GRUPA ROBOCZA DS. OCHRONY DANYCH POWOŁANA NA MOCY ART. 29

0836-02/10/PL
WP 179

Opinia 8/2010 w sprawie prawa właściwego

przyjęta w dniu 16 grudnia 2010 r.

Streszczenie

W niniejszej opinii wyjaśniony zostaje zakres stosowania dyrektywy 95/46/WE, a w szczególności artykułu 4 tej dyrektywy. We wspomnianym artykule określono, które przepisy prawa krajowego przyjęte na mocy dyrektywy mogą mieć zastosowanie w odniesieniu do przetwarzania danych osobowych. W opinii uwypuklono również kilka obszarów, w których możliwe są dalsze ulepszenia.

Określenie sposobu stosowania przepisów UE w odniesieniu do przetwarzania danych osobowych służy wyjaśnieniu zakresu stosowania unijnych przepisów o ochronie danych zarówno na terytorium UE/EOG jak i w szerszym kontekście międzynarodowym. Jasne zrozumienie prawa właściwego pomoże w zapewnieniu administratorom danych pewności prawa, zaś osobom fizycznym oraz innym zainteresowanym stronom – w ustaleniu wyraźnych ram. Ponadto właściwe zrozumienie przepisów prawa właściwego powinno zagwarantować eliminację luk w zakresie ochrony danych osobowych na tak wysokim poziomie, jaki zapewnia dyrektywa 95/46.

Jeżeli chodzi o art. 4 ust. 1 lit. a), odniesienie do (*jakiejkolwiek*) działalności gospodarczej oznacza, że zastosowanie przepisów jednego z państw członkowskich będzie uwarunkowane miejscem prowadzenia przez administratora danych działalności gospodarczej w danym państwie członkowskim, zaś przepisy innych państw członkowskich mogą zostać zastosowane w związku z inną działalnością gospodarczą tego administratora danych prowadzoną w tych państwach członkowskich. Dla zastosowania przepisów prawa krajowego decydujące znaczenie ma pojęcie „kontekstu działań". Oznacza to, iż *działalność gospodarcza* administratora danych jest zaangażowana w *działania* wiążące się z przetwarzaniem danych osobowych, przy czym uwzględnić należy stopień zaangażowania w działania polegające na przetwarzaniu, charakter działań oraz potrzebę zapewnienia skutecznej ochrony danych.

Jeżeli chodzi o zawarty w art. 4 ust. 1 lit. c) przepis mówiący o „wykorzystaniu środków", który może powodować zastosowanie dyrektywy w odniesieniu do administratorów danych nieprowadzących działalności na terytorium UE/EOG, w opinii doprecyzowano, że powinien mieć on zastosowanie w przypadkach, w których na terytorium UE/EOG nie prowadzi się działalności gospodarczej, która *powodowałaby zastosowanie art. 4 ust. 1 lit. a)*, lub gdy przetwarzanie *nie jest realizowane w kontekście* takiej działalności. W opinii zauważono ponadto, że szeroka interpretacja pojęcia „wyposażenia" – uzasadniona użyciem pojęcia „środki" w innych językach UE – może w niektórych przypadkach prowadzić do zastosowania unijnych przepisów o ochronie danych tam, gdzie przedmiotowe przetwarzanie nie ma faktycznego związku z terytorium UE/EOG.

W opinii zawarto również wskazówki i przykłady dotyczące: pozostałych przepisów zawartych w art. 4; wymogów bezpieczeństwa wypływających z prawa mającego zastosowanie zgodnie z art. 17 ust. 3; możliwości wykorzystywania przez organy ds. ochrony danych ich kompetencji do weryfikowania operacji przetwarzania, które mają miejsce na ich terytorium, oraz do ingerowania w takie operacje – również wtedy, gdy prawem właściwym jest prawo innego państwa członkowskiego (art. 28 ust. 6).

W opinii zasugerowano również, że sformułowania wykorzystane w dyrektywie oraz spójność między poszczególnymi elementami art. 4 zyskałyby dzięki dalszym wyjaśnieniom, które powinny stanowić element rewizji ogólnych ram w zakresie ochrony danych.

Z tego punktu widzenia, uproszczenie zasad określania prawa właściwego obejmowałoby powrót do zasady państwa pochodzenia: do wszelkiej działalności gospodarczej administratora danych prowadzonej w obrębie UE zastosowanie miałyby wówczas te same przepisy (te, które obowiązują w odniesieniu do jego głównej działalności gospodarczej) – niezależnie od terytorium, na którym działalność ta jest prowadzona. Jednak takie rozwiązanie można byłoby przyjąć jedynie wówczas, gdyby przepisy krajowe zostały w dużej mierze zharmonizowane, w tym zharmonizować należałoby również wymogi dotyczące bezpieczeństwa.

W przypadku gdy administrator danych prowadzi działalność poza terytorium UE, zastosowanie mogłyby mieć kryteria dodatkowe w celu zapewnienia, iż istnieje dostateczne powiązanie z

terytorium UE, oraz w celu zapobieżenia sytuacjom, w których administratorzy danych prowadzący działalność gospodarczą w państwach trzecich wykorzystują terytorium UE do podejmowania na nim nielegalnych działań związanych z przetwarzaniem danych. W tym kontekście można zastosować następujące dwa kryteria: ukierunkowania na osoby fizyczne, co prowadziłoby do stosowania unijnych przepisów o ochronie danych, gdy działania wiążące się z przetwarzaniem danych osobowych są ukierunkowane na osoby fizyczne w UE; zastosowania kryterium środków w formie szczątkowej i ograniczonej, co dotyczyłoby przypadków granicznych (dane dotyczące osób niepochodzących z UE, administratorzy danych nieposiadający powiązania z UE), w których na terytorium UE istnieje właściwa infrastruktura umożliwiająca przetwarzanie danych.

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. (Dz.U. L 281 z 23.11.1995, s. 31),

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

uwzględniając swój regulamin,

przyjmuje następującą opinię:

I. Wprowadzenie

Określenie prawa właściwego mającego zastosowanie w odniesieniu do przetwarzania danych osobowych na mocy dyrektywy 95/46/WE („dyrektywa" lub „dyrektywa 95/46) ma zasadnicze znaczenie z wielu powodów. Przepisy dotyczące prawa właściwego są kluczowe dla określenia zewnętrznego zakresu stosowania unijnych przepisów o ochronie danych, innymi słowy, dla określenia zakresu, w jakim unijne przepisy o ochronie danych mają zastosowanie w odniesieniu do przetwarzania danych osobowych, które w całości lub w części odbywa się poza terytorium UE/EOG, a mimo to jest istotnie powiązane z tym terytorium. Przepisy dotyczące prawa właściwego określają jednak również zakres przepisów o ochronie danych w obrębie UE/EOG, by zapobiegać ewentualnym konfliktom między przepisami poszczególnych państw członkowskich UE/EOG wdrażających dyrektywę oraz nakładaniu się tych przepisów na siebie[1].

Ponadto właściwe zrozumienie przepisów prawa właściwego powinno zagwarantować eliminację luk w zakresie ochrony danych osobowych na wysokim poziomie, jaki zapewnia dyrektywa 95/46.

Dyrektywa zawiera szereg reguł dotyczących kwestii prawa właściwego, w szczególności są to art. 4, 17 oraz 28. Reguły te określają, jakie przepisy prawa krajowego mają zastosowanie na mocy dyrektywy, a także jaki organ jest odpowiedzialny za ich egzekwowanie. Ważne jest aby pamiętać o interakcji zachodzącej między prawem materialnym a jurysdykcją. Kwestia ta zostanie poruszona szczegółowo nieco dalej.

Pojawiły się sugestie, że wdrożenie i interpretacja przepisów dyrektywy dotyczących prawa właściwego są w poszczególnych państwach Unii Europejskiej bardzo zróżnicowane. W pierwszym sprawozdaniu Komisji z wdrażania dyrektywy o ochronie danych podkreślono fakt, że wdrożenie art. 4 dyrektywy było „w wielu wypadkach niedoskonałe, i że mogło powodować powstanie kolizji praw, których uniknięciu omawiany artykuł służy"[2]. Zgodnie z załącznikiem technicznym do sprawozdania, w którym zawarto szczegółową analizę szeregu przepisów krajowych, przyczyną takiej niedoskonałej transpozycji może być po części stopień złożoności samych przepisów.

Podobne wnioski wyciągnięto w analizie zleconej przez Komisję Europejską[3]: podkreślono w niej dwuznaczność i rozbieżne wdrożenie przepisów dyrektywy dotyczących prawa właściwego i zwrócono uwagę, że „zdecydowanie potrzebne są lepsze, jaśniejsze i jednoznaczne przepisy w zakresie prawa właściwego".

W opublikowanym niedawno komunikacie Komisji „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej"[4] wspomniano, że „Komisja zbada, w

---

1 Dyrektywa 95/46/WE ma zastosowanie również do państw EFTA – Norwegii, Islandii oraz Liechtensteinu – na mocy porozumienia EOG (zob. decyzja Wspólnego Komitetu EOG nr 83/1999 z dnia 25 czerwca 1999 zmieniająca protokół 37 oraz załącznik XI (Usługi telekomunikacyjne) do Porozumienia EOG; Dz.U. L 296/41 z 23.11.2000).

2 Pierwsze sprawozdanie na temat wykonania dyrektywy o ochronie danych (95/46/WE), maj 2003, s. 17. Sprawozdanie dostępne na stronie: http://ec.europa.eu/justice/policies/privacy/lawreport/report_en.htm.

3 „Porównywalna analiza różnych sposobów realizacji nowych wyzwań związanych z polityką prywatności, w szczególności w świetle rozwoju technologii", styczeń 2010, dostępna na stronie: http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm.

4 COM(2010) 609 wersja ostateczna z 4.11.2010.

jaki sposób zrewidować i wyjaśnić obowiązujące przepisy o prawie właściwym, w tym obecne kryteria ustalania tego prawa, aby zwiększyć pewność prawną, wyjaśnić zakres odpowiedzialności państw członkowskich za stosowanie przepisów o ochronie danych oraz ostatecznie zapewnić unijnym osobom, których dane dotyczą, ten sam stopień ochrony, niezależnie od lokalizacji geograficznej administratora danych".

Stopień złożoności kwestii związanych z prawem właściwym rośnie także ze względu na nasilenie globalizacji oraz rozwój nowych technologii: przedsiębiorstwa coraz częściej i w coraz większym zakresie prowadzą działalność w obrębie różnych jurysdykcji, świadcząc usługi i udzielając wsparcia przez 24 godziny na dobę; Internet ułatwia świadczenie usług na odległość, a ponadto gromadzenie i udostępnianie danych osobowych w wirtualnym środowisku; wykorzystywanie chmur obliczeniowych utrudnia ustalenie miejsca przechowywania danych osobowych oraz środków, które wykorzystywane są o dowolnych porach.

Tym samym bardzo ważne jest, aby precyzyjne znaczenie tych przepisów dyrektywy, które dotyczą prawa właściwego, było dostatecznie jasne dla wszystkich zaangażowanych w realizację dyrektywy oraz w codzienne stosowanie krajowych przepisów o ochronie danych – zarówno w sektorze państwowym, jak i w prywatnym.

W związku z powyższym Grupa Robocza podjęła decyzję o przyczynieniu się do wyjaśnienia kilku kluczowych przepisów dyrektywy oraz do zajęcia się koncepcją prawa właściwego, tak jak zrobiła to już w odniesieniu do pojęcia danych osobowych oraz pojęcia „administratora danych" i „przetwarzającego"[5]. W niniejszej opinii Grupa Robocza odniesie się również do innych opinii, w których poruszała ona kwestię prawa właściwego, jeżeli kwestia ta będzie wiązać się z konkretnymi tematami, poruszanymi w tych opiniach[6].

Ostatecznym celem Grupy Roboczej jest doprowadzenie do sytuacji, w której istnieje pewność prawa w zakresie stosowania unijnych przepisów o ochronie danych. Z jednej strony implikuje to, że osoby, których dane dotyczą, będą wiedziały, które przepisy mają zastosowanie w odniesieniu do ochrony ich danych osobowych, zaś z drugiej strony – że przedsiębiorstwa, a także inne podmioty prywatne i państwowe będą wiedziały, które przepisy o ochronie danych odnoszą się do przetwarzania przez nie danych osobowych.

Wyjaśnienie pojęcia prawa właściwego ma ogromne znaczenie, niezależnie od ewentualnych zmian obowiązujących przepisów dyrektywy, które mogą zostać wprowadzone w przyszłości. Obowiązujące obecnie przepisy pozostaną w mocy do momentu zmiany, oraz w zakresie, w jakim nie zostaną zmienione. Wyjaśnienie przepisów prawa właściwego pomoże zatem zapewnić lepszą zgodność z dyrektywą w oczekiwaniu na ewentualne zmiany w prawodawstwie. Ponadto, przygotowując niniejszą opinię Grupa Robocza wyciągnęła wnioski z doświadczeń w stosowaniu obowiązujących

---

5 Opinia 4/2007 w sprawie pojęcia danych osobowych (WP 136); Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169). Wszystkie opinie są dostępne na stronie: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

6 Przede wszystkim Dokument roboczy w sprawie określenia międzynarodowego stosowania unijnych przepisów o ochronie danych w odniesieniu do przetwarzania danych osobowych w Internecie przez witryny zlokalizowane poza terytorium UE (WP 56), Opinia 10/2006 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Worldwide Interbank Financial Telecommunication, SWIFT) (WP 128) oraz Opinia 1/2008 dotycząca zagadnień ochrony danych związanych z wyszukiwarkami (WP 148).

obecnie przepisów w celu przygotowania wytycznych dla prawodawcy, które będą mogły stanowić wskazówkę podczas ewentualnych rewizji dyrektywy w przyszłości.

I wreszcie, przepisy określające prawo właściwe w odniesieniu do ochrony danych są zaprojektowane tak, aby regulować stosowanie dyrektywy w jej własnym zakresie, jak stanowi art. 3. W takiej formie często będą miały powiązanie z innymi obszarami prawa, nie wpływając na nie w stopniu wykraczającym poza zakres dyrektywy[7].

II. Uwagi ogólne i kwestie dotyczące polityki

II.1. Zarys historyczny: od Konwencji nr 108 do dyrektywy 95/46/WE

W 1981 r. autorzy Konwencji nr 108 sporządzonej pod auspicjami Rady Europy określili zagrożenia, jakie stwarzają konflikty prawne lub luki prawne powstałe w wyniku zastosowania odbiegających od siebie przepisów krajowych poszczególnych państw. Konwencja ta jednak nie zawierała konkretnych przepisów, które rozwiązywałyby powyższe problemy: za podstawową gwarancję tego, że nawet w przypadku istnienia różnych uregulowań prawnych, stosowane w efekcie zasady byłyby jednolite (co pomogłoby wyeliminować różnice w kontekście poziomu ochrony), uznano fakt, że Konwencja wprowadza „wspólną podstawę prawa materialnego".

Potrzebę wprowadzenia kryteriów umożliwiających określenie prawa właściwego uwzględniła Komisja Europejska na etapie przygotowywania dyrektywy w sprawie ochrony danych. W swoim pierwotnym wniosku[8] Komisja określiła, że nadrzędnym czynnikiem decydującym byłoby miejsce, w którym znajdują się dane, zaś czynnikiem drugorzędnym – w przypadku, gdy dane są zlokalizowane w państwie trzecim – miejsce zamieszkania/siedziba administratora danych.

