiem że wszystkie inne wymogi zostaną spełnione. Na przykład, aby otworzyć zindywidualizowaną dokumentację medyczną *on-line* pacjenci mogą wyrazić zgodę poprzez podanie swoich danych kontaktowych i zaznaczenie odpowiedniego pola wyboru oznaczającego ich przyzwolenie. Użycie silniejszych metod uwierzytelniania - na przykład, korzystania z podpisów cyfrowych - osiągnie ten sam wynik i stanowić będzie mocniejszy dowód³⁵.

W niektórych przypadkach państwa członkowskie mogą zdecydować, że dana operacja przetwarzania danych musi być umocowana na podstawie zgody oraz określić typ zgody. Na przykład, aby ubiegać się o kartę zdrowia umożliwiającą dostęp do dokumentacji medycznej, państwa członkowskie mogą postanowić, że osoby fizyczne, które rejestrują się *on-line*, muszą podpisać się szczególnym podpisem cyfrowym. Ta opcja zapewni, że zgoda jest wyraźna; daje również administratorowi danych większą pewność, że będzie w stanie udowodnić udzielenie zgody przez osobę fizyczną.

III.A.4. Art. 26 ust. 1

Art. 26 ust. 1 lit. a) przewiduje jednoznaczną zgodę osoby, której dane dotyczą, jako wyjątek od zakazu przekazywania danych do państw trzecich niezapewniających odpowiedniego poziomu ochrony. Powyższe rozważania dotyczące art. 7 lit. a) mają również zastosowanie w tym przypadku. Oznacza to, że oprócz wymogów dotyczących ważnej zgody *ex art. 2 lit. g)*, zgoda musi być jednoznaczna.

Grupa Robocza Art. 29 poświęciła wiele wysiłku, aby zapewnić wsparcie w zakresie stosowania art. 25 i 26 dyrektywy, również w sprawie wyjątku zgody. W tym kontekście warto przypomnieć dokument roboczy Grupy Roboczej WP 12³⁶, co do rozumienia jednoznacznej zgody: *„Ponieważ zgoda musi być jednoznaczna, wszelkie wątpliwości co do faktu, czy zgoda została udzielona także sprawiają, że wyjątek nie ma zastosowania. Prawdopodobne jest to, że w wielu sytuacjach, w których zgoda jest domyślna, (np. w przypadku, gdy osoba fizyczna została poinformowana o przekazaniu danych i nie wyraziła sprzeciwu) nie kwalifikuje się do tego zwolnienia”*.

³⁴ Poza zakresem niniejszej Opinii jest analiza warunków technicznych, które muszą być spełnione przez dokumenty elektroniczne i podpisy, aby była im przyznana równoważna wartość dowodowa w porównaniu z ich odrębnymi odpowiednikami. Jest to kwestia, która wykracza poza przepisy o ochronie danych i która została uregulowana na poziomie UE.

³⁵ Ma to miejsce ze względu na to, iż korzystanie z niektórych rodzajów podpisów cyfrowych (zaawansowane podpisy elektroniczne oparte o kwalifikowany certyfikat i złożone za pomocą bezpiecznego urządzenia do składania podpisów) są automatycznie uznawane za zapewniające taką samą wartość prawną jak dowody pisemne.

³⁶ WP 12 - Dokument roboczy w sprawie przekazywania danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych, przyjętego w dniu 24 lipca 1998 roku.

W świetle powyższego, uzyskanie jednoznacznej zgody jest bardziej prawdopodobne, gdy ludzie zaangażują się w pozytywne działania oznaczające przyzwolenie na przekazanie, na przykład poprzez podpisanie formularza zgody lub zaangażowanie się w inne działania, które nie budzą wątpliwości, że zgoda została udzielona.

W dokumencie WP 114³⁷ dotyczącego stosowania zgody na przekazywanie danych, Grupa Robocza stwierdziła, że: „... zgoda wyrażona przez podmiot danych 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 nierozzerwalną część 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 fizycznej, 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 nie posiadających pełnej zdolności do czynności prawnych

Zgodnie z dyrektywą 95/46/WE nie ma szczególnych przepisów dotyczących uzyskania zgody osób fizycznych nie posiadających pełnej zdolności do czynności prawnych, w tym dzieci. Ważne jest, aby wziąć to pod uwagę w kontekście przeglądu dyrektywy o ochronie danych. Oprócz kwestii poruszonych powyżej, uzyskanie zgody tych osób fizycznych wiąże się ze specyficznymi problemami.

W odniesieniu do dzieci, warunki udzielenia ważnej zgody mogą różnić się w zależności od danego państwa członkowskiego. Grupa Robocza Art. 29, przy różnych okazjach, analizowała kwestie związane z udzielaniem zgody przez dzieci i badała praktyki krajowe³⁸.

Dotychczasowe badania pokazują, że kiedy potrzebna jest zgoda dziecka, prawo może wymagać uzyskania zarówno zgody dziecka, jak i jej przedstawiciela prawnego, lub jedynie zgody dziecka, jeżeli osoba ta jest już pełnoletnia. Wiek, w zależności kiedy stosuje się jedną lub drugą zasadę, różni się. Brak jest zharmonizowanych procedur weryfikacji wieku dziecka.

