32000D0520



# DECYZJA KOMISJI
## z dnia 26 lipca 2000 r.
## przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA

*(notyfikowana jako dokument nr C(2000) 2441)*

**(Tekst mający znaczenie dla EOG)**

(2000/520/WE)

KOMISJA WSPÓLNOT EUROPEJSKICH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych [1], w szczególności jej art. 25 ust. 6,

a także mając na uwadze, co następuje:

(1) Na mocy dyrektywy 95/46/WE Państwa Członkowskie są zobowiązane zapewnić, że przekazywanie danych osobowych do państwa trzeciego może odbywać się tylko wtedy, gdy dane państwo trzecie zapewnia adekwatny poziom bezpieczeństwa, a prawa Państwa Członkowskiego wprowadzające w życie inne przepisy dyrektywy są przestrzegane przed przekazaniem danych.

(2) Komisja może stwierdzić, że państwo trzecie zapewnia adekwatny poziom bezpieczeństwa. W tym przypadku dane osobowe mogą być przekazywane z Państw Członkowskich bez konieczności dodatkowych gwarancji.

(3) Na mocy dyrektywy 95/46/WE poziom ochrony danych powinien zostać oceniony w świetle wszystkich okoliczności związanych z operacją przekazywania danych albo zespołem operacji przekazywania danych oraz w odniesieniu do danych warunków. Grupa robocza ds. ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych powołana na podstawie wspomnianej dyrektywy [2] wydała wytyczne na temat dokonywania takich ocen [3].

(4) Biorąc pod uwagę różne podejścia do problemu ochrony danych w państwach trzecich, ocena adekwatności i każda decyzja na podstawie art. 25 ust. 6 dyrektywy 95/46/WE powinna być wprowadzona w życie w taki sposób, który ani nie dokonuje dyskryminacji w sposób arbitralny lub nieusprawiedliwiony wobec państw trzecich lub między tymi państwami, w których panują podobne warunki, ani też nie stwarza ukrytych barier w handlu uwzględniając obecne zobowiązania międzynarodowe Wspólnoty.

(5) Adekwatny poziom ochrony przekazywania danych ze Wspólnoty do Stanów Zjednoczonych, uznany przez niniejszą decyzję, powinien zostać osiągnięty, jeżeli organizacje będą przestrzegać zasad ochrony prywatności w ramach „bezpiecznej przystani" dotyczących ochrony danych osobowych przekazywanych z Państwa Członkowskiego do Stanów Zjednoczonych (zwanych dalej „zasadami") i najczęściej zadawanych pytań (zwanych dalej „NZP"), zawierających wytyczne dotyczące wprowadzania w życie zasad wydanych przez Rząd Stanów Zjednoczonych w dniu 21 lipca 2000 r. Ponadto organizacje powinny publicznie ujawnić stosowane przez nie polityki ochrony prywatności, a także powinny zostać poddane bądź to właściwości (Federalnej Komisji Handlu (FKH)) na podstawie sekcji 5 Ustawy o Federalnej Komisji Handlu, która zakazuje nieuczciwych lub wprowadzających w błąd czynów bądź praktyk handlowych lub wpływających na handel, bądź innego ustawowego organu, który skutecznie zapewni przestrzeganie zasad wdrożonych zgodnie z NZP.

(6) Z zakresu niniejszej decyzji powinny być wyłączone sektory i/lub przetwarzanie danych niepodlegające właściwości żadnego spośród organów rządowych w Stanach Zjednoczonych, wymienionych w załączniku VII do niniejszej decyzji.

(7) W celu zapewnienia prawidłowego stosowania niniejszej decyzji konieczne jest, żeby organizacje przestrzegające zasad i NZP mogły być uznane przez strony zainteresowane, takie jak osoby, których dane dotyczą, eksporterzy danych i organy ochrony danych. W tym celu Departament Handlu USA albo osoba przez niego

---

[1] Dz.U. L 281 z 23.11.1995, str. 31.

[2] Adres internetowy grupy roboczej: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

[3] GR 12: Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE w sprawie ochrony danych, przyjętej przez grupę roboczą dnia 24 lipca 1998 r.

wyznaczonapowinna podjąć się prowadzenia i publicznego udostępniania wykazu organizacji deklarujących przestrzeganie zasad wdrożonych zgodnie z NZP oraz podlegających właściwości, co najmniej jednego organu rządowego wymienionego w załączniku VII do niniejszej decyzji.