W wyniku dyskusji w Parlamencie Europejskim oraz w Radzie UE nastąpiło odejście od kryterium miejsca, w którym znajdują się dane, na rzecz kryterium w postaci miejsca prowadzenia działalności gospodarczej przez administratora danych. Jako drugorzędne kryterium – w przypadku, gdy administrator danych nie prowadzi działalności gospodarczej na terytorium UE – przyjęto miejsce, w którym znajdują się środki.

Rada uzupełniła powyższe kryteria i przedstawiła dalsze wskazówki odnośnie do pojęcia działalności gospodarczej (ang. *establishment*). W uzupełnionym wniosku Komisji[9] wyszczególniono, że przetwarzanie powinno odbywać się „w

---

[7] Dyrektywa zawiera wprawdzie przepisy dotyczące odpowiedzialności (art. 23) oraz sankcji (art. 24), jednak pozostaje bez uszczerbku dla ogólnych zasad prawa cywilnego lub karnego, jak wspomniano w motywie 21 dyrektywy. Dyrektywa ma wpływ na te zasady jedynie w takim zakresie, w jakim niezbędne jest nałożenie sankcji w przypadku pogwałcenia zasad ochrony danych. Wdrażanie dyrektywy w poszczególnych krajach doprowadziło w praktyce do zastosowania różnych scenariuszy, spośród których niektóre przewidują sankcje karne, inne zaś ich nie przewidują. Kolejnym przykładem może być to, że dyrektywa zawiera wprawdzie przepisy dotyczące potrzebnej zgody – zob. art. 2 lit. h), art. 7 lit. a) oraz art. 8 ust. 1 lit a) – lub znaczenia zobowiązań umownych – zob. art. 7 lit. b) – nie ingeruje jednak w prawo zobowiązań (np. warunki zawarcia umowy, prawo właściwe) lub w inne aspekty prawa cywilnego w stopniu wykraczającym poza zawarte w niej przepisy.

[8] COM (1990) 314 - 2 z 18.7.1990 r., Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

[9] COM(1992) 422 wersja ostateczna z 15.10.1992.

kontekście prowadzenia działalności gospodarczej" przez administratora danych, oraz uwzględniono fakt, że administrator danych może prowadzić działalność gospodarczą w szeregu różnych państw członkowskich. Jedna z poważnych zmian polegała na tym, że głównym kryterium określającym prawo właściwe było nie to miejsce, w którym administrator danych ma swoją główną siedzibę, lecz miejsce, w którym administrator danych prowadzi (*jakąkolwiek*) działalność gospodarczą. Konsekwencje wypływające z powyższych zmian, związane z rozproszonym, nie zaś jednolitym stosowaniem przepisów różnych krajów w przypadku działalności gospodarczej prowadzonej w wielu krajach, zostaną rozwinięte poniżej.

II.2. Znaczenie koncepcji

II.2.a) Kontekst i znaczenie strategiczne

Określenie sposobu stosowania przepisów UE w odniesieniu do przetwarzania danych osobowych służy, jak wspomniano już wcześniej, wyjaśnieniu zakresu stosowania unijnych przepisów o ochronie danych zarówno na terytorium UE/EOG jak i w szerszym kontekście międzynarodowym. Jasne zrozumienie prawa właściwego pomoże w zagwarantowaniu administratorom danych pewności prawa, zaś osobom fizycznym oraz innym zainteresowanym podmiotom – w ustaleniu wyraźnych ram.

Określenie prawa właściwego jest ściśle powiązane z określeniem administratora danych [10] i jego działalności gospodarczej (jednej lub wielu): najważniejszą konsekwencją tego powiązania jest potwierdzenie obowiązków administratora danych oraz – w przypadku, gdy administrator danych prowadzi działalność w państwie trzecim – jego przedstawicieli.

Jak wyjaśnimy w dalszym ciągu opinii, nie oznacza to, że zawsze będziemy mieli do czynienia z jednym prawem właściwym, zwłaszcza jeżeli administrator danych prowadzi działalność gospodarczą w kilku państwach: decydujące będzie również miejsce, w którym znajduje się dana działalność gospodarcza oraz charakter prowadzonych przez nią działań. Jednak wyraźne powiązanie między prawem właściwym a administratorem danych może być gwarancją skuteczności i wykonalności, zwłaszcza w sytuacji, gdy ustalenie miejsca, w którym znajduje się zbiór danych, okazuje się trudne lub czasami wręcz niemożliwe (jak może zdarzać się w przypadku wykorzystywania chmur obliczeniowych).

W rozwiązywaniu problemów związanych z nowymi tendencjami – czy to technologicznymi (Internet, zbiory danych dostępne w sieci/wykorzystywanie chmur obliczeniowych) czy to gospodarczymi (spółki wielonarodowe) – pomocne byłyby wyraźne wytyczne dotyczące zasad związanych z prawem właściwym.

II.2.b) Zakres prawa unijnego oraz prawa krajowego na terytorium UE/EOG

Głównym kryterium dla określenia prawa właściwego jest miejsce prowadzenia działalności przez administratora danych oraz – w przypadku, gdy działalność administratora danych jest zarejestrowana poza terytorium EOG – miejsce, w

[10] Zobacz Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169);

którym znajdują się wykorzystywane przez niego środki lub wyposażenie[11]. Oznacza to, że decydujące nie jest tutaj ani obywatelstwo czy też miejsce zwykłego pobytu osób, których dane dotyczą, ani miejsce, w którym fizycznie znajdują się dane osobowe[12].

Powoduje to szeroki zakres zastosowania, zaś następstwa prawne wykraczają poza terytorium EOG: dyrektywa – oraz krajowe przepisy wdrażające – mają zastosowanie w odniesieniu do przetwarzania danych osobowych poza terytorium EOG (realizowanego w kontekście działalności gospodarczej administratora danych na terytorium EOG), a także w odniesieniu do administratorów danych prowadzących działalność gospodarczą poza terytorium EOG (gdy korzystają ze środków na terytorium EOG). W konsekwencji przepisy dyrektywy mogą mieć zastosowanie do usług o wymiarze międzynarodowym, takich jak usługi wyszukiwarek, serwisów społecznościowych oraz związane z wykorzystywaniem chmur obliczeniowych). Przykłady rozwinięto poniżej.

Jeżeli dane osobowe są przetwarzane przez administratora danych (X), którego jedyna działalność gospodarcza prowadzona jest w państwie członkowskim A, prawem właściwym w odniesieniu do przetwarzania danych – niezależnie od tego, gdzie jest ono realizowane – będzie prawo krajowe państwa członkowskiego A.

Jeżeli X ma również działalność gospodarczą (Y) w państwie członkowskim B, krajowym prawem właściwym dla przetwarzania realizowanego przez Y będzie prawo krajowe państwa członkowskiego B, pod warunkiem, że przetwarzanie realizowane jest w kontekście działalności Y. Jeżeli przetwarzanie jest realizowane przez Y w kontekście działalności gospodarczej X w państwie członkowskim A, prawem właściwym dla przetwarzania będzie prawo państwa członkowskiego A.

Jeżeli dane osobowe są przetwarzane przez administratora danych, który nie prowadzi działalności gospodarczej w żadnym z państw członkowskich, przetwarzanie będzie objęte zakresem prawa krajowego danego państwa członkowskiego, w którym znajduje się wyposażenie (lub środki) wykorzystywane przez administratora danych w celu przetwarzania danych. Przykłady tych różnych sytuacji będą rozpatrywane w dalszej części niniejszej opinii.

Celem przyjęcia takiego szerokiego zakresu stosowania jest w pierwszym rzędzie dopilnowanie, aby osoby fizyczne nie zostały pozbawione ochrony, do której mają prawo na mocy dyrektywy, oraz jednoczesne zapobieganie przypadkom obchodzenia prawa.

W dyrektywie znajdują się kryteria decydujące o odpowiedzi na oba podane poniżej pytania:

---

[11] Jak wyjaśniono w pkt III.2.b poniżej, pojęcie „wyposażenia" zostało przetłumaczone na inne języki UE za pośrednictwem pojęcia „środki". Dzięki temu możliwa jest szeroka interpretacja pojęcia wyposażenia; jest to jednocześnie wyjaśnieniem, dlaczego w niniejszym dokumencie stosuje się oba pojęcia.

[12] Zobacz podobne rozwiązanie w Dyrektywie 2000/31/WE w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego. Dodatkowym istotnym czynnikiem jest – w odniesieniu do prawa właściwego dla środków bezpieczeństwa (art. 17) – miejsce, w którym znajduje się przetwarzający. Jednak kryterium to nie jest samo w sobie decydujące i musi być stosowane w związku z głównym kryterium, którym jest działalność gospodarcza administratora danych.

(i) czy w odniesieniu do konkretnej działalności związanej z przetwarzaniem danych osobowych zastosowanie ma prawo europejskie – czy to łącznie z prawem państwa trzeciego czy też nie; oraz
(ii) prawo krajowe którego państwa członkowskiego ma zastosowanie do przetwarzania w przypadku, gdy do przetwarzania stosuje się prawo europejskie.

Należy również zwrócić uwagę, że niektóre działania związane z przetwarzaniem na terytorium UE nie są objęte zakresem stosowania dyrektywy, jednak mogą spowodować zastosowanie innych aktów prawnych UE, takich jak decyzja ramowa 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[13] czy też rozporządzenie 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe[14], bądź innych aktów dotyczących konkretnych organów lub systemów informatycznych UE (np. Europol, Eurojust, SIS, CIS itd.)[15].

II.2.c) Unikanie luk i zbędnego nakładania się przepisów

Celem stworzenia wyraźnych kryteriów umożliwiających określenie prawa właściwego jest zapobieganie przypadkom obchodzenia przepisów prawa krajowego państw członkowskich jak i nakładania się na siebie tych przepisów. To, czy w odniesieniu do przetwarzania danych zastosowanie będą miały przepisy jednego czy też kilku państw, będzie uzależnione od tego, czy administrator prowadzi działalność gospodarczą w jednym czy w kilku państwach oraz jaki jest charakter działań realizowanych przez daną działalanność gospodarczą:

- Jeżeli administrator danych prowadzi jedną działalność gospodarczą, obowiązywać będzie jedno prawo na całym terytorium UE/EOG, w zależności od miejsca, w którym znajduje się ta działalność[16].

- Jeżeli działalność gospodarcza prowadzona jest w kilku państwach: stosowanie przepisów prawa krajowego będzie uzależnione od działań realizowanych przez daną działalność gospodarczą.

Zastosowanie kryteriów ma zapobiec jednoczesnemu stosowaniu w odniesieniu do tej samej działalności przetwarzającego przepisów prawa krajowego kilku państw.

II.2.d) Prawo właściwe i jurysdykcja w kontekście dyrektywy

W obszarze ochrony danych szczególnie istotne jest odróżnienie pojęcia *prawa właściwego* (które określa system prawny mający zastosowanie w danym przypadku) od pojęcia *jurysdykcji* (które zazwyczaj określa zdolność sądu krajowego do rozstrzygnięcia

[13] Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. L 350 z 30.12.2008, s. 60).

[14] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

[15] Europol: Decyzja Rady 2009/371/WSiSW, Dz.U. L 121 z 15.5.2009, s. 37); Eurojust: Decyzja Rady 2002/187/WSiSW, Dz.U. L 63 z 6.3.2002, s. 1, zmieniona decyzją Rady 2009/426/WSiSW, Dz.U. L 138 z 4.6.2009, s. 14.

[16] Zgodnie z art. 17 ust. 3 dyrektywy wyjątek dotyczy środków bezpieczeństwa, w przypadku których prawo właściwe będzie uzależnione od miejsca, w którym znajduje się ewentualny przetwarzający.

sprawy bądź wykonania wyroku lub postanowienia). Prawo właściwe oraz jurysdykcja w odniesieniu do jakiegokolwiek przetwarzającego nie zawsze muszą być takie same.

Zewnętrzny zakres stosowania prawa UE jest wyrazem możliwości stanowienia przez UE przepisów w celu ochrony podstawowych interesów na terytorium jej jurysdykcji. Przepisy dyrektywy określają również zakres stosowania przepisów prawa krajowego poszczególnych państw członkowskich, lecz pozostają bez uszczerbku dla jurysdykcji krajowych sądów odnośnie do rozstrzygania przez nie właściwych spraw. Przepisy dyrektywy odwołują się jednak do zakresu terytorialnego kompetencji organów nadzorczych, które mogą stosować i egzekwować prawo właściwe.

Wprawdzie w większości przypadków oba te czynniki – prawo właściwe kompetencje organów nadzorczych – mają tendencję do występowania jednocześnie, co zazwyczaj prowadzi do zastosowania prawa państwa członkowskiego A przez organy państwa członkowskiego A, jednak w dyrektywie wyraźnie przewidziano możliwość innych ustaleń. Artykuł 28 ust. 6 stanowi, że krajowe organy ds. ochrony danych powinny być w stanie wykonywać swoje uprawnienia w sytuacji, gdy w odniesieniu do przetwarzania danych osobowych realizowanego w obrębie ich jurysdykcji zastosowanie ma prawo o ochronie danych innego państwa członkowskiego. Praktyczne skutki tej kwestii zostaną bliżej rozpatrzone w jednej z przyszłych opinii Grupy Roboczej.

W konsekwencji powyższych sytuacji pojawia się konieczność transgranicznego rozpatrywania spraw; sytuacje te uwydatniają także potrzebę współpracy organów ds. ochrony danych, z uwzględnieniem uprawnień wykonawczych poszczególnych zaangażowanych organów ds. ochrony danych. Obrazują one również potrzebę właściwego wdrożenia odpowiednich przepisów dyrektywy w prawie krajowym, ponieważ może być to decydujące dla skutecznej współpracy transgranicznej i wykonania przepisów.

III. Analiza przepisów

Kluczowym przepisem dotyczącym prawa właściwego jest art. 4 określający, które przepisy prawa krajowego przyjęte na mocy dyrektywy mogą być stosowane w odniesieniu do przetwarzania danych osobowych.

III.1. Administrator danych prowadzi działalność w jednym lub w kilku państwach członkowskich (art. 4 ust. 1 lit. a)

Pierwsza sytuacja, której dotyczy art. 4 ust. 1, zakłada, że administrator danych prowadzi jedną lub więcej działalności gospodarczych na terytorium UE. W takim przypadku art. 4 ust. 1 stanowi, że państwo członkowskie powinno zastosować krajowe przepisy o ochronie danych gdy „[...] przetwarzanie danych odbywa się w kontekście prowadzenia przez administratora danych działalności gospodarczej na terytorium Państwa Członkowskiego; jeżeli ten sam administrator danych prowadzi działalność gospodarczą na terytorium kilku Państw Członkowskich, musi on podjąć niezbędne działania, aby zapewnić, że każde z tych przedsiębiorstw wywiązuje się z obowiązków przewidzianych w odpowiednich przepisach prawa krajowego".

Warto przypomnieć, że pojęcie „administratora danych" zostało zdefiniowane w art. 2 lit. d) dyrektywy. Pojęcie to nie będzie analizowane w niniejszej opinii, jako że zostało już

wyjaśnione przez Grupę Roboczą ds. Ochrony Danych powołaną na mocy art. 29 w jej Opinii w sprawie pojęć „administrator danych" i „przetwarzający"[17].