Brak ogólnych zasad w tym zakresie prowadzi do fragmentarycznego podejścia i brak jest uznania potrzeby szczególnej ochrony dzieci w szczególnych okolicznościach, ze względu na ich podatność, i dlatego że tworzona jest niepewność prawna, zwłaszcza jeśli chodzi o sposób uzyskania zgody dzieci.

³⁷ WP 114 - 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.

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).

Grupa Robocza uważa, że brak harmonizacji ma konsekwencje w zakresie pewności prawnej. Harmonizacja warunków umożliwiających osobom fizycznym nie posiadającym pełnej zdolności do czynności prawnych korzystanie ze swoich praw na szczeblu UE, zwłaszcza w odniesieniu do progu wieku, z pewnością przyniosłaby dodatkowe gwarancje. Jednak Grupa Robocza ma świadomość, że sprawy te mogą wykraczać poza zakres ochrony danych i dotyczyć bardziej ogólnych zagadnień cywilnoprawnych. Grupa Robocza zwraca uwagę Komisji na wyzwania wskazane w tej dziedzinie.

Ponadto, Grupa Robocza Art. 29 uważa, że interesy dzieci i innych osób fizycznych nie posiadających pełnej zdolności do czynności prawnych będą lepiej chronione, jeśli dyrektywa zawierałaby dodatkowe przepisy, w szczególności dotyczące gromadzenia i dalszego przetwarzania ich danych. Przepisy te mogłyby przewidywać okoliczności, w których zgoda przedstawiciela ustawowego byłaby wymagana, wraz z, lub w miejsce, zgody osoby fizycznej nie posiadającej pełnej zdolności do czynności prawnych; mogłyby również przewidywać okoliczności, w których niemożliwe byłoby wykorzystywanie zgody jako podstawy dla legalnego przetwarzania danych osobowych. Powinny one również przewidywać wymóg stosowania mechanizmów weryfikacji wieku *on-line*. Istnieją różne mechanizmy i różne progi (wieku). Na przykład, weryfikacja wieku, zamiast podlegać jednej regule, mogłaby być oparta na 'podejściu ruchomej skali', przy czym wykorzystywany mechanizm zależałby od okoliczności, takich jak rodzaj przetwarzania (cele), czy szczególnie ryzykowne, rodzaj gromadzonych danych, cele przetwarzania, (czy dane te są przeznaczone do ujawnienia), itp.

III.B. Dyrektywa 2002/58/WE

Niedawno nowelizowana dyrektywa o prywatności i łączności elektronicznej (dyrektywa 2002/58/WE)³⁹ stanowi *lex specialis* w stosunku do dyrektywy 95/46/WE, w zakresie, w jakim proponuje specjalny reżim sektorowy w odniesieniu do prywatności i łączności elektronicznej. Większość jej przepisów stosuje się wyłącznie do dostawców publicznie dostępnych usług łączności elektronicznej (np. dostawców telefonii, dostawców usług internetowych, itp.).

Niektóre z przepisów dyrektywy o prywatności i łączności elektronicznej bazują na zgodzie jako podstawie prawnej, na której dostawcy publicznie dostępnych usług łączności elektronicznej mogą przetwarzać dane⁴⁰. Tak jest w przypadku na przykład korzystania z danych o ruchu lub danych dotyczących lokalizacji.

Grupa Robocza Art. 29 uważa za przydatne skomentowanie wybranych aspektów związanych z wykorzystaniem zgody w ramach dyrektywy o prywatności i łączności elektronicznej, które są przedmiotem szczególnego zainteresowania. W tym celu zajmiemy się pięcioma następującymi zagadnieniami:

³⁹ Dyrektywa 2009/136/WE Parlamentu Europejskiego i Rady 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 dane przetwarzane dla celów przekazywania komunikatów w sieci łączności elektronicznej lub dane do rozliczeń w odniesieniu do tej komunikacji, w tym danych odnoszących się do wyznaczania trasy, długości i czasu komunikacji.

a) Związek między definicją i ogólnym znaczeniem zgody, między dyrektywą 95/46/WE a dyrektywą o prywatności i łączności elektronicznej. Oparte jest to na art. 2 ust. 2 lit. f) dyrektywy o prywatności i łączności elektronicznej.

b) Pytanie, czy do naruszenia poufności komunikacji (np. do monitorowania lub przechwycenia komunikacji telefonicznej) konieczne jest uzyskanie zgody jednej lub obu stron komunikacji. Regulowane jest to przez art. 6 ust. 3 oraz ust. 5 pkt. 1.

c) Pytanie o czas, kiedy należy uzyskać zgodę. Omawiane jest to w różnych przepisach dyrektywy o prywatności i łączności elektronicznej, w tym art. 5 ust. 3, art. 6 oraz art. 13.

d) Zakres stosowania prawa do sprzeciwu i jego odróżnienie od zgody. Rozróżnienie to należy analizować pod kątem art. 13 dyrektywy o prywatności i łączności elektronicznej.