(8) Dla zachowania przejrzystości i w celu zagwarantowania właściwym władzom w Państwach Członkowskich możliwości zapewnienia ochrony osób fizycznych w zakresie przetwarzania ich danych osobowych, konieczne jest wyszczególnienie w niniejszej decyzji okoliczności wyjątkowych, w których zawieszenie określonych przekazów danych powinno być usprawiedliwione, bez względu na to czy stwierdzono ich właściwą ochronę.

(9) W świetle doświadczenia oraz nowych rozwiązań dotyczących ochrony prywatności w okolicznościach, w których technika umożliwia coraz łatwiejsze przekazywanie i przetwarzanie danych osobowych, a także w świetle sprawozdań w sprawie wprowadzenia w życie sporządzonych przez zaangażowane władze wykonawcze, może zajść potrzeba dokonania przeglądu „bezpiecznej przystani" tworzonej przez zasady i NZP.

(10) Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, powołana na mocy art. 29 dyrektywy 95/46/WE, wydała opinie o poziomie bezpieczeństwa, jaką zapewniają zasady „bezpiecznej przystani" w Stanach Zjednoczonych, które zostały uwzględnione przy przygotowaniu niniejszej decyzji [1].

(11) Środki przewidziane w niniejszej decyzji są zgodne z opinią Komitetu powołanego na mocy art. 31 dyrektywy 95/46/WE.

(12) Zgodnie z decyzją Komisji nr 1999/468/WE, w szczególności jej art. 8, w dniu 5 lipca 2000 r. Parlament Europejski przyjął rezolucję nr A5–0177/2000 w sprawie projektu decyzji Komisji w sprawie adekwatności ochrony przyznanej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" i związanymi z nią najczęściej zadawanymi pytaniami wydany przez Departament Handlu USA [2]. Komisja ponownie zbadała projekt decyzji w świetle tej rezolucji i stwierdziła, że pomimo, iż Parlament Europejski wyraził pogląd, że należy dokonać pewnych ulepszeń w zasadach „bezpiecznej przystani" i odnośnych NZP zanim uzna się, że zapewniają adekwatną ochronę, nie ustanowił on, że Komisja przekroczyłaby swoje uprawnienia przyjmując tę decyzję,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

*Artykuł 1*

1. Do celów art. 25 ust. 2 dyrektywy 95/46/WE, w odniesieniu do wszystkich działań wchodzących w zakres niniejszej dyrektywy przyjmuje się, że zasady ochrony prywatności w ramach „bezpiecznej przystani" (zwane dalej „zasadami"), jak określono w załączniku I do niniejszej decyzji, wprowadzane w życie zgodnie z wytycznymi zawartymi w najczęściej zadawanych pytaniach (zwanych dalej NZP) wydanych przez Departament Handlu USA w dniu 21 lipca 2000 r., jak określono w załączniku II do niniejszej decyzji, zapewniają adekwatny poziom ochrony danych osobowych przekazywanych ze Wspólnoty do organizacji mających siedzibę w Stanach Zjednoczonych, z uwzględnieniem następujących dokumentów wydanych przez Departament Handlu USA:

a) przegląd egzekwowania „bezpiecznej przystani", przedstawiony w załączniku III;

b) memorandum w sprawie odszkodowań z tytułu naruszenia prywatności i wyraźnych upoważnień w prawie amerykańskim, przedstawione w załączniku IV;

c) list Federalnej Komisji Handlu, przedstawiony w załączniku V;

d) list Departamentu Transportu USA, przedstawiony w załączniku VI.

2. W stosunku do każdego przekazu danych powinny zostać spełnione następujące warunki:

a) organizacja otrzymująca dane jednoznacznie i publicznie ujawniła swoje zobowiązanie przestrzegania zasad wdrożonych zgodnie z NZP; oraz

b) organizacja podlega ustawowym uprawnieniom organu rządowego Stanów Zjednoczonych wymienionego w załączniku VII do niniejszej decyzji, który w przypadku nieprzestrzegania zasad wdrożonych przy pomocy NZP jest upoważniony do badania skarg i uwalniania od nieuczciwych lub wprowadzających w błąd praktyk oraz uzyskiwania odszkodowania dla osób fizycznych, niezależnie od ich kraju zamieszkania bądź przynależności państwowej.