Ponadto ważne jest podkreślenie, iż działalność gospodarcza nie musi mieć osobowości prawnej, a także iż pojęcie działalności gospodarczej ma elastyczne powiązania z pojęciem administracji. Administrator danych może prowadzić działalność gospodarczą w szeregu państw, kilku administratorów danych może skupić swoje wspólne działania w obrębie jednej lub kilku działalności gospodarczych. Decydującym elementem służącym zakwalifikowaniu działalności gospodarczej na mocy dyrektywy jest efektywne i rzeczywiste prowadzenie działań w kontekście, w którym przetwarzane są dane osobowe.

a) „…prowadzenia przez administratora danych działalności gospodarczej na terytorium Państwa Członkowskiego…"

Pojęcie działalności gospodarczej nie zostało zdefiniowane w dyrektywie. Jednak w preambule dyrektywy wskazano, że „prowadzenie działalności gospodarczej na terytorium Państwa Członkowskiego zakłada efektywne i rzeczywiste prowadzenie działań poprzez stabilne rozwiązania (oraz że) forma prawna (…) działalności gospodarczej, niezależnie czy jest to oddział lub filia posiadająca osobowość prawną, nie jest w tym względzie czynnikiem decydującym" *(motyw 19)*.

Jeżeli chodzi o swobodę przedsiębiorczości, zapewnioną w art. 50 TFUE (dawny art. 43 TWE), Trybunał Sprawiedliwości uznał, że stabilna działalność gospodarcza wymaga, by „zarówno ludzkie jak i techniczne zasoby niezbędne dla realizacji określonych usług były nieustannie dostępne". [18]

Silny nacisk, jak położono w preambule dyrektywy na „efektywne i rzeczywiste prowadzenie działań poprzez stabilne rozwiązania" jest wyraźnym odzwierciedleniem „stabilnej działalności gospodarczej", do której odwoływał się Trybunał Sprawiedliwości w momencie przyjmowania dyrektywy. Wprawdzie nie jest jasne, czy ta oraz kolejne interpretacje Trybunału Sprawiedliwości dotyczące swobody przedsiębiorczości na mocy art. 50 TFUE mogłyby zostać w pełni zastosowane w odniesieniu do sytuacji objętych art. 4 dyrektywy o ochronie danych, jednak interpretacja Trybunału w może w takich sytuacjach dostarczyć przydatnych wskazówek na etapie analizowania treści dyrektywy.

Interpretacja ta została wykorzystana w następujących przykładach:

- Jeżeli mamy do czynienia z „efektywnym i rzeczywistym prowadzeniem działań", na przykład przez kancelarię prawną, w oparciu o „stabilne rozwiązania", kancelaria zostałaby zakwalifikowana jako działalność gospodarcza.

---

17 Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169).

18 Wyrok Trybunału Sprawiedliwości z dnia 4 lipca 1985 r., *Bergholz* (sprawa 168/84, Rec. [1985] s. 2251, pkt 14) oraz wyrok z dnia 7 maja 1998 r., *Lease Plan Luxembourg / Belgische Staat* (C-390/96, Rec. [1998] s. I-2553). W tej ostatniej sprawie kwestią kluczową było określenie, czy serwer przedsiębiorstwa, znajdujący się w innym państwie niż państwo strony świadczącej usługi, może zostać uznany za stabilną działalność gospodarczą. Celem było ustalenie, w którym państwie powinien zostać opłacony podatek VAT. Sędzia odmówił uznania środków komputerowych za przedsiębiorstwo wirtualne (powracając przy tej interpretacji do bardziej „klasycznego" pojęcia „działalności gospodarczej", w odróżnieniu od pojęcia przyjętego w pierwszym wyroku z dnia 17 lipca 1997 r. *ARO Lease / Inspecteur der Belastingdienst Grote Ondernemingen te Amsterdam* (C-190/95, Rec. 1997 s. I-4383)).

- Serwer lub komputer prawdopodobnie nie zostanie zakwalifikowany jako działalność gospodarcza, ponieważ jest to jedynie urządzenie techniczne lub instrument służący przetwarzaniu informacji[19].

- Jednoosobowe biuro kwalifikowałoby się tak długo, jak długo jego działania obejmują więcej niż jedynie reprezentowanie administratora danych prowadzącego działalność gospodarczą gdzie indziej, i jak długo jest ono aktywnie zaangażowane w działania w kontekście, w którym odbywa się przetwarzanie danych osobowych.

- W każdym razie, forma organizacji biura nie jest decydująca: za istotną działalność gospodarczą może zostać uznany nawet zwykły przedstawiciel, jeżeli jego obecność w danym państwie członkowskim wykazuje wystarczającą stabilność.

Przykład nr 1: publikacje dla podróżujących

Spółka prowadząca działalność w państwie członkowskim A gromadzi – w celu przygotowania publikacji dla podróżnych – dane dotyczące usług realizowanych przez stacje benzynowe w państwie członkowskim B. Dane gromadzone są przez pracownika, który podróżuje po terytorium państwa B, gromadzi zdjęcia i przesyła je wraz z uwagami do swojego pracodawcy na terenie państwa A. W tym przypadku dane gromadzone są na terytorium państwa B (przy czym „działalność gospodarcza" w tym państwie nie istnieje) i przetwarzane są w kontekście działań prowadzonych przez spółkę w państwie A: prawem właściwym jest prawo państwa A.

W art. 4 ust. 1 lit. a), w którym jest odniesienie do (*jakiejkolwiek*) działalności gospodarczej *administratora danych* na terytorium *państwa członkowskiego*, poruszona jest kwestia – inna niż pojęcie działalności gospodarczej – która wymaga wyjaśnienia.

Przede wszystkim odniesienie do (*jakiejkolwiek*) działalności gospodarczej oznacza, że zastosowanie przepisów prawa danego państwa członkowskiego będzie uzależnione od miejsca prowadzenia przez administratora danych działalności gospodarczej w tym państwie członkowskim, zaś przepisy innych państw członkowskich mogą zostać zastosowane w związku z miejscem, w którym prowadzona jest inna działalność gospodarcza przedmiotowego administratora danych w tych państwach członkowskich.

Nawet wówczas gdy miejsce głównej działalności gospodarczej administratora danych znajduje się w państwie trzecim, sam fakt posiadania działalności gospodarczej w jednym z państw członkowskich mógłby spowodować zastosowanie prawa tego państwa, pod warunkiem spełnienia pozostałych założeń art. 4 ust. 1 lit. a) (zob. poniżej lit. b). Potwierdza to również druga część przepisu, w której wyraźnie przewidziano, że jeżeli ten sam administrator danych prowadzi działalność gospodarczą na terytorium kilku państw członkowskich, powinien dopilnować, aby każda działalność gospodarcza prowadzona była zgodnie z odnośnym prawem właściwym.

> b) „…przetwarzanie danych odbywa się w kontekście prowadzenia (…) działalności gospodarczej…"

Dyrektywa wiąże możliwość stosowania prawa o ochronie danych danego państwa członkowskiego z przetwarzaniem danych osobowych. Pojęcie „przetwarzania" zostało

[19] W dalszym ciągu opinii dyskusji poddana zostanie kwestia, czy można go zakwalifikować inaczej – np. jako „środki".

już kilkakrotnie podjęte przez Grupę Roboczą przy okazji sporządzania innych opinii, w których podkreślono, że różne operacje lub szereg operacji na danych osobowych może być realizowany jednocześnie lub na różnych etapach[20]. W kontekście określania prawa właściwego może to oznaczać, że różne prawo właściwe może być uruchomione na różnych etapach przetwarzania danych osobowych.

Mnożenie prawa właściwego stanowi zatem poważne zagrożenie, należy zatem zastanowić się nad możliwością alternatywną, gdy powiązanie między różnymi operacjami przetwarzania na poziomie makro mogłoby prowadzić do zastosowania jednego prawa krajowego. W celu ustalenia, czy w odniesieniu do poszczególnych etapów przetwarzania zastosowanie ma jedno czy kilka praw, istotne jest pamiętanie o łącznym obrazie działań związanych z przetwarzaniem: w odniesieniu do zestawu operacji przeprowadzanych w szeregu różnych państw członkowskich, spośród których wszystkie mają służyć jednemu celowi, może być zastosowane jedno prawo krajowe.

W takich okolicznościach czynnikiem determinującym określenie prawa właściwego jest pojęcie „kontekstu działalności gospodarczej", nie zaś miejsca, w którym znajdują się dane.

Pojęcie „kontekstu działalności gospodarczej" nie implikuje, że prawem właściwym jest prawo państwa członkowskiego, w którym *administrator danych* prowadzi działalność gospodarczą, lecz w którym *działalność gospodarcza* administratora danych jest zaangażowana w *działania* związane z przetwarzaniem danych.

Rozważenie różnych scenariuszy może być pomocne w wyjaśnieniu, co dokładnie kryje się pod pojęciem „kontekstu działalności gospodarczej" oraz jego wpływu na określenie prawa właściwego dla różnych działań związanych z przetwarzaniem prowadzonych w szeregu różnych państw.

a. Jeżeli administrator danych prowadzi działalność gospodarczą w Austrii i przetwarza dane osobowe w Austrii w kontekście działań wykonywanych przez wspomnianą działalność gospodarczą, prawem właściwym byłoby oczywiście prawo Austrii – to znaczy państwa, w którym znajduje się działalność gospodarcza.

b. W drugim scenariuszu administrator danych prowadzi działalność gospodarczą w Austrii i przetwarza w kontekście działań tej działalności dane osobowe gromadzone za pośrednictwem jej strony internetowej. Strona internetowa jest dostępna dla użytkowników w różnych państwach. Prawem właściwym regulującym kwestie ochrony danych w dalszym ciągu będzie prawo Austrii, to znaczy państwa, w którym znajduje się działalność gospodarcza – niezależnie od tego, gdzie znajdują się użytkownicy danych.

c. W trzecim scenariuszu administrator danych prowadzi działalność gospodarczą w Austrii i zleca przetwarzanie danych przetwarzającemu na terytorium Niemiec. Przetwarzanie w Niemczech odbywa się w kontekście działań administratora danych w Austrii. Oznacza to, że przetwarzanie danych wykonywane jest w celach związanych z działaniami przedsiębiorstwa w Austrii oraz zgodnie z jego wytycznymi. W odniesieniu do przetwarzania realizowanego przez przetwarzającego w Niemczech zastosowanie będzie miało prawo Austrii. Ponadto przetwarzający

[20] Zobacz np. Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169).

będzie związany wymogami prawa niemieckiego w odniesieniu do środków bezpieczeństwa, które jest zobowiązany uruchomić w związku z przetwarzaniem[21]. Takie ustalenia wymagałyby skoordynowanego nadzoru niemieckich i austriackich organów ds. ochrony danych.

d. W czwartym scenariuszu administrator danych prowadzący działalność w Austrii otwiera biuro przedstawicielskie we Włoszech, które organizuje włoską część strony internetowej i zajmuje się wnioskami składanymi przez włoskich użytkowników. Działania związane z przetwarzaniem danych i wykonywane przez włoskie biuro są realizowane w kontekście włoskiej działalności gospodarczej, a zatem do działań tych zastosowanie miałoby prawo włoskie.

Wnioski dotyczące prawa właściwego mogą być wyciągnięte jedynie w oparciu o precyzyjne zrozumienie pojęcia „w kontekście działalności gospodarczej". W celu przeprowadzenia analizy należy wziąć pod uwagę następujące rozważania:

Kluczowy jest stopień zaangażowania działalności gospodarczej w działania, w kontekście których przetwarzane są dane osobowe. Kwestią, którą należy tutaj sprawdzić, jest to „kto czym się zajmuje", a zatem które działania są wykonywane przez którą działalność gospodarczą; dzięki temu możliwe jest określenie, czy działalność gospodarcza ma znaczenie dla zastosowania krajowych przepisów o ochronie danych. Jeżeli w działalności gospodarczej dane osobowe przetwarzane są w kontekście własnych działań, prawem właściwym będzie prawo państwa członkowskiego, w którym siedzibę ma dana działalność gospodarcza. Jeżeli w działalności gospodarczej dane osobowe przetwarzane są w kontekście działań innej działalności gospodarczej, prawem właściwym będzie prawo państwa członkowskiego, w którym siedzibę ma inna działalność gospodarcza.

Charakter działań działalności gospodarczej jest elementem drugorzędnym, jednak pomoże w określeniu prawa właściwego dla danej działalności gospodarczej: to, czy działania wiążą się z przetwarzaniem danych czy nie, oraz czyje przetwarzanie ma miejsce w kontekście czyjej działalności, zależy w dużej mierze od charakteru tych działań. Fakt, że różne działalności gospodarcze mogą być zaangażowane w całkowicie różne działania, w kontekście których dane osobowe są przetwarzane, będzie miał alternatywnie wpływ na prawo właściwe. Rozważania te zilustrowano w przykładzie nr 4.

Należy pod uwagę wziąć również ogólny cel dyrektywy, jako że celem jej jest zagwarantowanie skutecznej ochrony osobom fizycznym – w prosty, możliwy do zrealizowania i przewidywalny sposób.

[21] Zgodnie z art. 17 ust. 3 dyrektywy 95/46/WE przetwarzający jest związany wymogami zdefiniowanymi w odniesieniu do środków bezpieczeństwa przez przepisy państwa członkowskiego, w którym przetwarzający prowadzi działalność. W przypadku konfliktu między przedmiotowymi wymogami w odniesieniu do środków bezpieczeństwa, obowiązuje *lex loci* (prawo przetwarzającego). Ostateczna odpowiedzialność pozostaje po stronie administratora danych, przetwarzający musi udowodnić, że podjął wszystkie niezbędne kroki zgodnie z jego umową z przetwarzającym, jak również obowiązki związane z bezpieczeństwem zgodnie z definicją prawa państwa członkowskiego, w którym przetwarzający prowadzi działalność (zob. więcej w pkt III.5).

Przykład nr 2: Transfer danych osobowych w związku z faktoringiem

Włoskie przedsiębiorstwo użyteczności publicznej przekazuje informacje o swoich dłużnikach do francuskiego banku inwestycyjnego. Celem transferu jest faktoring wierzytelności. Wierzytelności powstały w wyniku nieopłaconych rachunków za energię elektryczną. Przekazanie informacji o wierzytelnościach wiąże się z transferem danych osobowych klientów do francuskiego banku inwestycyjnego, a konkretnie do jego oddziału we Włoszech (to znaczy jest to działalność gospodarcza francuskiego banku prowadzona we Włoszech).

Francuski bank inwestycyjny jest administratorem danych w odniesieniu do operacji przetwarzania, którą stanowi transfer, a jego włoski oddział realizuje zarządzanie wierzytelnościami oraz pobieranie ich w jego imieniu. Dane są przetwarzane zarówno przez administratora danych we Francji jak i w oddziale we Włoszech. Francuski administrator danych dostarcza wszystkim włoskim klientom informacje o powyższych operacjach za pośrednictwem oddziału we Włoszech.