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

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

„zgoda użytkownika lub abonenta”

Art. 2 dyrektywy o prywatności i łączności elektronicznej wyraźnie stwierdza, że definicje zawarte w dyrektywie 95/46/WE stosuje się względem dyrektywy 2002/58/WE. Art. 2 lit. f) stanowi, że *„zgoda użytkownika lub abonenta odpowiada zgodzie osoby, której dane dotyczą, określonej w dyrektywie 95/46/WE”*.

Oznacza to, że gdy zgoda jest wymagana w ramach dyrektywy o prywatności i łączności elektronicznej, kryteria ustalenia, czy zgoda jest ważna są takie same jak te określone w dyrektywie 95/46/WE, a mianowicie zgodnie z definicją w art. 2 lit. g), doprecyzowaną w art. 7 lit. a). Pogląd, że zgodę w dyrektywie o prywatności i łączności elektronicznej należy rozumieć w odniesieniu do art. 2 lit. g) oraz art. 7 lit. a) potwierdzony jest w motywie 17⁴¹.

III.B.2. Art. 5 ust. 1 – Czy zgoda jest wymagana od jednej strony czy dwóch stron

„... zgoda zainteresowanych użytkowników...”

Art. 5 ust. 1) dyrektywy o prywatności i łączności elektronicznej chroni poufność komunikacji poprzez zakaz jakiegokolwiek przejęcia lub nadzoru komunikatu bez zgody wszystkich zainteresowanych użytkowników.

W tym przypadku, art. 5 ust. 1 wymaga zgody „wszystkich zainteresowanych użytkowników”, innymi słowy, obu strony komunikacji. Zgoda jednej ze stron jest nie wystarczająca.

⁴¹ Stanowi on, że: *„Do celów niniejszej dyrektywy, zgoda... powinna mieć to samo znaczenie co zgoda podmiotu danych opisana i szerzej określona w dyrektywie 95/46/WE.”*

W kontekście opracowywania Opinii 2/2006⁴², Grupa Robocza Art. 29 przeanalizowała kilka usług, które polegały na skanowaniu treści e-maili i, w niektórych przypadkach, śledzenie otwierania e-maili. Grupa Robocza wyraziła obawę, że w takich usługach jedna ze stron komunikacji nie została poinformowana. Aby usługi te były zgodne z art. 5 ust. 1 zgoda obu stron komunikacji jest konieczna.

III.B.3 Art. 6 ust. 3, art. 9, art. 13 oraz art. 5 ust. 3 – Określenie sytuacji, w których zgoda jest wymagana

„... po otrzymaniu jasnych i wyczerpujących informacji ...”

Szereg przepisów dyrektywy o prywatności i łączności elektronicznej zawiera wyraźny lub dorozumiany tekst wskazujący, że zgoda musi być uzyskana przed rozpoczęciem przetwarzania. Jest to zgodne z dyrektywą 95/46/WE.

Art. 6 ust. 3 dyrektywy o prywatności i łączności elektronicznej zawiera wyraźne odniesienie do uprzedniej zgody zainteresowanych użytkowników i abonentów, określającego obowiązek udzielania informacji i uzyskania uprzedniej zgody przed rozpoczęciem przetwarzania danych o ruchu dla celów marketingu usług łączności elektronicznej lub usług o wartości dodanej. W przypadku niektórych rodzajów usług, zgodę można uzyskać od abonenta w momencie subskrypcji usługi. W innych przypadkach uzyskanie zgody może być możliwe bezpośrednio od użytkownika. Podobne podejście zostało przyjęte w art. 9 dotyczącym 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. Art. 13 określa wymóg uzyskania uprzedniej zgody od abonentów do korzystania z automatycznych systemów wywołujących bez ludzkiej ingerencji, faksem lub e-mailem dla celów marketingu bezpośredniego.

Art. 5 ust. 3) zawiera szczegółowe regulacje dotyczące przechowywania informacji lub uzyskania dostępu do informacji na terminalu użytkownika, w tym w celu śledzenia działań użytkownika *on-line*. Podczas gdy art. 5 ust. 3 nie stosuje słowa „uprzednia”, jest to jasny i oczywisty wniosek z treści tego przepisu.

Sensowne jest uzyskanie zgody przed rozpoczęciem przetwarzania danych. W przeciwnym razie, przetwarzanie przeprowadzone od momentu rozpoczęcia przetwarzania do chwili uzyskania zgody byłoby niezgodne z prawem z powodu braku podstawy prawnej. Ponadto w takich przypadkach, jeżeli osoba fizyczna nie wyraziłaby zgody, wszelkie przetwarzanie danych, które miałyby miejsce do tego momentu, byłoby niezgodne z prawem z tego samego powodu.

Wynika z tego, że gdy zgoda jest *wymagana*, należy ją uzyskać przed rozpoczęciem przetwarzania danych. Możliwość rozpoczęcia przetwarzania bez uzyskania uprzedniej zgody jest zgodna z prawem tylko w przypadku, gdy dyrektywa o ochronie danych lub dyrektywa o prywatności i łączności elektronicznej nie wymaga zgody lecz zapewnia alternatywną podstawę prawną i odnosi się do prawa sprzeciwu lub odmowy przetwarzania. Mechanizmy te są wyraźnie oddzielone od zgody. W tych przypadkach

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

przetwarzanie danych może już się rozpocząć, a osoba fizyczna ma prawo do sprzeciwu lub odmowy.