3. Przyjmuje się, że warunki określone w ust. 2 spełnia każda organizacja, która deklaruje przestrzeganie zasad wdrożonych zgodnie z NZP od dnia, w którym ta organizacja zawiadomi Departament Handlu USA (albo osobę przez niego wyznaczoną) o publicznym ujawnieniu zobowiązania określonego w ust. 2 lit. a) oraz danych organu rządowego, określonego w ust. 2 lit. b).

---

[1] GR 15: Opinia 1/99 dotycząca poziomu ochrony danych w Stanach Zjednoczonych i bieżących rozmów pomiędzy Komisją Europejską a Stanami Zjednoczonymi.
GR 19: Opinia 2/99 w sprawie adekwatności „międzynarodowych zasad bezpiecznejprzystani" wydanych przez Departament Handlu USA dnia 19 kwietnia 1999 r.
GR 21: Opinia 4/99 w sprawie najczęściej zadawanych pytań, które mają zostać wydane przez Departament Handlu USA w odniesieniu do proponowanych „zasad bezpiecznej przystani" w sprawie adekwatności „międzynarodowych zasad bezpiecznej przystani".
GR 23: Dokument roboczy w sprawie aktualnego stanu trwających rozmów pomiędzy Komisją Europejską a rządem Stanów Zjednoczonych dotyczących „międzynarodowych zasad bezpiecznej przystani".
GR 27: Opinia 7/99 w sprawie poziomu ochrony danych zapewnianego przez zasady „bezpiecznej przystani" opublikowane łącznie z „najczęściej zadawanymi pytaniami" (NZP) i innymi odnośnymi dokumentami w dniach 15 i 16 listopada 1999 r. przez Departament Handlu USA.
GR 31: Opinia 3/200 w sprawie dialogu/USA dotyczącego umowy „bezpiecznej przystani".
GR 32: Opinia 4/2000 w sprawie poziomu ochrony zapewnianego przez „zasady bezpiecznej przystani".

[2] Rezolucja dotychczas nieopublikowana w Dzienniku Urzędowym.

*Artykuł 2*

Niniejsza decyzja dotyczy jedynie adekwatności ochrony zapewnianej w Stanach Zjednoczonych na mocy zasadwdrożonych zgodnie z NZP w celu spełnienia wymagań art. 25 ust. 1 dyrektywy 95/46/WE i nie wpływa na stosowanie innych przepisów tej dyrektywy, które dotyczą przetwarzania danych osobowych w Państwach Członkowskich, w szczególności jej art. 4.

*Artykuł 3*

1. Bez uszczerbku dla ich uprawnień do podejmowania działania zmierzającego do zapewnienia zgodności z przepisami krajowymi przyjętymi na mocy przepisów innych niż art. 25 dyrektywy 95/46/WE, właściwe władze Państw Członkowskich mogą wykonywać posiadane uprawnienia w celu zawieszenia przepływu danych do organizacji, która złożyła zaświadczenie o przestrzeganiu zasad wdrożonych zgodnie z NZP, w celu ochrony osób fizycznych w odniesieniu do przetwarzania ich danych osobowych w przypadkach, gdy:

a) organ rządowy w Stanach Zjednoczonych, określony w załączniku VII do niniejszej decyzji lub mechanizm niezależnej ochrony prawnej w rozumieniu lit. a) Zasady Realizacji Prawa określonej w załączniku I do niniejszej decyzji ustali, że organizacja narusza zasady wdrożone zgodnie z NZP; lub

b) istnieje duże prawdopodobieństwo, że zasady są łamane; istnieje uzasadnione domniemanie, że mechanizm realizacji prawa o którym mowa nie podejmuje lub nie podejmie właściwych kroków w odpowiednim czasie w celu załatwienia spornej sprawy; dalszy przekaz tworzyłby bezpośrednie ryzyko wystąpienia poważnej szkody dla osób, których dane dotyczą; a właściwe władze Państwa Członkowskiego dołożyły należytych starań w tych okolicznościach w celu powiadomienia danej organizacji i umożliwienia udzielenia odpowiedzi.

Zawieszenie ustaje z chwilą, gdy zostanie zapewnione przestrzeganie zasad wdrożonych zgodnie z NZP oraz właściwe władze Wspólnoty zostaną o tym powiadomione.

2. Państwa Członkowskie bezzwłocznie powiadomią Komisję o przyjęciu środków na podstawie ust. 1.

3. Państwa Członkowskie i Komisja powiadomią się także o przypadkach, w których działanie organów odpowiedzialnych za zapewnienie przestrzegania zasad wdrożonych zgodnie z NZP w Stanach Zjednoczonych nie zapewnia ich przestrzegania.