Oddział we Włoszech stanowi dla celów niniejszej dyrektywy działalność gospodarczą, a jego działania obejmujące przetwarzanie danych osobowych w celu informowania klientów o ustaleniach muszą być zgodne z włoskimi przepisami o ochronie danych. Środki bezpieczeństwa stosowane w ramach włoskiego oddziału również będą musiały być zgodne z warunkami określonymi we włoskim ustawodawstwa regulującego kwestie ochrony danych, podczas gdy francuski administrator danych będzie musiał zachować jednocześnie zgodność z francuskimi wymogami w zakresie bezpieczeństwa dotyczącymi danych przetwarzanych w ramach jego działalności gospodarczej na terytorium Francji. Osoby, których dane dotyczą, tzn. wierzyciele, mogą zwracać się do biura włoskiego oddziału, aby na mocy prawa włoskiego korzystać ze swoich praw związanych z ochroną danych, takich jak dostęp, sprostowanie oraz usunięcie.

W analizie tych kryteriów należy przyjąć podejście funkcjonalne: czynnikami, które powinny być czynnikami determinującymi, powinny być raczej postępowanie stron w praktyce i interakcje między stronami, nie zaś teoretyczna ewaluacja dokonana przez strony w zakresie prawa właściwego: jaka jest rzeczywista rola poszczególnych przedsiębiorstw, jakie działania mają miejsce w kontekście której działalności gospodarczej?

Należy zwrócić uwagę na stopień zaangażowania każdej z działalności gospodarczych, w odniesieniu do działań, w kontekście których przetwarzane są dane osobowe. W złożonych przypadkach przydatne jest również zrozumienie pojęcia „w kontekście", które umożliwia rozdzielenie różnych działań realizowanych przez podmioty prowadzące działalność gospodarczą w różnych państwach UE w ramach jednego przedsiębiorstwa.

Przykład nr 3: Gromadzenie danych klientów przez sklepy

Sieć sklepów „prêt à porter" ma swoją główną siedzibę w Hiszpanii, zaś sklepy znajdują się w różnych państwach UE. Gromadzenie danych dotyczących klientów odbywa się w każdym sklepie, jednak dane te są przekazywane do siedziby głównej w Hiszpanii, gdzie mają miejsce określone działania związane z przetwarzaniem danych osobowych (analiza profilu klientów, usługi na rzecz klientów, tzw. targetowanie).

Działania takie jak marketing bezpośredni ukierunkowany na klientów w całej Europie, jest realizowany wyłącznie przez siedzibę główną w Hiszpanii. Działania tego typu można byłoby zakwalifikować jako odbywające się w kontekście działania działalności gospodarczej w Hiszpanii. Zastosowanie w odniesieniu do powyższych działań związanych z przetwarzaniem miałyby zatem przepisy Hiszpanii.

Jednak za poszczególne aspekty związane z przetwarzaniem danych osobowych klientów, które odbywa się w kontekście działań sklepu (na przykład gromadzenie danych osobowych klientów) odpowiedzialne są poszczególne sklepy. W zakresie, w jakim przetwarzanie jest realizowane w kontekście działań poszczególnych sklepów, przetwarzanie to jest objęte przepisami państwa, w którym znajduje się dany sklep.

Bezpośrednią konsekwencją praktyczną tej analizy jest fakt, że każdy sklep musi podjąć niezbędne kroki, aby zgodnie z obowiązującymi w jego kraju przepisami poinformować osoby fizyczne o warunkach gromadzenia i dalszego przetwarzania ich danych.

W przypadku skargi klienci mogą zwrócić się bezpośrednio do organu ds. ochrony danych w ich kraju. Jeżeli skarga związana jest z działaniami polegającymi na marketingu bezpośrednim w kontekście działań siedziby głównej w Hiszpanii, lokalny organ ds. ochrony danych przekazuje sprawę do hiszpańskiego organu ds. ochrony danych.

Tym samym możliwe jest, że jedna działalność gospodarcza będzie zaangażowana w szereg różnych rodzajów działań, oraz że przepisy prawa krajowego różnych państw będą miały zastosowanie w odniesieniu do przetwarzania danych w kontekście tych różnych działań. W celu zapewnienia przewidywalnego i możliwego do zrealizowania podejścia w sytuacji, w której w odniesieniu do różnych działań realizowanych w ramach jednej działalności gospodarczej mogą mieć zastosowanie przepisy różnych krajów, należy zastosować podejście funkcjonalne, w tym rozważenie obszerniejszego kontekstu prawnego.

Przykład nr 4: Scentralizowana baza danych o zasobach ludzkich

W praktyce coraz częściej zdarzają się sytuacje, w których ta sama baza danych może być przedmiotem prawa właściwego różnych państw. Często dzieje się tak w sektorze zasobów ludzkich, gdy jednostki zależne/jednostki działalności gospodarczej prowadzone w różnych krajach skupiają dane pracowników centralnie – w jednej bazie danych. Zazwyczaj dzieje się tak z powodów związanych z korzyściami skali, jednak nie powinno mieć to wpływu na odpowiedzialność poszczególnych podmiotów wynikającą z prawa lokalnego. Jest to aktualne nie tylko w perspektywie ochrony danych, ale również w kontekście prawa pracy i przepisów porządku publicznego.

Jeżeli na przykład dane pracowników zatrudnionych w irlandzkiej jednostce zależnej (która kwalifikuje się jako działalność gospodarcza) zostały przekazane do scentralizowanej bazy danych w Zjednoczonym Królestwie, gdzie przechowywane są również dane pracowników jednostki zależnej/działalności gospodarczej z siedzibą w Zjednoczonym Królestwie, zastosowanie miałyby dwa różne reżimy prawne w zakresie ochrony danych (prawo Irlandii i Zjednoczonego Królestwa).

Zastosowanie przepisów dwóch różnych państw nie wynika z prostego faktu, że dane pochodzą z dwóch różnych państw członkowskich, lecz tego, że przetwarzanie danych pracowników irlandzkich przez przedsiębiorstwo w Zjednoczonym Królestwie odbywa się w kontekście działań realizowanych przez irlandzką działalność gospodarczą w jej roli pracodawcy.

Powyższy przykład ilustruje fakt, że to nie miejsce, do którego dane są przesyłane, czy też w którym się znajdują, jest decydujące dla zastosowania przepisów określonego państwa; kluczowym czynnikiem jest charakter i miejsce normalnych działań określających „kontekst", w którym jest realizowane przetwarzanie: tym samym zasoby ludzkie lub dane dotyczące klientów są zazwyczaj przedmiotem prawa regulującego ochronę danych w państwie, w którym mają miejsce działania, w kontekście których przetwarzane są dane. Jest to również potwierdzeniem faktu, że nie ma bezpośredniej korelacji między właściwym prawem krajowym a jurysdykcją, jako że prawo krajowe może mieć zastosowanie poza obszarem jurysdykcji krajowej.

Podsumowując, kryteria wykorzystane do określenia prawa właściwego mogą mieć znaczenie na różnych płaszczyznach:

- Po pierwsze, pomagają w określeniu, czy unijne przepisy o ochronie danych w ogóle mają zastosowanie w odniesieniu do przetwarzania danych;

- Po drugie, w przypadku gdy zastosowanie mają unijne przepisy o ochronie danych, kryteria będą decydujące dla określenia:
  a) przepisy o ochronie danych którego państwa członkowskiego mają zastosowanie, oraz
  b) przepisy o ochronie danych którego państwa członkowskiego będą miały zastosowanie do której czynności przetwarzania danych w przypadku, gdy mamy do czynienia z wieloma podmiotami prowadzącymi działalność gospodarczą w różnych państwach członkowskich;

- Po trzecie, kryteria będą pomocne w sytuacji, gdy w związku z przetwarzaniem pojawi się wymiar pozaeuropejski, jak w przypadku poniższego przykładu, w którym administrator danych prowadzi działalność poza terytorium EOG.

Przykład nr 5: Dostawca usług internetowych

Dostawca usług internetowych (administrator danych) ma swoją siedzibę poza terytorium UE, np. w Japonii. W większości państw członkowskich UE prowadzi on biura handlowe, ma także biuro w Irlandii, które zajmuje się kwestiami związanymi z przetwarzaniem danych osobowych, w tym przede wszystkim wsparciem informatycznym. Administrator danych otwiera centrum danych na Węgrzech, gdzie zatrudni ludzi i umieści serwery przeznaczone do przetwarzania i przechowywania danych dotyczących osób korzystających z usług przedsiębiorstwa.

Administrator danych w Japonii posiada również inne przedsiębiorstwa w różnych państwach członkowskich, które prowadzą działalność różnego rodzaju:

- centrum danych na Węgrzech prowadzi jedynie obsługę techniczną;

- biura handlowe dostawcy usług internetowych organizują ogólne kampanie reklamowe;

- biuro w Irlandii jest jedynym przedsiębiorstwem na terenie UE prowadzącym działania, w kontekście których dane osobowe są faktycznie przetwarzane (bez uwzględnienia danych napływających z siedziby głównej w Japonii).

Działania prowadzone przez biuro w Irlandii powodują zastosowanie unijnych przepisów o ochronie danych: dane osobowe są przetwarzane w kontekście działalności biura w Irlandii, a zatem takie przetwarzanie jest przedmiotem unijnych przepisów o ochronie danych.

Prawo właściwe dla przetwarzania realizowanego w kontekście działalności biura w Irlandii to irlandzkie ustawodawstwo o ochronie danych – niezależnie od tego, czy przetwarzanie ma miejsce w Portugalii, we Włoszech czy w jakimkolwiek innym państwie członkowskim.

Oznacza to, że przy takim założeniu, centrum danych na Węgrzech musiałoby stosować się do irlandzkich przepisów o ochronie danych w odniesieniu do przetwarzania danych osobowych użytkowników korzystających z usług usługodawcy. Pozostałoby to jednak bez uszczerbku dla zastosowania węgierskich przepisów w odniesieniu do przetwarzania danych osobowych przez centrum danych na Węgrzech w związku z jego własnymi działaniami – na przykład przetwarzania danych osobowych dotyczących osób zatrudnionych w tym centrum.

Jeżeli chodzi o biura handlowe mające siedzibę w innych państwach członkowskich, nie są one przedmiotem unijnych przepisów o ochronie danych w sytuacji, gdy ich działania są ograniczone do ogólnych, nieukierunkowanych na użytkownika kampanii reklamowych, które nie wiążą się z przetwarzaniem danych osobowych użytkowników. Jeżeli jednak biura te podejmą decyzję o realizowaniu w kontekście swojej działalności przetwarzania z wykorzystaniem danych osobowych osób fizycznych w państwach, w których prowadzą działalność gospodarczą (dotyczy to na przykład przesyłania użytkownikom oraz potencjalnym przyszłym użytkownikom skierowanych do nich reklam w ramach własnej działalności gospodarczej), będą musiały stosować się do lokalnych przepisów o ochronie danych.

Jeżeli nie można ustalić powiązania między przetwarzaniem danych a irlandzkim przedsiębiorstwem (wsparcie informatyczne jest bardzo ograniczone i nie występuje zaangażowanie w przetwarzanie danych osobowych), stosowanie zasad dotyczących ochrony danych może mieć mimo wszystko miejsce w oparciu o inne przepisy dyrektywy, na przykład gdy administrator danych wykorzystuje środki na terytorium UE. Zostaje to poddane analizie w rozdziale III.3 poniżej.

III.2. Administrator danych prowadzi działalność w miejscu, gdzie zgodnie z międzynarodowym prawem publicznym zastosowanie mają przepisy państwa członkowskiego (art. 4 ust. 1 lit. b)

W art. 4 ust. 1 lit. b) poruszono przypadek, który występuje rzadziej, i w którym przepisy o ochronie danych państwa członkowskiego mają zastosowanie gdy „administrator danych nie prowadzi działalności gospodarczej na terytorium Państwa Członkowskiego, lecz w miejscu, gdzie jego prawo krajowe obowiązuje na mocy międzynarodowego prawa publicznego”.

III.2.a) „…administrator danych nie prowadzi działalności gospodarczej na terytorium Państwa Członkowskiego…”

Pierwszy warunek należy rozumieć tak, że – ze względu na spójność w obrębie art. 4 ust. 1 – administrator danych nie prowadzi na terytorium państwa członkowskiego żadnej działalności gospodarczej, która powodowałaby zastosowanie art. 4 ust. 1 lit. a) (zob. również pkt III.3.a poniżej). Innymi słowy, jeżeli na terytorium UE nie występuje stosowna działalność gospodarcza, nie można określić krajowych przepisów o ochronie danych na mocy art. 4 ust. 1 lit. a).

III.2.b) „…lecz w miejscu, gdzie jego prawo krajowe obowiązuje na mocy międzynarodowego prawa publicznego…”

Zewnętrzne kryteria wynikające z międzynarodowego prawa publicznego mogą jednak w określonej sytuacji przesądzać o rozszerzeniu zastosowania krajowych przepisów o ochronie danych na obszar wykraczający poza granice danego państwa. Może zdarzyć się tak w przypadku, gdy międzynarodowe prawo publiczne lub międzynarodowe porozumienia decydują o prawie mającym zastosowanie w danej ambasadzie lub w konsulacie, bądź o prawie mającym zastosowanie w odniesieniu do statku lub samolotu. W takich przypadkach, gdy administrator danych prowadzi działalność w jednym z tych szczególnych miejsc, o zastosowaniu krajowych przepisów o ochronie danych zdecyduje prawo międzynarodowe.

Ważne jest jednak, aby podkreślić również, iż krajowe przepisy o ochronie danych mogą nie mieć zastosowania w odniesieniu do misji zagranicznych lub organizacji międzynarodowych na terytorium UE w zakresie, w jakim mają one szczególny statut na mocy prawa międzynarodowego – czy to ogólnie czy to na mocy porozumienia o siedzibie głównej: taki wyjątek zapobiegałby stosowaniu art. 4 ust. 1 lit. a) w odniesieniu do misji lub organizacji międzynarodowych.

Przykład nr 6: Ambasady zagraniczne

Ambasada państwa członkowskiego UE w Kanadzie jest przedmiotem krajowych przepisów o ochronie danych tego państwa członkowskiego, nie zaś przepisów o ochronie danych obowiązujących w Kanadzie.

Żadna ambasada obcego państwa na terytorium Niderlandów nie podlega niderlandzkim przepisom o ochronie danych, ponieważ każda ambasada posiada status specjalny na mocy prawa międzynarodowego. Naruszenie bezpieczeństwa danych występujące w kontekście działalności takiej ambasady nie spowodowałoby zatem zastosowania niderlandzkich przepisów o ochronie danych, a w konsekwencji środków represyjnych.

Organizacja pozarządowa, której biura znajdują się w państwach członkowskich UE, zasadniczo nie skorzysta z podobnego wyłączenia, chyba że międzynarodowa umowa zawarta z państwem przyjmującym wyraźnie stanowi inaczej.

III.3. Administrator danych nie prowadzi działalności gospodarczej na terytorium Wspólnoty lecz wykorzystuje do celów przetwarzania danych osobowych środki znajdujące się na terytorium państwa członkowskiego (art. 4 ust. 1 lit. c)

Celem art. 4 ust. 1 lit. c) jest zapewnienie prawa do ochrony danych osobowych ustanowionej na mocy dyrektywy UE również w tych przypadkach, w których administrator danych nie prowadzi działalności na terytorium UE/EOG lecz realizowane przez niego przetwarzanie danych osobowych ma z tym terytorium wyraźny związek, jak wskazano w motywie 20[22].