Przykład tego można znaleźć w art. 5 ust. 3 poprzedniej dyrektywy o prywatności i łączności elektronicznej, który stanowi (dodane podkreślenie), że: „*korzystanie z sieci łączności elektronicznej w celu przechowywania informacji lub uzyskania dostępu do informacji przechowywanych w urządzeniach końcowych abonenta lub użytkownika jest dozwolone tylko pod warunkiem, że abonent lub użytkownik otrzyma jasne i wyczerpujące informacje zgodnie z dyrektywą 95/46/WE, między innymi o celach przetwarzania, oraz zostanie zaoferowane mu prawo do odmówienia zgody na takie przetwarzanie przez administratora danych.*”. Powinno to być porównane z nowym brzmieniem art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej zmienionej dyrektywą 2009/136/WE⁴³, który stwierdza, że: „*(...) przechowywanie informacji lub uzyskiwanie dostępu do informacji już zapisanych w urządzeniu końcowym abonenta lub użytkownika jest dozwolone tylko pod warunkiem, że abonent lub dany użytkownik udzielił swojej zgody (...)*”. Konsekwencje tej zmiany w treści art. 5 ust. 3 zostały wyjaśnione przez Grupę Roboczą Art. 29 w Opinii 2/2010 w sprawie internetowej reklamy behawioralnej⁴⁴. Różnica między odmową a zgodą jest również bardziej wyjaśniona w następnym rozdziale.

W wielu przypadkach, tam gdzie dyrektywa o prywatności i łączności elektronicznej lub dyrektywa o ochronie danych przewidują możliwość odmowy przetwarzania danych osobowych, przyczyną jest to, że podstawą prawną do wstępnego przetwarzania danych jest podstawa prawna inna niż zgoda, np. istniejąca umowa. Jest to bardziej opisane w następnej sekcji, która komentuje art. 13 dyrektywy o prywatności i łączności elektronicznej.

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

„... klienci zostali jasno i wyraźnie poinformowani o możliwości wyrażenia sprzeciwu...”

Art. 13 dyrektywy o prywatności i łączności elektronicznej przewiduje stosowanie zgody w celu wysłania komunikatów elektronicznych do celów marketingu bezpośredniego zgodnie z prawem. Czyni to opierając się na standardowych zasadach i przepisach szczególnych.

Jeśli chodzi o wykorzystanie urządzeń do wywołań automatycznych, telefaksów i poczty e-mail, wymagane jest uzyskanie uprzedniej zgody podmiotu danych.

Jeśli adresat handlowego przekazu to istniejący klient i dany komunikat ma na celu promowanie własnych produktów lub usług usługodawcy lub podobnych produktów lub usług, wymóg nie dotyczy zgody, ale zapewnienia, że osoba fizyczna ma możliwość skorzystania z prawa sprzeciwu z art. 13 ust. 2. Motyw 41 preambuły wyjaśnia,

⁴³ Dyrektywa 2009/136/WE Parlamentu Europejskiego i Rady 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. Urz. L 337, 18/12/2009, str. 0011 – 0036.*

⁴⁴ Opinia z dnia 22 czerwca 2010 r., WP 171: kwestia, czy zgoda może być wyrażona przez „odpowiednie ustawienia w przeglądarce internetowej lub innej aplikacji” [motyw 66 dyrektywy 2009/136/WE] jest szczegółowo opisana w pkt 4.1.1 WP 171.

dlaczego ustawodawca w tym przypadku nie wymaga zgody: „*W kontekście istniejącej relacji z klientem, uzasadnione staje się zezwolenie wykorzystywania szczegółowych elektronicznych danych kontaktowych w celu oferowania podobnych produktów lub usług...*”. Tak więc, w zasadzie, stosunek umowy pomiędzy osobą fizyczną a dostawcą usług jest podstawą prawną, która umożliwia pierwszy kontakt przez e-mail. Jednakże osoby fizyczne powinny mieć możliwość sprzeciwienia się dalszym kontaktom. Jak wskazała już Grupa Robocza: „Ta możliwość powinna nadal być oferowana w każdej kolejnej wiadomości marketingu bezpośredniego, bezpłatnie, za wyjątkiem kosztów transmisji odmowy”.⁴⁵

Potrzeba zgody powinna być odróżniona od prawa do wyrażenia sprzeciwu. Jak przedstawiono powyżej w rozdziale III.A.2, zgoda udzielona na podstawie braku działań osoby fizycznej, na przykład poprzez uprzednie wybranie pola wyboru, nie spełnia wymagań ważnej zgody na mocy dyrektywy 95/46/WE. Ten sam wniosek odnosi się do ustawień przeglądarki internetowej, które akceptują domyślnie ukierunkowanie użytkownika (za pomocą plików *cookies*). Jest to jasno określone w nowym brzmieniu art. 5 ust. 3 cytowanego powyżej w rozdziale III.B.3. Te dwa przykłady nie spełniają w szczególności wymagania jednoznacznego wskazania woli (osoby). Istotne jest, aby osoba, której dane dotyczą, miała możliwość podjęcia decyzji oraz jej wyrażenia, na przykład samemu zaznaczając pole wyboru, w świetle celu przetwarzania danych.