4. Jeżeli informacje zebrane zgodnie z ust. 1, 2 i 3 dostarczą dowodów, że jakikolwiek organ odpowiedzialny za zapewnienie przestrzegania zasad wdrożonych zgodnie z NZP w Stanach Zjednoczonych nie spełnia skutecznie swojej roli, Komisja informuje o tym Departament Handlu USA oraz, w razie potrzeby, przedstawia projekt środków zgodnie z procedurą, określoną w art. 31 dyrektywy 95/46/WE, w celu uchylenia albo zawieszenia niniejszej decyzji lub też ograniczenia jej zakresu.

*Artykuł 4*

1. Niniejsza decyzja może być dostosowywana w dowolnym czasie w świetle doświadczenia uzyskanego podczas wprowadzania jej w życie i/lub, jeżeli wymagania ustawodawstwa USA będą wyższe niż poziom bezpieczeństwa zapewniany przez zasad *y* i NZP.

W każdym przypadku, Komisja oceni wprowadzanie w życie niniejszej decyzji na podstawie dostępnych informacji trzy lata od jej notyfikowania Państwom Członkowskim i złoży sprawozdanie na temat wszelkich stosownych ustaleń komitetowi, ustanowionemu na podstawie art. 31 dyrektywy 95/46/WE, łącznie z wszelkimi dowodami, które mogą wpływać na ocenę przepisów określonych w art. 1 niniejszej decyzji w odniesieniu do zapewniania przez nie właściwej ochrony w rozumieniu art. 25 dyrektywy 95/46/WE oraz wszelkimi dowodami na stosowanie praktyk dyskryminacyjnych przy wprowadzaniu w życie niniejszej decyzji.

2. Komisja, w miarę potrzeb, przedstawia projekt środków zgodnie z procedurą określoną w art. 31 dyrektywy 95/46/WE.

*Artykuł 5*

Państwa Członkowskie podejmą wszelkie niezbędne środki w celu zapewnienia zgodności z niniejszą decyzją najpóźniej do końca okresu 90 dni upływającego od dnia jej notyfikowania Państwom Członkowskim.

*Artykuł 6*

Niniejsza decyzja skierowana jest do Państw Członkowskich.

Sporządzono w Brukseli, dnia 26 lipca 2000 r.

*W imieniu Komisji*

Frederik BOLKESTEIN

*Członek Komisji*

*ZAŁĄCZNIK I*

## ZASADY OCHRONY PRYWATNOŚCI W RAMACH „BEZPIECZNEJ PRZYSTANI"

**wydane przez Departament Handlu USA dnia 21 lipca 2000 r.**

Ogólne prawodawstwo Unii Europejskiej dotyczące ochrony prywatności, dyrektywa w sprawie ochrony danych (zwana dalej dyrektywą), weszło w życie w dniu 25 października 1998 r. Wymaga ono, żeby dane osobowe były przekazywane wyłącznie do takich państw nienależących do Wspólnoty, które zapewniają „adekwatny" poziom ochrony prywatności. Chociaż Stany Zjednoczone i Unia Europejska dążą do tego samego celu, jakim jest podniesienie poziomu ochrony prywatności swoich obywateli, to Stany Zjednoczone mają inne podejście do prywatności niż Unia Europejska. Stany Zjednoczone stosują podejście sektorowe, które polega na połączeniu ustawodawstwa, regulacji i samoregulacji. Biorąc pod uwagę te różnice, wiele amerykańskich organizacji wyraża niepewność dotyczącą wpływu wymaganej przez UE „normy adekwatności" na przekazywanie danych z Unii Europejskiej do Stanów Zjednoczonych.

W celu zmniejszenia niepewności i stworzenia bardziej przewidywalnych ram dla przekazywania takich danych, Departament Handlu wydaje niniejszy dokument i najczęściej zadawane pytania (zwane dalej „zasadami") na mocy swych ustawowych uprawnień do ustanawiania, wspierania i rozwijania handlu międzynarodowego. Zasady zostały opracowane w konsultacji z kręgami przemysłowymi i publicznością w celu ułatwienia handlu między Stanami Zjednoczonymi a Unią Europejską. Są one przeznaczone do wyłącznego użytku przez amerykańskie organizacje otrzymujące dane osobowe z Unii Europejskiej, w celu zakwalifikowania ich jako „bezpiecznej przystani" i domniemania „adekwatności", jakie ta przystań stwarza. Ponieważ zasady miały służyć wyłącznie temu szczególnemu celowi, ich przyjęcie do innych celów może być niewłaściwe. Zasad nie można stosować zamiast krajowych przepisów wprowadzających w życie dyrektywę, które stosuje się do przetwarzania danych osobowych w Państwach Członkowskich.