Artykuł 4 ust. 1 lit. c) stanowi o stosowaniu przepisów prawa członkowskiego w przypadku, gdy „administrator danych nie prowadzi działalności gospodarczej na terytorium Wspólnoty a do celów przetwarzania danych osobowych wykorzystuje środki, zarówno zautomatyzowane jak i inne, znajdujące się na terytorium wymienionego Państwa Członkowskiego, o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium Wspólnoty".

Przepis ten jest szczególnie istotny w świetle rozwoju nowych technologii, a przede wszystkim Internetu, które ułatwiają gromadzenie i przetwarzanie danych osobowych na odległość i niezależnie od fizycznej obecności administratora danych na terytorium UE/EOG[23].

a) „…administrator danych nie prowadzi działalności gospodarczej na terytorium Wspólnoty…"

Przepis ten zyskuje na znaczeniu, gdy administrator danych nie prowadzi na terytorium UE/EOG działalności, która mogłaby zostać uznana za działalność gospodarczą na potrzeby art. 4 ust. 1 lit a) dyrektywy, jak przedstawiono powyżej.

Ważne jest wyjaśnienie interpretacji słów „nie prowadzi działalności gospodarczej". Powinno być jasne, że art. 4 ust. 1 lit. c) ma zastosowanie jedynie wtedy, gdy zastosowania nie ma art. 4 ust. 1 lit. a): to znaczy wtedy, gdy administrator danych nie prowadzi żadnej działalności gospodarczej, która *miałaby znaczenie w związku z przedmiotowymi działaniami* na terytorium UE/EOG. Dlatego fakt, że administrator danych prowadzący działalność poza terytorium UE/EOG korzysta ze środków w państwie członkowskim A, w którym nie prowadzi działalności gospodarczej, nie spowoduje zastosowania przepisów tego państwa członkowskiego, pod warunkiem że administrator danych prowadzi już działalność gospodarczą w państwie członkowskim B i przetwarza dane osobowe w kontekście działań realizowanych przez tą działalność gospodarczą. Zarówno przetwarzanie w państwie członkowskim A (w którym wykorzystywane są środki), jak również w państwie członkowskim B (w którym prowadzona jest działalność gospodarcza) będzie objęte przepisami państwa

[22] Motyw 20: „Przetwarzanie danych przez osobę prowadzącą działalność w państwie trzecim nie może stać na przeszkodzie ochronie osób fizycznych przewidzianej w niniejszej dyrektywie; w tych przypadkach przetwarzanie danych powinno podlegać przepisom prawa Państwa Członkowskiego, w którym znajdują się wykorzystywane do tego celu środki oraz powinny istnieć gwarancje zapewniające przestrzeganie w praktyce praw i obowiązków przewidzianych w niniejszej dyrektywie".

[23] Zobacz Dokument Grupy Roboczej w sprawie określenia międzynarodowego stosowania unijnych przepisów ochronie danych w odniesieniu do przetwarzania danych osobowych w Internecie przez witryny zlokalizowane poza terytorium UE (WP 56).

członkowskiego B. Wyjaśniła to Grupa Robocza w swojej opinii dotyczącej zagadnień ochrony danych związanych z wyszukiwarkami[24]

Z drugiej strony art. 4 ust. 1 lit. c) będzie miał zastosowanie w przypadku, gdy administrator danych prowadzi na terytorium UE „nieistotną" działalność gospodarczą. Oznacza to, że administrator danych prowadzi działalność gospodarczą (jedną lub wiele) w obrębie UE, lecz jej działania są *niezwiązane z przetwarzaniem danych osobowych*. Działalność gospodarcza tego rodzaju nie powodowałaby zastosowania art. 4 ust. 1 lit. a).

Oznacza to, że o ile na etapie stosowania przepisów dyrektywy nie powinny występować luki lub niespójności, fakt prowadzenia nieistotnej działalności nie powinien wstrzymywać zastosowania kryterium „środków": od stosowania tego kryterium można odstąpić w związku z istnieniem działalności gospodarczej jedynie w takim zakresie, w jakim działalność ta przetwarzała dane osobowe w kontekście tych samych działań.

Następstwem powyższej interpretacji jest fakt, że przedsiębiorstwo prowadzące różne działania może spowodować zastosowanie zarówno art. 4 ust. 1 lit. a) jak i art. 4 ust. 1 lit. c) – pod warunkiem, że stosowało ono środki i prowadziło działalność gospodarczą w różnych kontekstach. Innymi słowy, administrator danych prowadzący działalność poza terytorium UE/EOG oraz wykorzystujący środki w UE musi postępować zgodnie z przepisami art. 4 ust. 1 lit. c); dzieje się tak również wtedy, gdy prowadzi on działalność gospodarczą w UE, o ile w ramach tejże działalności przetwarzano dane osobowe *w kontekście innych działań*. Taka działalność gospodarcza spowodowałaby zastosowanie art. 4 ust. 1 lit. a) w odniesieniu do tych szczególnych działań.

Okazja do lepszego wyjaśnienia zakresu art. 4 ust. 1 lit. c) oraz dokładnego znaczenia słów: „administrator danych nie prowadzi działalności gospodarczej na terytorium Wspólnoty" może pojawić się podczas rewizji ram dotyczących ochrony danych, zgodnie z duchem dyrektywy oraz treścią motywu nr 20. W preambule dyrektywy wyraźne stwierdzono, że celem jest ochrona osób fizycznych oraz unikanie luk w stosowaniu przepisów. Z tej przyczyny Grupa Robocza uznaje, że art. 4 ust. 1 lit c) powinien mieć zastosowanie w tych przypadkach, w których na terytorium UE/EOG nie występuje działalność gospodarcza, *która skutkowałaby zastosowaniem art. 4 ust. 1 lit. a)*, lub w przypadku której przetwarzanie *nie jest realizowane w kontekście* działań realizowanych przez taką działalność gospodarczą.

> b) „... a do celów przetwarzania danych osobowych wykorzystuje środki, zarówno zautomatyzowane jak i inne, znajdujące się na terytorium wymienionego państwa członkowskiego… "

Kluczowym elementem, który decyduje o zastosowaniu tego artykułu, a tym samym o przepisach o ochronie danych danego państwa członkowskiego, jest wykorzystanie środków znajdujących się na terytorium tego państwa członkowskiego.

Grupa Robocza wyjaśniła już, że pojęcie „wykorzystywania" zakłada dwa elementy: pewien rodzaj działań administratora danych oraz jego wyraźny zamiar przetwarzania danych[25]. W związku z powyższym wprawdzie nie każde wykorzystanie środków na

---

[24] Opinia Grupy Roboczej ds. Ochrony Danych powołanej na mocy art. 29 nr 1/2008 dotycząca zagadnień ochrony danych związanych z wyszukiwarkami (WP 148).

[25] WP56, op. cit.

terytorium UE/EOG prowadzi do zastosowania dyrektywy, jednak administrator danych nie musi być właścicielem takich środków umożliwiających przetwarzanie lub sprawować nad nimi pełną kontrolę, aby przetwarzanie zostało objęte zakresem dyrektywy.

Należy zauważyć, że występuje różnica między słowem użytym w angielskiej wersji art. 4 ust. 1 lit. c) – „wyposażenie" (ang. *equipment*), a słowem użytym w innych wersjach językowych art. 4 ust. 1 lit. c), które zbliża się raczej do angielskiego słowa „środki" (ang. *means*). Terminologia wykorzystana w innych wersjach językowych art. 4 ust. 1 lit. c) jest również spójna z treścią art. 2 lit. d), w którym znajduje się definicja administratora danych: osoba, która określa cele i „sposoby" przetwarzania.

Biorąc pod uwagę powyższe rozważania, Grupa Robocza rozumie słowo „wyposażenie" jako „środki"[26]. Grupa zauważa również, że zgodnie z dyrektywą, mogą być one „zautomatyzowane jak i inne".

Prowadzi to do szerokiej interpretacji kryterium, które obejmuje tym samym ludzkich lub technicznych pośredników, jak w przypadku sondaży lub zapytań. W efekcie przepis ma zastosowanie w odniesieniu do gromadzenia informacji z wykorzystaniem kwestionariuszy, co ma miejsce na przykład w przypadku niektórych badań farmaceutycznych.

Powstaje pytanie, czy za „środki" mogą być uznane działania polegające na outsourcingu, zwłaszcza przez przetwarzających, realizowane na terytorium UE/EOG w imieniu administratorów danych prowadzących działalność poza terytorium EOG. Obszerna interpretacja, uzasadniona powyżej, prowadzi do odpowiedzi twierdzącej, pod warunkiem, że działania nie są wykonywane w kontekście działań realizowanych w ramach działalności gospodarczej administratora danych na terytorium EOG – w takim przypadku zastosowanie miałby art. 4 ust. 1 lit. a). Należy jednak wziąć pod uwagę pewne niepożądane skutki takiej interpretacji, przedstawione w pkt III.4 poniżej: jeżeli administratorzy danych prowadzący działalność w różnych państwach na całym świecie zlecają przetwarzanie danych w jednym z państw członkowskich UE, w którym znajduje się baza danych i przetwarzający – będą musieli oni zachować zgodność z przepisami o ochronie danych obowiązującymi w tym państwie członkowskim.

Niezbędne jest dokonywanie oceny poszczególnych przypadków, w oparciu o którą przeanalizować można sposób wykorzystywania środków do gromadzenia i przetwarzania danych osobowych. W oparciu o taką argumentację Grupa Robocza przyjęła, że istnieje możliwość, by gromadzenie danych osobowych za pośrednictwem komputerów użytkowników – jak na przykład w przypadku tzw. ciasteczek (ang. *cookies*) lub banerów javascript – powodowało zastosowanie w odniesieniu do usługodawców prowadzących działalność gospodarczą w państwach trzecich art. 4 ust. 1 lit. c), a tym samym unijnych przepisów o ochronie danych [27].

Taka interpretacja przepisu o „wykorzystaniu środków" sprzyja szerokiemu zakresowi stosowania. Jednak jak już wspomniano, w interpretacji tej podkreśla się również pewne

---

[26] Należy również przypomnieć, że w treści poprzednich wersji dyrektywy (na przykład w zmienionej wersji z 1992 r. – COM(92) 422 wersja ostateczna) również zastosowano pojęcie „środków", mimo że na późniejszym etapie negocjacji zostało ono zastąpione pojęciem „wyposażenia", co widoczne jest w tekście wspólnego stanowiska z marca 1995 r.

[27] WP56, op. cit., s. 10 f.

niepożądane konsekwencje, a mianowicie gdy w efekcie europejskie przepisy o ochronie danych mają zastosowanie w przypadkach, w których powiązanie z UE jest ograniczone (np. administrator danych prowadzi działalność gospodarczą poza terytorium UE, przetwarzane są dane osób niemieszkających w UE, wykorzystywane są jedynie środki na terytorium UE). Istnieje wyraźna potrzeba większej jasności oraz określenia dalszych warunków dla stosowania tego kryterium, co pozwoli na zapewnienie większej pewności w przyszłych ramach ochrony danych. Punkt ten zostanie rozwinięty poniżej, w części zawierającej wnioski.

Kolejnym przykładem jest brak jasności odnośnie do tego, w jakim zakresie za środki należy uznawać końcowe urządzenia telekomunikacyjne. Fakt, że narzędzie zostało zaprojektowane lub jest wykorzystywane w pierwszym rzędzie w celu gromadzenia lub dalszego przetwarzania danych osobowych, może zostać uznany za wskazówkę w tym względzie. Jednak fakt, że administrator danych świadomie gromadzi dane osobowe, nawet gdy dzieje się tak „przy okazji", wykorzystując w tym celu środki znajdujące się na terytorium UE, powoduje zastosowanie dyrektywy.

Przykład 7: Usługi geolokalizacji

Przedsiębiorstwo z siedzibą w Nowej Zelandii korzysta z samochodów na całym świecie, w tym w państwach członkowskich UE, aby gromadzić informacje o punktach dostępu Wi-Fi (w tym informacje o prywatnym wyposażeniu osób fizycznych w postaci terminali) w celu świadczenia usług geolokalizacji na rzecz swoich klientów. Taka działalność w wielu przypadkach wiąże się z koniecznością przetwarzania danych.

Spowoduje to zastosowanie dyrektywy o ochronie danych w dwojaki sposób:
- Po pierwsze, krążące po ulicach samochody gromadzące informacje Wi-Fi mogą zostać uznane za środki w rozumieniu art. 4 ust. 1 lit. c);
- Po drugie, realizując usługi geolokalizacji na rzecz osób fizycznych, administrator danych korzysta również z urządzeń przenośnych będących w posiadaniu osób fizycznych (za pośrednictwem specjalnego oprogramowania zainstalowanego w urządzeniach) jako ze środków udostępniania bieżących informacji o lokalizacji urządzenia i jego użytkownika.

Zarówno gromadzenie informacji w celu świadczenia usług, jak i świadczenie samych usług geolokalizacji, będzie musiało przebiegać w zgodzie z dyrektywą.

Przykład nr 8: Wykorzystywanie chmur obliczeniowych

Wykorzystywanie chmur obliczeniowych, w przypadku których dane osobowe są przetwarzane i przechowywane na serwerach w wielu miejscach na świecie, jest złożonym przykładem stosowania przepisów dyrektywy. Nie zawsze znane jest dokładne miejsce przechowywania danych, które może się zmieniać; nie jest to jednak decydujące dla zastosowania prawa właściwego. Dla zastosowania prawa UE wystarczające jest, że administrator danych realizuje przetwarzanie w kontekście działalności gospodarczej w obrębie UE, lub że istotne środki znajdują się na terytorium UE, jak przewiduje art. 4 ust. 1 lit. c) dyrektywy.

Pierwszy decydujący krok to określenie, kim jest administrator danych, a także jakie działania mają miejsce na jakim poziomie. Wyróżnić można dwie perspektywy:

Użytkownikiem usług związanych z przetwarzaniem w chmurze jest administrator danych: na przykład przedsiębiorstwo korzysta z usług terminarza *on-line* w celu organizowania spotkań ze swoimi klientami. Jeżeli przedsiębiorstwo korzysta z usług w kontekście działań swojej działalności gospodarczej na terytorium UE, w oparciu o art. 4 ust. 1 lit. a) w odniesieniu do tego przetwarzania danych za pośrednictwem terminarza *on-line* zastosowanie będzie miało prawo UE. Przedsiębiorstwo powinno upewnić się, że usługi są realizowane z zastosowaniem adekwatnych środków ochrony danych, zwłaszcza w odniesieniu do bezpieczeństwa danych osobowych przechowywanych w chmurze obliczeniowej. Przedsiębiorstwo będzie musiało również poinformować swoich klientów o celu i warunkach wykorzystania ich danych.

Usługodawcą realizującym usługi związane z wykorzystaniem chmur obliczeniowych może w niektórych przypadkach być również administrator danych: sytuacja taka ma miejsce, gdy administrator udostępnia terminarz *on-line*, w którym osoby prywatne mogą wprowadzać wszystkie swoje prywatne terminy, oraz gdy oferuje on usługi dodatkowe takie jak synchronizacja terminów i kontaktów. Jeżeli usługodawca realizujący usługi związane z wykorzystaniem chmur obliczeniowych korzysta ze środków na terytorium UE, zgodnie z art. 4 ust. 1 lit. c) objęty zostanie on unijnymi przepisami o ochronie danych. Jak przedstawiono poniżej, zastosowania dyrektywy nie spowodowałoby wykorzystywanie środków jedynie do celów tranzytu, lecz środków bardziej specjalistycznych, np. jeżeli serwis korzysta z urządzeń obliczeniowych, uruchamia skrypty java lub instaluje tzw. ciasteczka (ang. *cookies*) w celu przechowywania i pobierania danych osobowych użytkowników. Usługodawca realizujący usługi związane z wykorzystaniem chmur obliczeniowych będzie musiał wówczas udostępnić użytkownikom informacje dotyczące sposobu przetwarzania danych, ich przechowywania, ewentualnego dostępu przez strony trzecie; będzie musiał on również zagwarantować odpowiednie środki bezpieczeństwa w celu ochrony informacji.