W opinii na temat reklamy behawioralnej, Grupa Robocza stwierdziła, że „wydaje się, że zasadnicze znaczenie ma wprowadzenie w przeglądarkach internetowych 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 internetowe powinny wymagać od użytkowników przejścia kreatora prywatności, kiedy po raz pierwszy instalują bądź aktualizują przeglądarkę oraz zapewnienia możliwości łatwego dokonywania wyboru podczas użytkowania⁴⁶.

III.B.5. Art. 6 ust. 3, art. 9 ust. 3 i 4 - możliwość odwołania zgody

„... możliwość odwołania zgody w każdej chwili...”

Możliwość odwołania zgody, co jest dorozumiane w dyrektywie 95/46/WE, omówiona jest w szeregu przepisów dyrektywy o prywatności i łączności elektronicznej. Było to wyraźnie wskazane w Opinii Grupy Roboczej w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną⁴⁷:

„Na mocy art. 9 dyrektywy 2002/58/WE osoby fizyczne, 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

⁴⁵ Opinia 5/2004 w sprawie niezamówionych komunikatów do celów marketingowych 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, przyjętej w dniu 25 listopada 2005 r. (WP 115).

punktu widzenia 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 fizycznej, że jej urządzenie końcowe zostało, będzie lub może być zlokalizowane. Umożliwi to tej osobie fizycznej wykonanie prawa do wycofania zgody na mocy art. 9 dyrektywy 2002/58/WE, jeżeli będzie chciała z niego skorzystać.”

Jak już wspomniano powyżej, oznacza to, że wycofanie (zgody) dotyczy przyszłości, a nie przetwarzania danych, które miało miejsce w przeszłości, w okresie, w którym dane zostały zgromadzone w sposób zgodny z prawem. Decyzje lub działania wcześniej podjęte na podstawie tych informacji nie mogą być po prostu unieważnione. Jednakże, jeśli nie ma innej podstawy prawnej uzasadniającej dalsze przechowywanie danych, powinny one zostać usunięte przez administratora danych.

IV. Wnioski

Opinia ta odnosi się do ram prawnych dotyczących korzystania ze zgody na mocy dyrektywy 95/46/WE i dyrektywy 2002/58/WE. Cel opinii jest dwójaki: po pierwsze, wyjaśnienie istniejących wymogów prawnych i pokazanie, jak one funkcjonują w praktyce; po drugie, przedstawienie refleksji na temat tego, czy istniejące ramy prawne są wystarczające w świetle wielu nowych sposobów przetwarzania danych osobowych i czy zmiany tych ram są konieczne.

IV.1. Wyjaśnienie kluczowych aspektów obecnych ram prawnych

Art. 2 lit. h) dyrektywy 95/46/WE definiuje 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*”. Art. 7 dyrektywy, który określa podstawę prawną dla przetwarzania danych osobowych, określa *jednoznaczną* zgodę jako jedną z podstaw prawnych. Art. 8 wymaga wyraźnej zgody jako podstawy prawnej do przetwarzania danych wrażliwych. Art. 26 ust. 1 dyrektywy 95/46/WE i niektóre przepisy dyrektywy o prywatności i łączności elektronicznej wymagają zgody jako podstawy do wykonywania określonego przetwarzania danych w zakresie ich stosowania. Punkty opracowane w niniejszej opinii mają na celu wyjaśnienie poszczególnych elementów przedmiotowych ram prawnych w celu ułatwienia ich stosowania przez zainteresowane podmioty.

Uwagi o charakterze ogólnym

- Zgoda jest jednym z sześciu podstaw prawnych do przetwarzania danych osobowych (jedna z pięciu podstaw w przypadku danych szczególnie chronionych); jest ważnym narzędziem, ponieważ daje pewną kontrolę osobie, której dane dotyczą, w odniesieniu do przetwarzania danych jej dotyczących. Znaczenie zgody jako część niezależności i samostanowienia osoby fizycznej zależy od jej użycia w odpowiednim kontekście wraz z niezbędnymi elementami.
- Ogólnie rzecz biorąc, ramy prawne dyrektywy 95/46/WE stosuje się, gdy zgoda jest wymagana, niezależnie od tego, czy ma to miejsce *off-line* czy *on-line*. Na przykład,

te same zasady mają zastosowanie, gdy sprzedawca materiałów budowlanych stara się zapisywać osoby fizyczne do programu lojalnościowego poprzez formę papierową, jak w przypadku, gdyby tak działał za pośrednictwem swojej strony internetowej. Ponadto, dyrektywa o prywatności i łączności elektronicznej określa niektóre operacje przetwarzania danych, do których wymagana jest zgoda: są one związane głównie z przetwarzaniem danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej. Wymagania dotyczące tego, aby zgoda była ważna w dyrektywie 2002/58/WE są takie same, jak w dyrektywie 95/46/WE.

- Sytuacje, w których administratorzy danych używają zgody jako podstawy prawnej do przetwarzania danych osobowych nie powinny być mylone z sytuacjami, w których administrator danych opiera przetwarzanie na innych podstawach prawnych, które pociągają za sobą prawo do sprzeciwu. Na przykład, może być tak w przypadku, gdy przetwarzanie opiera się na „uzasadnionym interesie” administratora danych z art. 7 lit. f) dyrektywy 95/46/WE, ale osoba fizyczna ma prawo do sprzeciwu z art. 14 lit. a) dyrektywy 95/46/WE. Innym przykładem jest sytuacja, w której administrator danych wysła komunikaty za pomocą poczty elektronicznej do dotychczasowych klientów w celu wspierania własnych lub podobnych produktów lub usług administratora danych, niemniej, osoby fizyczne mają prawo do sprzeciwu na podstawie art. 13 ust. 2 dyrektywy 2002/58/WE. W obu przypadkach osoby, której dane dotyczą, mają prawo do wyrażenia sprzeciwu wobec przetwarzania; to jest tożsame ze zgodą.
- Poleganie na zgodzie jako podstawie przetwarzania danych osobowych nie zwalnia administratora danych z obowiązku spełnienia innych wymogów związanych z ramami prawnymi ochrony danych, na przykład, przetwarzania danych zgodnie z zasadą proporcjonalności na podstawie art. 6 ust. 1 lit. c), bezpieczeństwa przetwarzania z art. 17, itp.
- Wyrażenie ważnej zgody zakłada, że osoba fizyczna jest w stanie ją wyrazić. Zasady dotyczące zdolności do wyrażenia zgody nie są ujednolicone i mogą być różnie uregulowane w państwach członkowskich.
- Osoby, które wyraziły zgodę powinny mieć możliwość jej odwołania, co uniemożliwiłoby dalsze przetwarzanie ich danych. Potwierdzone jest to także w dyrektywie o prywatności i łączności elektronicznej dla pewnych operacji przetwarzania danych na podstawie zgody, takich jak przetwarzanie danych dotyczących lokalizacji innych niż dane o ruchu.
- Zgoda musi być udzielona przed rozpoczęciem przetwarzania danych osobowych, ale może być również wymagana w trakcie przetwarzania, gdy dane przetwarzane są w nowym celu. Podkreślone jest to w różnych przepisach dyrektywy 2002/58/WE, poprzez wymóg „uprzedniej” [zgody] (np. art. 6 ust. 3) bądź też poprzez samo brzmienie przepisów (np. art. 5 ust. 3).

Poszczególne elementy ram prawnych dotyczących zgody

- Aby zgoda była ważna, musi być *udzielona dobrowolnie*. Oznacza to, że nie może być ryzyko oszustwa, zastraszenia lub znaczącego negatywnego skutku dla osoby, której dane dotyczą, jeśli dana osoba nie wyrazi zgody. Operacje przetwarzania danych w środowisku pracy, gdzie występuje element podporządkowania, jak również w kontekście usług publicznych, takich jak sektor zdrowia, może wymagać uważnej oceny, czy osoba fizyczna może swobodnie udzielić zgody.
- Zgoda musi być *konkretna*. Zgoda blankietowa bez określenia dokładnych celów nie spełnia tego wymogu. Zamiast wstawiania informacji w ogólnych warunkach

- umowy, wymaga to zastosowania specjalnych klauzul zgody, oddzielonych od ogólnych warunków (umowy).
- Zgoda musi być *świadoma*. Art. 10 i 11 dyrektywy wymienia rodzaje informacji, które muszą obowiązkowo być przekazane osobie fizycznej. W każdym razie podane informacje muszą być wystarczające, aby zagwarantować, że osoby fizyczne będą mogły podejmować świadome decyzje dotyczące przetwarzania ich danych osobowych. Potrzeba, aby zgoda była „świadoma” przekłada się na dwa dodatkowe wymagania. Po pierwsze, sposób, w jaki informacja jest podawana musi zapewnić stosowanie właściwego języka, tak aby osoba, której dane dotyczą, mogła zrozumieć, na co wyraża zgodę na i do jakich celów. Jest to zależne od kontekstu. Stosowanie zbyt skomplikowanego żargonu prawnego lub technicznego nie spełniłoby wymogów prawa. Po drugie, informacje dostarczane użytkownikom powinny być jasne i dostatecznie widoczne, tak, aby użytkownicy ich nie pominęli. Informacje muszą być przekazywane bezpośrednio osobom fizycznym. Nie wystarczy, aby były tylko gdzieś dostępne.
 - Zgodnie z art. 8 ust. 2 przetwarzanie danych wrażliwych wymaga, aby zgoda była wyraźna, czyli przejaw czynnego działania, ustnego lub na piśmie, w którym osoba fizyczna wyraża swoje zamiary dotyczące przetwarzania jej danych dla określonych celów. Dlatego wyraźna zgoda nie może być udzielona za pomocą wcześniej zaznaczonego pola wyboru. Osoba, której dane dotyczą, musi podjąć pewne pozytywne działania oznaczające wyrażenie zgody i musi również mieć możliwość nie udzielenia zgody.
 - W przypadku innych danych niżeli dane wrażliwe, art. 7 lit. a) wymaga, aby zgoda była jednoznaczna. „Jednoznaczność” wymaga korzystania z mechanizmów, które nie pozostawiają wątpliwości co do zamiaru wyrażenia zgody przez osobę fizyczną. W praktyce wymóg ten umożliwi administratorom danych korzystanie z różnych rodzajów mechanizmów uzyskiwania zgody, od oświadczeń wskazujących przyzwolenie do mechanizmów, które opierają się na działaniach mających na celu wskazanie przyzwolenia.
 - Zgoda na podstawie bezczynności lub milczenia zwykle nie stanowi ważnej zgody, zwłaszcza w kontekście *on-line*. Jest to problem, który pojawia się w szczególności w odniesieniu do korzystania z domyślnych ustawień, które osoba, której dane dotyczą, musi zmienić, aby odmówić przetwarzania. Na przykład, ma to miejsce w przypadku stosowania wstępnie zaznaczonego ustawienia przeglądarki internetowej, które są domyślnie ustawione do zbierania danych.