Przykład nr 9: Administrator danych publikuje listę pedofilów z podziałem na kraje

Administrator danych prowadzący działalność w państwie członkowskim UE/EOG publikuje listę osób – z podziałem na państwa – podejrzanych o popełnienie przestępstwa z udziałem osób małoletnich lub skazanych za jego popełnienie. W odniesieniu do prawa do ochrony danych osobowych osób znajdujących się na takiej liście, prawem właściwym – zgodnie z którym należałoby oceniać, czy takie przetwarzanie jest zgodne z prawem – są krajowe przepisy o ochronie danych państwa członkowskiego, w którym administrator danych prowadzi działalność.

Dla określenia przepisów o ochronie danych mających zastosowanie nie ma znaczenia, czy administrator danych korzysta ze środków w innych państwach członkowskich (takich jak serwery internetowe z różnymi nazwami domen najwyższego poziomu, w tym .fr, .it, .pl itd.) oraz czy – przetwarzając dane w tym celu – bezpośrednio kieruje się do obywateli z innych państw UE (na przykład publikując listy nazwisk osób z danego państwa i w języku tego państwa).

Organ nadzorczy państwa członkowskiego, w którym prowadzona jest dana działalność gospodarcza, może być w każdym razie poproszony o współpracę przez organ nadzorczy innego państwa, podejmujący działania w sprawie skarg złożonych przez osoby fizyczne z innych państw członkowskich.

Oczywiście w innych obszarach prawa można zastosować inne kryteria powiązania, a tym samym prawo właściwe; dotyczy to np. wniesienia pozwu w związku ze zniesławieniem na mocy prawa karnego lub cywilnego.

c) „…o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium Wspólnot…"

Stosowanie przepisów krajowych państwa członkowskiego UE jest wyłączone, gdy środki wykorzystywane przez administratora danych i znajdujące się na terytorium państwa członkowskiego są wykorzystywane jedynie w celu zapewnienia tranzytu przez terytorium Unii, tak jak na przykład dzieje się w przypadku sieci telekomunikacyjnych (przewody) lub usług pocztowych, które jedynie gwarantują tranzyt treści komunikacyjnych przez terytorium UE w celu przekazania ich do państw trzecich.

Jest to wyjątek od zastosowania kryterium środków, a zatem powinien być przedmiotem wąskiej interpretacji. Należy zauważyć, że faktyczne stosowanie tego wyjątku jest coraz rzadsze: w praktyce coraz więcej usług telekomunikacyjnych łączy sam tranzyt i usługi dodatkowe, w tym na przykład sprawdzanie poczty pod kątem spamu lub inne czynności wykonywane w odniesieniu do danych przy okazji ich przesyłania. Zwykła transmisja za pomocą przewodów, realizowana od jednego nadawcy do jednego odbiorcy, stopniowo zanika. Należy o tym pamiętać przygotowując rewizję ram ochrony danych.

d) „…musi wyznaczyć swojego przedstawiciela na terytorium tego Państwa Członkowskiego…" (art. 4 ust. 2)

Dyrektywa nakłada na administratora danych obowiązek wyznaczenia „przedstawiciela" na terytorium państwa członkowskiego, którego prawo ma zastosowanie ze względu na wykorzystanie przez administratora danych środków w tym państwie członkowskim w celu przetwarzania danych osobowych. Dzieje się tak „bez uszczerbku dla postępowań sądowych, jakie mogłyby być podjęte przeciwko samemu administratorowi danych".

W tym ostatnim przypadku trudności praktyczne stwarza kwestia egzekwowania przepisów wobec przedstawiciela, czego dowiodły doświadczenia państw członkowskich. Dotyczy to przypadku, w którym na przykład jedynym przedstawicielem administratora danych na terytorium UE jest kancelaria prawna. W krajowych przepisach wykonawczych nie ma jednolitej odpowiedzi na pytanie, czy przedstawiciela można obciążyć odpowiedzialnością w zastępstwie administratora danych i nałożyć na niego sankcje – czy to na mocy prawa cywilnego, czy też karnego. Decydujący jest tutaj charakter kontaktów między przedstawicielem a administratorem danych. W niektórych państwach członkowskich przedstawiciel zastępuje administratora danych również w odniesieniu do postępowania egzekucyjnego i sankcji, zaś w innych dysponuje zwykłym upoważnieniem. Niektóre przepisy krajowe wyraźnie przewidują nakładanie kar na przedstawicieli[28], podczas gdy w innych państwach członkowskich nie przewidziano takiej możliwości[29].

[28] Belgijska ustawa o ochronie danych z dnia 8 grudnia 1992 r., Dz.U. 18 z marca 1993 r.; Niderlandzka ustawa z dnia 6 lipca 2000 r. dotycząca ochrony danych osobowych, Biuletyn urzędowy,

W tym względnie niezbędna jest harmonizacja przepisów na poziomie europejskim, przy czym celem jest zapewnienie większej skuteczności po stronie przedstawiciela. W szczególności osoby, których dotyczą dane, powinny mieć możliwość dochodzenia swoich praw wobec przedstawiciela, bez uszczerbku dla postępowań sądowych, jakie mogłyby być podjęte przeciwko samemu administratorowi danych.

III.4. Rozważania dotyczące praktycznych konsekwencji stosowania art. 4 ust. 1 lit. c)

Decydujący aspekt stosowania art. 4 ust. 1 lit. c) wiąże się z jego praktycznymi konsekwencjami dla administratora danych. Gdy administrator danych znajduje się poza terytorium UE/EOG będzie musiał zastosować zasady dyrektywy, jeżeli w operacjach przetwarzania danych osobowych wykorzystuje środki znajdujące się na terytorium UE. Można byłoby podać w wątpliwość, czy zasady będą miały zastosowanie jedynie w odniesieniu do etapów przetwarzania mającego miejsce w UE, czy tez w odniesieniu do administratora danych jako takiego, na wszystkich etapach przetwarzania – również tych, które mają miejsce w państwie trzecim. Kwestie te mają szczególne znaczenie w środowiskach sieciowych, takich jak przetwarzanie w chmurze obliczeniowej, oraz w kontekście spółek wielonarodowych.

Rozważmy na przykład konsekwencje dla administratorów danych prowadzących działalność w różnych państwach na świecie, którzy zlecają przetwarzanie danych we Francji, gdzie znajdują się baza danych oraz środki umożliwiające przetwarzanie. Jeżeli różni administratorzy danych korzystają z infrastruktury we Francji, zastosowanie ma art. 4 ust. 1 lit. c), a wszyscy administratorzy danych muszą zachować zgodność z przepisami prawa francuskiego. Może to powodować niepożądane konsekwencje w odniesieniu do skutków ekonomicznych i możliwości egzekwowania.

Przyczyny praktyczne przemawiałyby za ograniczeniem stosowania kryterium „wyposażenia/środków", jednak na drodze do takiego ograniczenia znajduje się fakt, że przepisy o ochronie danych mają na celu ochronę prawa podstawowego. Ograniczenie praw osób fizycznych w odniesieniu do niektórych etapów przetwarzania ich danych wydaje się niedopuszczalne. Nie do przyjęcia byłoby również ograniczenie zakresu ochrony jedynie do osób przebywających w UE, jako że prawo podstawowe do ochrony danych osobowych jest realizowane bez względu na obywatelstwo lub miejsce pobytu. W konsekwencji zastosowanie kryterium wynikającego z art. 4 ust. 1 lit. c) prowadzi do stosowania przepisów dyrektywy w odniesieniu do administratora danych jako takiego, na wszystkich etapach przetwarzania, również tych, które mają miejsce w państwie trzecim.

Należy skłaniać się ku zastosowaniu dyrektywy w odniesieniu do administratora danych na wszystkich etapach przetwarzania o ile powiązanie z UE jest skuteczne i nie wydaje się wątpliwe (tak jak na przykład w przypadku bardziej niezamierzonego niż celowego wykorzystania środków w jednym z państw członkowskich).

---

rozporządzenia i dekrety (Staatsblad) nr 302 z 20 lipca 2000 r. Zobacz również przepisy greckie (art. ust. 3 lit. b) w powiązaniu zart.21 ust. 1 ustawy 2472/1997).

[29] Na przykład obowiązująca we Francji ustawa nr 78/17 z dnia 6 stycznia 1978 r. nie przewiduje nakładania takiego rodzaju kar na przedstawicieli.

Przydatny w kontekście pewności prawa byłby bardziej konkretny czynnik łączący, uwzględniający ukierunkowanie na osoby fizyczne, mający znaczenie jako kryterium będące uzupełnieniem kryterium „wyposażenia/środków; zostanie to wyjaśnione dalej, w części zawierającej wnioski. Takie kryterium nie jest nowe i było już wykorzystywane w innych kontekstach w UE[30]; wykorzystano je również w przepisach Stanów Zjednoczonych służącym ochronie dzieci w środowisku *on-line*[31]. Podobna sytuacja ma miejsce w przypadku niektórych przepisów krajowych transponujących dyrektywę 2000/31/WE o handlu elektronicznym[32], które stanowią, że usługodawcy nieprowadzący działalności na terytorium EOG będą objęci zakresem tych przepisów krajowych, jeżeli będą kierować swoje usługi do odbiorców na ich konkretnym terytorium.

W prowadzonych w przyszłości dyskusjach dotyczących rewizji ram o ochronie danych można rozważyć zastosowanie podobnego kryterium w odniesieniu do unijnych ram ochrony danych .

Kolejna praktyczna konsekwencja zastosowania art. 4 ust. 1 lit. c) dotyczy interakcji między tym przepisem a art. 25 i 26 dyrektywy. Fakt, że administrator danych prowadzący działalność poza terytorium UE/EOG korzysta ze środków na terytorium UE/EOG – a tym samym musi przestrzegać wszystkich istotnych przepisów dyrektywy – wiązałby się z ewentualnym zastosowaniem art. 25 i 26. Jednak w praktyce określenie dokładnych skutków takiego scenariusza może być trudne.

Jeżeli na przykład administrator danych X prowadzący działalność gospodarczą poza terytorium EOG gromadzi dane osobowe za pośrednictwem środków znajdujących się na terytorium UE (przykładowo za pośrednictwem tzw. ciasteczek (ang. *cookies*) lub za pośrednictwem przetwarzającego), musi przestrzegać przepisów dyrektywy na wszystkich etapach przetwarzania. Istnieje tutaj pewna zbieżność z sytuacją, w której administrator danych prowadzący działalność gospodarczą na terytorium EOG przekazuje dane osobowe przetwarzającemu znajdującemu się poza terytorium EOG: również w takim przypadku administrator danych i przetwarzający prowadzący działalność poza terytorium EOG będą związani dyrektywą. Jednak nie jest całkowicie jasne, w jaki sposób zasady te wykonywane są – zgodnie z zawartymi w art. 25 i 26 dyrektywy wymogami o odpowiednim stopniu ochrony danych – w praktyce, w scenariuszu przewidzianym w art. 4 ust. 1 lit. c) dotyczącym administratora danych prowadzącego działalność gospodarczą poza terytorium EOG. Grupa Robocza jest zdania, że należy w dalszym ciągu poświęcić uwagę istniejącym narzędziom regulującym zasady transferu, dążąc do lepszego poparcia takiej sytuacji przepisami.

---

30 Por. art. 15 ust. 1 rozporządzenia Rady (WE)nr 44 /2001 z dnia 22 grudnia 2000 w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz.U. L 12 z 16.1.2001, s. 1), zaś interpretacja rozporządzenia – zob. Wnioski rzecznika generalnego Trstenjaka z dnia 18 maja 2010 r., w C-144/09, *Hotel Alpenhof*.

31 Zastosowanie amerykańskiej ustawy chroniącej dzieci w środowisku on-line (*Children's Online Privacy Protection Act, COPPA*) może być w rzeczywistości uruchomione przez fakt, że publikator treści znajduje się na terenie USA, bądź przez fakt, że strona internetowa jest skierowana do amerykańskich dzieci: jeżeli strony internetowe lub serwisy internetowe o zagranicznej kierują swoje treści do dzieci na terytorium USA lub świadomie gromadzą lub udostępniają dane osobowe dotyczące dzieci na terytorium USA, muszą zachować zgodność z przepisami COPPA. Zobacz 16 CFR 312.2, dostępny pod adresem: http://www.ftc.gov/os/1999/10/64fr59888.pdf, s. 59912.

32 Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), Dz.U. L 178 z 17.7.2000, s. 1.

III.5. Prawo właściwe dla środków bezpieczeństwa (art. 17 ust. 3)

Zgodnie z art. 17 ust. 3 umowa lub akt prawny stwarzający powiązanie między przetwarzającym a administratorem danych powinien również zapewnić zgodność ze środkami bezpieczeństwa, które są „określone przez ustawodawstwo Państwa Członkowskiego, w którym przetwarzający prowadzi działalność gospodarczą".

Zasada ta służy zapewnieniu jednolitych wymogów w obrębie jednego państwa członkowskiego w odniesieniu do środków bezpieczeństwa, a także ułatwienie wykonania. Należy jednak zauważyć, że z perspektywy europejskiej wymogi dotyczące bezpieczeństwa w poszczególnych państwach członkowskich znacznie się od siebie różnią: w niektórych przepisach zawarto bardzo szczegółowe regulacje, podczas gdy inne stanowią przeniesienie ogólnych przepisów zawartych w dyrektywie. W przypadkach, w których przepisy krajowe są ogólne, zaś ich treść została przejęta z dyrektywy, sytuacja ta nie będzie miała żadnych praktycznych konsekwencji. Dla przetwarzającego nie będzie problemem zachowanie zgodności z bardziej szczegółowymi obowiązkami nałożonymi na niego przez administratora danych na mocy jego prawa krajowego; również administrator danych będzie w stanie przyjąć bardziej szczegółowe wymogi nałożone na mocy prawa przetwarzającego. Artykuł 17 ust. 3 decyduje na korzyść prawa przetwarzającego jedynie w tych przypadkach, w których szczegółowe przepisy są odmienne lub wręcz sprzeczne[33]. Wydaje się jednak właściwe, aby w dyskusjach poprzedzających rewizję ram ochrony danych przewidziano zagadnienie dalszej harmonizacji obowiązków związanych z bezpieczeństwem.

III.6. Kompetencje i współpraca organów nadzorczych (art. 28 ust. 6)

Jak wspomniano powyżej (zob. pkt II.2.e), celem art. 28 ust. 6 jest zamknięcie ewentualnej luki między prawem właściwym a jurysdykcją organów nadzorczych, która może wystąpić w obszarze ochrony danych w obrębie rynku wewnętrznego.