IV.2 Oceny obecnych ram i ewentualnej konieczności zmiany

Ogólna ocena

Grupa Robocza uważa, że obecne ramy ochrony danych zawierają dobrze przemyślany zestaw reguł, które ustanawiają warunki udzielania ważnej zgody w celu zalegalizowania operacji przetwarzania danych. Mają one zastosowanie zarówno w środowiskach *off-line*, jak i *on-line*. W szczególności:

Ramy prawne z powodzeniem zapewniają bilansowanie pewnych zagadnień. Z jednej strony gwarantują, że tylko prawdziwie świadoma zgoda jest zgodą jako taką. W związku z tym, art. 2 lit. h) wyraźnie wymaga, aby zgoda była dobrowolna, konkretna i świadoma, oraz odpowiednia i wystarczająca. Z drugiej strony, wymóg ten nie jest sztywną regułą, ale raczej zapewnia wystarczającą elastyczność, unikając

technologicznie zależnych przepisów szczególnych. Przedstawione jest to w tym samym art. 2 lit. h), gdzie określona jest zgoda jako wskazanie woli osoby fizycznej. Daje to pole manewru w zakresie sposobu, w jaki określenie woli może być dokonane. Art. 7 i 8, wymagające odpowiednio jednoznacznej i wyraźnej zgody, dobrze ujmują konieczność zachowania równowagi pomiędzy dwoma wymaganiami, tj. zapewnieniu elastyczności i unikaniu zbyt sztywnych struktur, przy jednoczesnym zapewnieniu ochrony.

W rezultacie istnieją ramy, które, jeśli są prawidłowo stosowane i wdrażane, są w stanie dotrzymać kroku różnym operacjom przetwarzania danych, które często wynikają z rozwoju technologicznego.

W praktyce jednak, ustalenie, kiedy zgoda jest potrzebna, a w szczególności wymagania dotyczące ważnej zgody, w tym sposobów prawidłowego stosowania, nie zawsze jest łatwe ze względu na brak jednolitości pomiędzy państwami członkowskimi. Wdrożenie na szczeblu krajowym zaowocowało różnymi podejściami. Bardziej szczegółowe niedociągnięcia zostały zidentyfikowane podczas dyskusji w ramach Grupy Roboczej Art. 29, które przyczyniły się do powstania tej Opinii. Zostały opisane bardziej szczegółowo poniżej.

Ewentualne zmiany

- Pojęcie jednoznacznej zgody jest pomocne dla opracowania systemu, który nie jest zbyt sztywny, ale zapewnia silną ochronę. Mimo, że ma potencjał, aby doprowadzić do utworzenia rozsądnego systemu, niestety jego znaczenie jest często źle rozumiane lub po prostu ignorowane. Choć przykłady wymienione powyżej powinny przyczynić się do zwiększenia pewności prawnej i ochrony praw jednostki w przypadku, gdy zgoda jest używana jako podstawa prawna, powyższa sytuacja wydaje się wskazywać na konieczność dokonania pewnych zmian.
- W szczególności Grupa Robocza Art. 29 uważa, że samo słowo („jednoznaczna”) mogłoby zyskać na większej klarowności w ramach przeglądu ogólnych ram ochrony danych. Wyjaśnienie powinno mieć na celu podkreślenie, że udzielenie jednoznacznej zgody wymaga zastosowania mechanizmów, które nie pozostawiają żadnych wątpliwości co do zamiarów osoby, której dane dotyczą, co do jej wyrażenia. Jednocześnie należy wyjaśnić, że korzystanie z domyślnych ustawień, które osoba, której dane dotyczą, jest zobowiązana zmodyfikować, aby odmówić przetwarzania (zgoda oparta o milczenie) nie stanowi samo w sobie jednoznacznej zgody. Jest to szczególnie istotne w środowisku *on-line*.
- W uzupełnieniu do wyjaśnień opisanych powyżej, Grupa Robocza Art. 29 proponuje następujące:
 - i. *Po pierwsze*, dodanie do definicji zgody w art. 2 lit. h) słowa „jednoznaczne” (lub słowo równoważne) w celu wzmocnienia przekonania, że tylko zgoda oparta na oświadczeniach lub działaniach wyrażających przyzwolenie stanowi ważną zgodę. Oprócz zwiększenia przejrzystości, dostosowałoby to definicję zgody na podstawie art. 2 lit. h) do wymagań ważnej zgody na mocy art. 7. Ponadto, znaczenie słowa „jednoznaczne” mogłoby zostać bardziej szczegółowo wyjaśnione w motywie przyszłego aktu prawnego.
 - ii. *Po drugie*, w kontekście ogólnego obowiązku rozliczalności, administrator danych powinien być w stanie wykazać, że zgoda została

udzielona. Rzeczywiście, jeśli ciężar dowodu jest wzmocniony tak, aby administratorzy danych mieli obowiązek wykazać, że faktycznie uzyskali zgodę osoby, której dane dotyczą, to będą zmuszeni do wprowadzenia standardowych praktyk i mechanizmów pozyskiwania i udowodnienia jednoznacznej zgody. Typ wykorzystanego mechanizmu zależeć będzie od kontekstu i powinien brać pod uwagę fakty i okoliczności przetwarzania, w szczególności związane z ryzykiem.

- Grupa Robocza Art. 29 nie jest przekonana, że przyszłe ramy prawne powinny wymagać wyraźnej zgody co do zasady dla wszystkich rodzajów operacji przetwarzania danych, w tym obecnie objętych art. 7 dyrektywy. Uważa, że jednoznaczna zgoda, która obejmuje wyraźną zgodę, ale także zgodę wynikającą z jednoznacznego działania, powinna pozostać obowiązującą normą. Wybór ten daje większą elastyczność dla administratorów danych do zbierania zgód i cała procedura może być przez to szybsza i bardziej przyjazna dla użytkownika.
- Niektóre aspekty ram prawnych, które dotyczą zgody wynikają z samej treści, historii prawnej bądź zostały rozwinięte przez orzecznictwo oraz opinie Grupy Roboczej Art. 29. Zapewniłoby to większą pewność prawną, jeżeli takie elementy zostałyby wyraźnie wbudowane w nowe ramy prawne ochrony danych. Następujące punkty mogłyby zostać wzięte uwagę:
 - i. Włączenie klauzuli ustanawiającej prawo osoby fizycznej do wycofania zgody.
 - ii. Wzmocnienie poglądu, że zgoda musi być udzielona przed rozpoczęciem przetwarzania lub przed dalszym wykorzystaniem danych dla celów nieobjętych wstępną zgodą, w przypadkach gdzie nie istnieje żadna inna podstawa prawna do przetwarzania.
 - iii. Włączenie wyraźnych wymogów w zakresie jakości (obowiązek dostarczenia informacji na temat przetwarzania danych w sposób, który jest łatwy do zrozumienia, przejrzysty i prosty) i dostępności informacji (obowiązek, aby informacje były widoczne, wystarczające i bezpośrednio dostępne). Jest to niezbędne do umożliwienia osobom fizycznym podejmowania świadomych decyzji.
- Wreszcie, w odniesieniu do osób fizycznych nie posiadających pełnej zdolności do czynności prawnych, wprowadzenie przepisów zapewniających lepszą ich ochronę, w tym:
 - i. Doprecyzowanie okoliczności, w których wymagana jest zgoda rodziców lub przedstawicieli prawnych osoby fizycznej nie posiadającej pełnej zdolności do czynności prawnych, w tym granicy wieku, poniżej której taka zgoda będzie obowiązkowa.
 - ii. Ustanowienie obowiązku stosowania mechanizmów weryfikacji wieku, które mogą się różnić w zależności od okoliczności, takich jak wiek dziecka, typ przetwarzania danych, czy przetwarzanie stwarza szczególne ryzyko, i czy informacje będą przechowywane przez administratora danych lub udostępniane osobom trzecim;
 - iii. Zobowiązanie do dostosowania informacji dla dzieci, o ile to ułatwiłoby dzieciom zrozumienie, co to znaczy, gdy dane są od nich zbierane, a tym samym stanowiłoby to zgodę;
 - iv. Szczególne zabezpieczenia względem pewnych rodzajów przetwarzania danych, takich jak w przypadku reklamy behawioralnej,

gdzie zgoda nie powinna być możliwą podstawą legalizującą przetwarzanie danych osobowych.

Grupa Robocza Art. 29 planuje zająć się tą tematyką ponownie w przyszłości. W szczególności krajowe organy ochrony danych, jak również Grupa Robocza, mogą podjąć decyzję, na dalszym etapie prac, o przygotowaniu wytycznych doprecyzowujących niniejszą Opinię, zapewniając dodatkowe praktyczne przykłady związane z wykorzystaniem zgody.

Sporządzono w Brukseli dnia 13 lipca 2011 r.

W imieniu Grupy Roboczej

*Przewodniczący
Jacob KOHNSTAMM*