W następstwie tego przepisu krajowe organy ds. ochrony danych są właściwe do nadzorowania wykonywania przepisów o ochronie danych na terytorium państwa członkowskiego, na którym prowadzą działalność. Jeżeli jednak na tym terytorium zastosowanie miało prawo innego państwa członkowskiego, kompetencje wykonawcze organu ds. ochrony danych nie będą ograniczone: zawarte w dyrektywie kryteria dotyczące prawa właściwego przewidują możliwość uprawnienia organu ds. ochrony danych do weryfikacji i interwencji w sprawie operacji przetwarzania, która ma miejsce na jego terytorium, nawet wtedy, gdy prawem właściwym jest prawo innego państwa członkowskiego.

III.6.a) „…organ nadzorczy jest właściwy, niezależnie od krajowych przepisów…"

W następstwie tego przepisu krajowy organ nadzorczy zawsze ma prawo podjąć działania w obrębie swojej właściwości miejscowej, niezależnie od tego, czy prawem właściwym jest jego krajowe prawo o ochronie danych czy też prawo o ochronie danych innego państwa członkowskiego.

[33] Powinno to pozwolić na uniknięcie sytuacji, w których przetwarzający dane jest umiejscawiany w innym państwie, w którym obowiązki są mniejsze, co uznawane jest za naruszenie obowiązków administratora danych.

III.6.b) „…do wykonywania na terytorium Państwa Członkowskiego uprawnień powierzonych mu …”

Również wtedy, gdy zastosowanie mają przepisy o ochronie danych innego państwa członkowskiego, organ nadzorczy będzie w stanie w pełni wykonywać na swoim terytorium wszelkie uprawnienia powierzone mu w krajowym systemie prawnym. Obejmuje to uprawienia dochodzeniowe, uprawnienia interwencyjne, prawo udziału w postępowaniach prawnych i nakładania sankcji.

W przypadku zaangażowania szeregu organów ds. ochrony danych, w tym organu ds. ochrony danych właściwego pod względem miejsca oraz organu ds. ochrony danych kraju, którego przepisy mają zastosowanie, bardzo ważne jest zorganizowanie ich współpracy, a także jasne określenie roli każdego z tych organów. Należy w związku z tym podjąć kilka kwestii, a zwłaszcza:

- kwestie proceduralne, takie jak identyfikacja organu wiodącego oraz sposobu, w jaki będzie on współpracował z innymi organami ds. ochrony danych;
- zakres kompetencji, jakimi dysponować będą poszczególne organy ds. ochrony danych. Przede wszystkim, na ile organ ds. ochrony danych właściwy pod względem miejsca będzie korzystał ze swoich uprawnień w odniesieniu do stosowania zasad materialnych i sankcji? Czy powinien on ograniczyć stosowanie swoich kompetencji jedynie do weryfikacji faktów, czy może podejmować prowizoryczne środki wykonawcze czy też nawet środki ostateczne? Czy może dokonywać własnej interpretacji przepisów prawa właściwego, czy też jest to przywilejem organu ds. ochrony danych państwa członkowskiego, którego prawo jest prawem właściwym? W tym kontekście należy zwrócić uwagę, że nie we wszystkich państwach przepisy przewidują możliwość nakładania sankcji na wszystkie zaangażowane strony[34].

Wysoki stopień harmonizacji kompetencji nadzorczych powierzonych organom nadzorczym na mocy art. 28 dyrektywy jest istotnym warunkiem gwarantującym skuteczne i niedyskryminujące transgraniczne wypełnianie przepisów o ochronie danych. Kwestia ta wymaga dalszej analizy; Grupa Robocza wyda wytyczne w tej sprawie w oddzielnym dokumencie.

Przykład nr 10: Wewnątrzujnijne transgraniczne przetwarzanie danych osobowych

Działania polegające na przetwarzaniu danych mają miejsce na terytorium Zjednoczonego Królestwa, jednak odbywają się w kontekście działań działalności gospodarczej administratora danych prowadzonej w Niemczech. Będzie to miało następujące konsekwencje:

- w odniesieniu do przetwarzania w Zjednoczonym Królestwie zastosowanie będzie miało prawo niemieckie;

- organ ds. ochrony danych w Zjednoczonym Królestwe powinien mieć prawo przeprowadzenia inspekcji na terenie siedziby w Zjednoczonym Królestwie, a także dokonania ustaleń, które przekazywane są niemieckiemu organowi ds. ochrony danych;

[34] Na przykład prawo Grecji przewiduje nakładanie sankcji jedynie na administratorów danych i ich przedstawicieli, nie zaś na przetwarzających.

- niemiecki organ ds. ochrony danych powinien być w stanie nałożyć sankcje na administratora danych prowadzącego działalność w Niemczech w oparciu o ustalenia dokonane przez organ ds. ochrony danych w Zjednoczonym Królestwie.

Dodatkowo uwzględnić należy, że gdy działalność gospodarcza w Zjednoczonym Królestwie to działalność przetwarzającego, aspekty związane z bezpieczeństwem przetwarzania są objęte wymogami przepisów o ochronie danych obowiązujących w Zjednoczonym Królestwie. W takiej sytuacji powstaje pytanie, jak w sposób należyty dopełnić wymogów tego prawa.

III.6.c) „… współpracują ze sobą w zakresie koniecznym do wykonywania swoich obowiązków…"

Organy nadzorcze mają obowiązek współpracowania ze sobą („współpracują ze sobą"), jednak jednocześnie obowiązek ten ograniczono do tego, co jest niezbędne do pełnienia ich obowiązków. Wnioski o współpracę powinny zatem odnosić się do wykonywania ich kompetencji; zazwyczaj dotyczą one spraw o charakterze transgranicznym.

Powyższy przepis odnosi się w szczególności do wymiany „wszelkich przydatnych informacji", które mogą na przykład dotyczyć informacji o właściwych przepisach i aktach prawnych mających zastosowanie w danym przypadku. Prawdopodobne jest jednak, że współpraca będzie miała miejsce również na innych płaszczyznach: realizacji skarg o charakterze transgranicznym, gromadzenia dowodów dla innych organów ds. ochrony danych lub nakładania sankcji.

Poruszona kwestia okazuje się jeszcze bardziej istotna w kontekście międzynarodowym, gdy administratorzy danych prowadzą działalność w skali światowej; w związku z czym niezbędne wydaje się udoskonalenie współpracy w zakresie egzekwowania. Potrzebnym i przydatnym krokiem w tym kierunku są inicjatywy takie jak Światowa Sieć na Rzecz Prywatności (ang. *Global Privacy Enforcement Network, GPEN),* w które zaangażowane są organy ds. ochrony danych reprezentujące różne kontynenty.

Przykład nr 11: Serwis społecznościowy posiadający siedzibę główną w państwie trzecim i prowadzący działalność gospodarczą na terytorium UE

Serwis społecznościowy posiadający główną siedzibę w państwie trzecim prowadzi działalność gospodarczą w państwie członkowskim UE. W ramach działalności gospodarczej określana i realizowana jest polityka związana z przetwarzaniem danych osobowych mieszkańców UE. Serwis społecznościowy aktywnie skupia się na mieszkańcach wszystkich państw członkowskich UE, którzy stanowią znaczną część jego klientów, i którzy są źródłem dużej części jego dochodów. Instaluje on również tzw. ciasteczka (ang. *cookies*) na komputerach użytkowników pochodzących z UE.

W tym przypadku prawem właściwym będą – zgodnie z art. 4 ust. 1 lit. a) – przepisy o ochronie danych państwa członkowskiego, w którym przedsiębiorstwo zarejestrowało swoją działalność gospodarczą na terytorium UE. Kwestia, czy serwis społecznościowy wykorzystuje środki znajdujące się na terytorium innego państwa członkowskiego, nie jest istotna, ponieważ całość przetwarzania odbywa się w kontekście działań jednej działalności gospodarczej, zaś dyrektywa wyklucza jednoczesne stosowanie art. 4 ust. 1 lit. a) oraz art. 4 ust. 1 lit. c).

Organ nadzorczy państwa członkowskiego, w którym portal społecznościowy prowadzi swoją europejską działalność gospodarczą, będzie miał jednak obowiązek – zgodnie z art. 28 ust. 6 – współpracować z innymi organami nadzorczymi, między innymi w celu realizowania wniosków lub skarg napływających od mieszkańców z innych państw UE.

Przykład nr 12: Europejska platforma „e-zdrowie"

Platforma została stworzona na szczeblu europejskim w celu ułatwienia przetwarzania dokumentacji pacjentów w przypadkach transgranicznych. Platforma pozwala na wymianę zestawień i podsumowań danych dotyczących pacjentów, ich dokumentacji medycznej i przepisanych leków, co ułatwiać ma opiekę zdrowotną podczas podróży zagranicznych.

Platforma ułatwia wymianę informacji, jednak w dalszym ciągu w każdym państwie członkowskim znajdować się będzie jedna lub kilka jednostek, w kontekście których przetwarzane będą dane dotyczące pacjentów. Jeżeli na przykład obywatel Bułgarii podróżujący do Portugalii potrzebuje pilnego leczenia, jego dane będą przetwarzane za pośrednictwem platformy przez portugalskie służby medyczne zgodnie z portugalskimi przepisami o ochronie danych. Jeżeli po powrocie do Bułgarii pacjent chciałby zażądać odszkodowania w związku z przetwarzaniem jego danych przez portugalskiego administratora danych, najpierw złoży swoją skargę do bułgarskiego organu ds. ochrony danych. Bułgarski organ ds. ochrony danych podejmie wówczas współpracę z portugalskim organem ds. ochrony danych, aby ustalić fakty, a także stwierdzić, czy w oparciu o portugalskie ustawodawstwo miało miejsce naruszenie przepisów.

Jeżeli Komisja Europejska interweniuje w funkcjonowanie platformy, organizując przepływ danych osobowych i gwarantując bezpieczeństwo systemu, może ona zostać uznana za przetwarzającego dane osobowe, co spowodowałoby zastosowanie rozporządzenia (WE) 45/2001. W powyższym przykładzie, jeżeli obywatel Bułgarii złożył skargę ze względu na naruszenie zabezpieczeń w związku z jego danymi medycznymi, bułgarski organ ds. ochrony danych podjąłby współpracę z Europejskim Inspektorem Ochrony Danych w celu zidentyfikowania okoliczności oraz skutków naruszenia.

IV. Wnioski

Celem niniejszej opinii jest wyjaśnienie zakresu stosowania dyrektywy 95/46/WE, a w szczególności art. 4 dyrektywy. Uwypuklono w niej jednak również kilka obszarów, w których przyszłości wprowadzić można ewentualne ulepszenia. Główne ustalenia w związku z powyższym zostały zamieszczone poniżej.

IV.1. Wyjaśnienie obowiązujących przepisów

Określenie sposobu stosowania przepisów UE w odniesieniu do przetwarzania danych osobowych służy wyjaśnieniu zakresu stosowania unijnych przepisów o ochronie danych zarówno na terytorium UE/EOG jak i w szerszym kontekście międzynarodowym. Jasne zrozumienie prawa właściwego pomoże w zapewnieniu administratorom danych

pewności prawa, zaś osobom fizycznym oraz innym zainteresowanym stronom – w zarysowaniu wyraźnych ram. Ponadto właściwe zrozumienie przepisów prawa właściwego powinno zagwarantować eliminację luk w zakresie ochrony danych osobowych na wysokim poziomie, jaką zapewnia dyrektywa 95/46.

Kluczowym przepisem dotyczącym prawa właściwego jest art. 4, w którym określono, które przepisy prawa krajowego przyjęte na mocy dyrektywy, mogą być stosowane w odniesieniu do przetwarzania danych osobowych.

Na podstawie art. 4 ust. 1 lit. a) państwo członkowskie powinno zastosować krajowe przepisy o ochronie danych gdy przetwarzanie danych odbywa się w kontekście prowadzenia przez administratora danych działalności gospodarczej na terytorium państwa członkowskiego. Kluczem umożliwiającym identyfikację działalności gospodarczej mającej znaczenie z punktu widzenia art. 4 ust. 1 lit. a) jest ustalenie, czy przedmiotowa organizacja prowadzi działania w sposób efektywny i rzeczywisty. Ponadto odniesienie do (*jakiejkolwiek*) działalności gospodarczej oznacza, że zastosowanie przepisów prawa danego państwa członkowskiego będzie uzależnione od miejsca prowadzenia przez administratora danych działalności gospodarczej w tym państwie członkowskim, zaś przepisy innych państw członkowskich mogą zostać zastosowane w związku z inną działalnością gospodarczą tego administratora danych prowadzoną w tych państwach członkowskich.

Czynnikiem determinującym określenie zakresu prawa właściwego jest pojęcie „kontekstu działań", nie zaś miejsca, w którym znajdują się dane. Pojęcie „kontekstu działań" implikuje, że prawo właściwe nie jest prawem państwa członkowskiego, w którym działalność gospodarczą prowadzi *administrator danych*, lecz tego, w którym w ramach *działalności gospodarczej* administratora danych prowadzone są *działania* związane z przetwarzaniem danych osobowych. W tym kontekście kluczowy jest stopień zaangażowania działalności gospodarczej (działalności gospodarczych) w działania, w kontekście których przetwarzane są dane osobowe. Ponadto należy rozważyć charakter działań realizowanych przez działalność gospodarczą oraz potrzebę zagwarantowania skutecznej ochrony praw osób fizycznych. W analizie tych kryteriów należy przyjąć podejście funkcjonalne: bardziej niż teoretyczne wskazanie przez strony prawa właściwego, to ich postępowanie w praktyce i interakcje stanowią czynniki, które powinny być czynnikami decydującymi.

W art. 4 ust. 1 lit. b) poruszono przypadek, który występuje rzadziej, i w którym przepisy o ochronie danych państwa członkowskiego mają zastosowanie gdy „administrator danych nie prowadzi działalności gospodarczej na terytorium Państwa Członkowskiego, lecz w miejscu, gdzie jego prawo krajowe obowiązuje na mocy międzynarodowego prawa publicznego". Zewnętrzne kryteria wynikające z międzynarodowego prawa publicznego przesądzą w konkretnych sytuacjach o rozszerzeniu zastosowania krajowych przepisów o ochronie danych na obszar wykraczający poza granice danego państwa, przykładowo w przypadku ambasad lub statków.

Celem art. 4 ust. 1 lit. c) jest zapewnienie prawa do ochrony danych osobowych ustanowionej na mocy dyrektywy UE również w tych przypadkach, w których administrator danych nie prowadzi działalności na terytorium UE/EOG, lecz realizowane przez niego przetwarzanie danych osobowych ma z tym terytorium wyraźny związek. Dla zapewnienia spójności w obrębie art. 4 oraz w celu uniknięcia luk w stosowaniu przepisów o ochronie danych, Grupa Robocza uznaje, że istnienie działalności

gospodarczej administratora danych na terytorium Wspólnoty, jeżeli działalność ta nie jest działalnością istotną z punktu widzenia art. 4 ust. 1 lit. a), nie powinno stanowić przeszkody dla stosowania art. 4 ust. 1 lit. c). Przepis dotyczący „wykorzystania środków" zawarty w art. 4 ust. 1 lit. c) powinien natomiast mieć zastosowanie w tych przypadkach, w których na terytorium UE/EOG nie występuje działalność gospodarcza, która *skutkowałaby zastosowaniem art. 4 ust. 1 lit. a)*, lub gdy przetwarzanie *nie jest realizowane w kontekście* takiej działalności gospodarczej.

Kluczowym elementem, który decyduje o zastosowaniu art. 4 ust. 1 lit. c), a tym samym krajowych przepisów o ochronie danych, jest wykorzystanie środków znajdujących się na terytorium danego państwa członkowskiego. Koncepcja „wykorzystania" zakłada istnienie dwóch elementów: pewnego rodzaju działań administratora danych oraz wyraźnego zamiaru administratora danych przetwarzania danych. W związku z powyższym wprawdzie nie każde wykorzystanie środków na terytorium UE/EOG prowadzi do zastosowania dyrektywy, jednak administrator danych nie musi być właścicielem takich środków umożliwiających przetwarzanie lub sprawować nad nimi pełną kontrolę, aby zostać objętym zakresem dyrektywy.

Jeżeli chodzi o pojęcie „wyposażenia/środków", jego wyrażenie za pomocą pojęcia „środki" w innych językach UE, może prowadzić do szerokiej interpretacji tego kryterium, co sprzyja szerokiemu zakresowi zastosowania. Taka interpretacja może w niektórych przypadkach prowadzić do stosowania europejskich przepisów o ochronie danych w sytuacjach, w których przedmiotowe przetwarzanie nie ma rzeczywistego powiązania z terytorium UE/EOG. W każdym przypadku przetwarzanie danych osobowych przez administratora danych prowadzącego działalność poza terytorium UE/EOG, z wykorzystaniem środków na terytorium UE/EOG, powoduje zastosowanie dyrektywy w oparciu o art. 4 ust. 1 lit. c), co oznacza, że wszystkie inne właściwe przepisy dyrektywy również będą stosowane.

Stosowanie przepisów krajowych państwa członkowskiego UE jest wyłączone, gdy środki wykorzystywane przez administratora danych i znajdujące się na terytorium państwa członkowskiego są wykorzystywane jedynie w celu zapewnienia tranzytu przez terytorium Wspólnoty, tak jak na przykład dzieje się w przypadku sieci telekomunikacji (przewody) lub usług pocztowych, które jedynie gwarantują tranzyt treści komunikacyjnych przez terytorium Wspólnoty w celu przekazania ich do państw trzecich.

Artykuł 4 ust. 2 nakłada na administratora danych obowiązek wyznaczenia przedstawiciela na terytorium państwa członkowskiego, którego prawo ma zastosowanie ze względu na wykorzystanie środków przez administratora danych w tym państwie członkowskim w celu przetwarzania danych osobowych. W tym ostatnim przypadku trudności sprawiać może egzekwowanie zobowiązań od przedstawiciela.

Artykuł 17 ust. 3 stanowi, że umowa lub akt prawny stwarzający powiązanie między przetwarzającym a administratorem danych powinien również wymagać od przetwarzającego zachowania zgodności ze środkami bezpieczeństwa, które są „określone przez ustawodawstwo Państwa Członkowskiego, w którym przetwarzający prowadzi działalność gospodarczą". Zasada ta służy zapewnienie jednolitych wymogów w obrębie jednego państwa członkowskiego w odniesieniu do środków bezpieczeństwa, a także ułatwienie wykonania.

Celem art. 28 ust. 6 jest zamknięcie ewentualnej luki między prawem właściwym a jurysdykcją organów nadzorczych, która może wystąpić w obszarze ochrony danych w obrębie rynku wewnętrznego; wspomniany artykuł stanowi, że organ ds. ochrony danych powinien mieć możliwość korzystania ze swoich praw w celu weryfikowania operacji przetwarzania, które mają miejsce na jego terytorium, oraz do ingerowania w takie operacje – również wtedy, gdy prawem właściwym jest prawo innego państwa członkowskiego.

IV.2. Ulepszenie obowiązujących przepisów

Wskazania i przykłady przedstawione powyżej powinny przyczynić się do zwiększenia pewności prawa oraz ochrony praw osób fizycznych na etapie określania prawa właściwego dla przetwarzania danych osobowych. Jednak podczas ich opracowywania stwierdzono istnienie pewnych niedociągnięć.

Pojęcia wykorzystane w dyrektywie, a także spójność między poszczególnymi fragmentami art. 4, skorzystałyby dzięki dalszym wyjaśnieniom, które mogłyby stanowić element rewizji ogólnych ram ochrony danych Grupa Robocza ustaliła, że potrzeba dalszych wyjaśnień istnieje w kilku obszarach:

a. Istnieje potrzeba wyjaśnienia braku spójności w treści art. 4 ust. 1 lit. a) oraz art. 4 ust. 1 lit. c) w odniesieniu do pojęcia „działalności gospodarczej", a także stwierdzenia, że administrator danych „nie prowadzi działalności" w UE. Aby spójność z art. 4 ust. 1 lit. a), w którym użyto kryterium „działalności gospodarczej", została zachowana, art. 4 ust. 1 lit. c) powinien mieć zastosowanie we wszystkich przypadkach, w których na terytorium UE nie występuje *działalność gospodarcza*, *która powodowałaby zastosowanie art. 4 ust. 1 lit. a),* lub w których przetwarzanie *nie jest realizowane w kontekście* działań takiej działalności gospodarczej.

b. Przydatne byłyby również dodatkowe wyjaśnienia w odniesieniu do pojęcia „kontekstu działań" realizowanych przez działalność gospodarczą. Grupa Robocza podkreśliła potrzebę oceny *stopnia zaangażowania* działalności gospodarczej (działalności gospodarczych) w działania, w kontekście których przetwarzane są dane osobowe, lub – mówiąc innymi słowy - potrzebę sprawdzenia „kto czym się zajmuje" w ramach której działalności gospodarczej. Kryterium to jest interpretowane z uwzględnieniem wyników prac przygotowawczych poprzedzających dyrektywę oraz określonego wówczas celu, jakim było zachowanie rozproszonych przepisów krajowych mających zastosowanie do różnych działalności gospodarczych administratorów danych w obrębie UE. Grupa Robocza jest zdania, że art. 4 ust. 1 lit. a) w obecnie obowiązującej formie prowadzi do wykonalnych lecz nierzadko złożonych rozwiązań, co wydaje się być argumentem przemawiającym za bardziej scentralizowanym i ujednoliconym podejściem.

c. Zmiana planowana w celu uproszczenia zasad umożliwiających określenie prawa właściwego obejmowałaby powrót do zasady państwa pochodzenia: do wszelkiej działalności gospodarczej administratora danych w obrębie UE zastosowanie miałyby wówczas te same przepisy, niezależnie od terytorium, na którym działalność ta jest prowadzona. W takiej sytuacji pierwszym kryterium, jakie miałoby zastosowanie, byłoby miejsce, w którym znajduje się siedziba główna działalności gospodarczej prowadzonej przez administratora danych. Fakt, że

działalność gospodarcza jest prowadzona w kilku państwach w obrębie UE, nie powodowałby rozproszonego stosowania przepisów krajowych.

d. Takie podejście można byłoby przyjąć jedynie wtedy, gdy między przepisami poszczególnych państw członkowskich nie występowałyby znaczące różnice. W przeciwnym przypadku skuteczne zastosowanie zasady państwa pochodzenia spowodowałoby wyszukiwanie przez administratorów danych na miejsca prowadzenia działalności tych państw członkowskich, których przepisy są uznawane za bardziej liberalne wobec administratorów danych (ang. *forum-shopping*). Mogłoby to oczywiście przynosić szkodę osobom, których dane dotyczą. Pewność prawa dla administratorów danych oraz dla osób, których dane dotyczą, będzie zagwarantowana jedynie wówczas, gdy osiągnięte zostanie obszerne ujednolicenie przepisów krajowych, w tym ujednolicenie obowiązków związanych z bezpieczeństwem. W związku z powyższym Grupa Robocza popiera zdecydowane ujednolicenie przepisów o ochronie danych, również jako warunek dla ewentualnego powrotu do zasady państwa pochodzenia.

e. W przypadkach, w których administrator danych prowadzi działalność poza terytorium UE, miałyby zastosowanie dodatkowe kryteria; dzięki temu istniałaby pewność, że istnieje wystarczające powiązanie z terytorium UE, oraz że terytorium UE nie będzie wykorzystywane przez administratorów danych prowadzących działalność gospodarczą w państwach trzecich do podejmowania nielegalnych działań związanych z przetwarzaniem danych. W tym względzie rozwinięte mogłyby zostać dwa następujące kryteria:

- Ukierunkowanie na osoby fizyczne lub „podejście ukierunkowane na usługi”: wiązałoby się to z wprowadzeniem kryterium dotyczącego zastosowania unijnych przepisów o ochronie danych, przewidującego ukierunkowanie działań wymagających przetwarzania danych osobowych na osoby fizyczne w UE. Musiałoby to wiązać się z znaczącym ukierunkowaniem, opartym na skutecznym powiązaniu między osobą fizyczną a konkretnym państwem UE, bądź takie ukierunkowanie uwzględniać. Poniższe przykłady ilustrują, co mogłoby obejmować wspomniane ukierunkowanie: fakt, że administrator danych gromadzi dane osobowe w kontekście usług dostępnych lub skierowanych wyłącznie do mieszkańców UE, za pośrednictwem informacji emitowanych w językach UE, dostawę usług lub produktów w państwach UE, dostępność usług uzależnionych od wykorzystania karty kredytowej UE, przesyłanie materiałów reklamowych w języku użytkownika lub dotyczących produktów i usług dostępnych w UE. Grupa Robocza odnotowuje, że kryterium to jest już wykorzystywane w obszarze ochrony konsumenta: jego zastosowanie w kontekście ochrony danych wiązałoby się z dodatkową pewnością prawa dla administratorów danych, musieliby oni bowiem stosować to samo kryterium w odniesieniu do działań, które często powodują zastosowanie przepisów dotyczących ochrony zarówno konsumentów jak i danych.

- Kryterium wyposażenia/środków: jak się okazało, kryterium to powoduje niepożądane konsekwencje, takie jak ewentualne uniwersalne stosowanie przepisów UE. Niemniej jednak istnieje potrzeba zapobiegania sytuacjom, w których luka prawna pozwoliłaby na wykorzystanie terytorium UE jako „bezpiecznej przystani” dla przechowywania danych, na przykład gdy

działanie polegające na przetwarzaniu wiąże się z niedopuszczalnymi z etycznego punktu widzenia treściami. Kryterium wyposażenia/środków mogłoby zostać zatem zachowane, w perspektywie praw podstawowych oraz w formie szczątkowej. Kryterium to byłoby stosowane dopiero w trzeciej kolejności, gdy dwie pozostałe dwie możliwości nie mają zastosowania: dotyczyłoby ono przypadków granicznych (dane dotyczące osób niepochodzących z UE, administratorzy danych nieposiadający powiązania z UE), gdy na terytorium UE istnieje istotna infrastruktura, powiązana z przetwarzaniem informacji. W tym drugim przypadku, opcją mogłoby być założenie, że zastosowanie mają jedynie określone przepisy o ochronie danych – takie jak dotyczące legalności czy środków bezpieczeństwa. Takie podejście, które powinno zostać oczywiście dodatkowo uzupełnione i dopracowane, prawdopodobnie rozwiązałoby większość problemów, występujących obecnie w związku z zastosowaniem art. 4 ust. 1 lit. c).

f. Jako ostatnie zalecenie, Grupa Robocza wzywa do większej harmonizacji w zakresie nałożenia na administratorów danych posiadających siedzibę w państwach trzecich obowiązku określenia przedstawiciela w UE, tak aby rola przedstawiciela wiązała się z większą skutecznością. W szczególności, wyjaśnić należy zakres, w jakim osoby, których dane dotyczą mają możliwość skutecznego dochodzenia swoich praw wobec przedstawiciela.

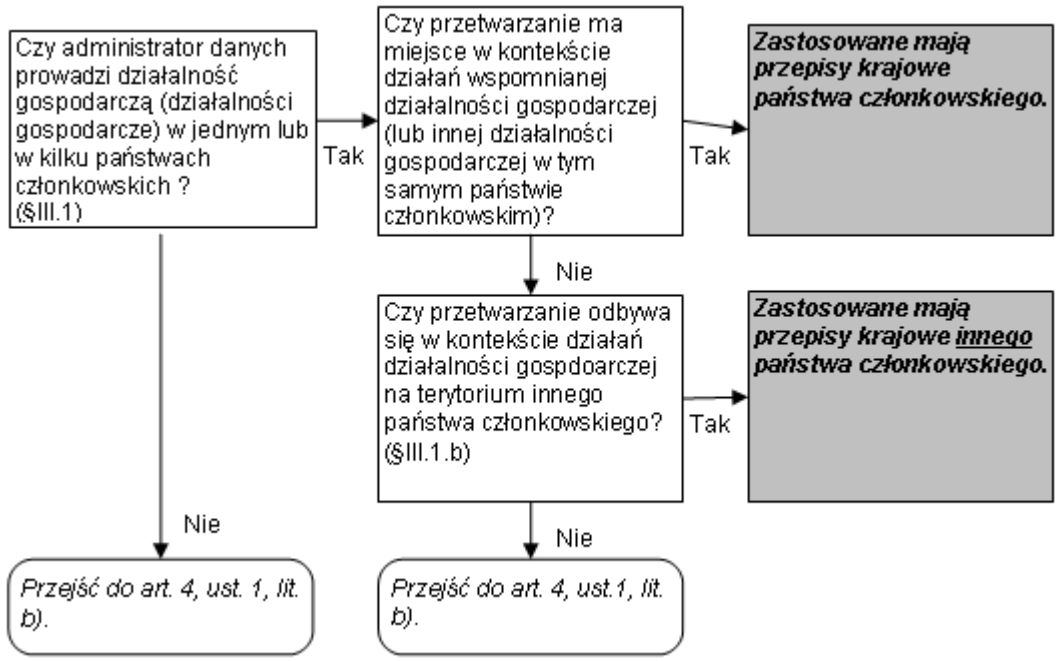
Bruksela, dnia 16 grudnia 2010 r.

W imieniu Grupy Roboczej,

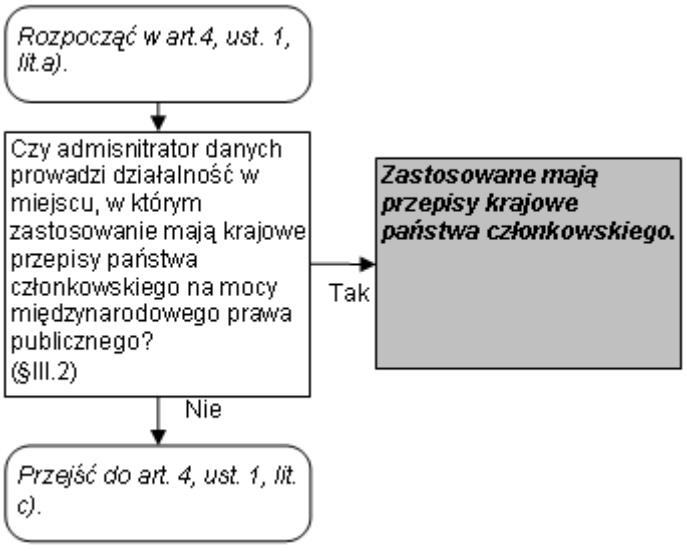
Przewodniczący
Jacob KOHNSTAMM

ZAŁĄCZNIK

Artykuł 4 ust. 1 lit. a)



Artykuł 4 ust. 1 lit. b)



Artykuł 4 ust. 1 lit. c)