Decyzje organizacji o zakwalifikowaniu się jako „bezpieczna przystań" są całkowicie dobrowolne i organizacje mogą kwalifikować się jako „bezpieczna przystań" w różny sposób. Organizacje, które zdecydują się przyjąć zasady muszą stosować zasady w celu uzyskania i utrzymania przywilejów płynących z zasad ochrony prywatności w ramach „bezpiecznej przystani" i publicznie oświadczyć, że tak postępują. Jeżeli na przykład dana organizacja przystąpi do programu samoregulacji ochrony prywatności, który przestrzega zasad, to kwalifikuje się ona jako „bezpieczna przystań". Organizacje mogą się też zakwalifikować poprzez rozwój swych własnych polityk samoregulacji przestrzegania ochrony prywatności pod warunkiem że będą one zgodne z zasadami. W przypadku gdy dla zachowania zgodności z zasadami organizacja polega całkowicie albo częściowo na samoregulacji, nieprzestrzeganie przez nią takiej samoregulacji musi także być zaskarżalne na podstawie sekcji 5 Ustawy o Federalnej Komisji Handlu zakazującej nieuczciwych lub wprowadzających w błąd czynów, lub na podstawie innych przepisów ustawowych lub wykonawczych zabraniających takich czynów. (Spis ustawowych organów USA uznawanych przez UE podano w Załączniku). Ponadto, organizacje podlegające ustawowemu, wykonawczemu, administracyjnemu lub innemu zbiorowi praw (lub przepisów) chroniącemu skutecznie prywatność osób fizycznych mogą się także kwalifikować do korzystania z przywilejów „bezpiecznej przystani". We wszystkich przypadkach, przywileje „bezpiecznej przystani" przysługują od dnia, w którym każda organizacja pragnąca zakwalifikować się jako „bezpieczna przystań" przedstawia swój certyfikat w Departamencie Handlu (albo osobie przez niego wyznaczonej) przestrzegania zasad zgodnie ze wskazówkami podanymi w najczęściej zadawanych pytaniach dotyczących samocertyfikacji.

Przyjęcie zasad może być ograniczone: a) w zakresie niezbędnym do spełnienia wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa; b) ustawą, rozporządzeniem rządu albo prawem precedensowym, ustanawiającym sprzeczne obowiązki albo udzielającym wyraźnego upoważnienia, pod warunkiem że działając na mocy tego upoważnienia organizacja potrafi wykazać, że nieprzestrzeganie przez nią zasad jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych uzasadnionych interesów wspieranych przez to upoważnienie; lub c) jeżeli efektem dyrektywy w prawie Państwa Członkowskiego jest dopuszczenie wyjątków lub odstępstw, pod warunkiem że takie wyjątki lub odstępstwa stosuje się w porównywalnych kontekstach. Zgodnie z celem zwiększenia ochrony prywatności, organizacje powinny dążyć do pełnego wdrożenia niniejszych zasad w sposób całkowity i przejrzysty, wskazując ponadto w swoich politykach ochrony prywatności przypadki, w których wyjątki od zasad dozwolone lit. b) powyżej będą stosowane na bieżąco. Z tego samego powodu w przypadku gdy zasady i/lub prawo amerykańskie dopuszcza taką możliwość, oczekuje się, że w miarę możliwości organizacje będą decydować się na wyższy poziom ochrony.

Ze względów praktycznych lub innych organizacje mogą życzyć sobie, aby stosować zasady w odniesieniu do wszystkich operacji przetwarzania danych przez nie przeprowadzanych, lecz zobowiązane są stosować zasady tylko do danych przekazanych po ich wejściu do „bezpiecznej przystani". W celu zakwalifikowania się jako „bezpieczna przystań", podmioty nie mają obowiązku stosowania niniejszych zasad do informacji osobowych zawartych w ręcznie przetwarzanych systemach ewidencji. Organizacje pragnące korzystać z „bezpiecznej przystani" wcelu

otrzymywania informacji z ręcznie przetwarzanych systemów ewidencji w UE muszą stosować zasady do wszystkich takich informacji przekazywanych po ich wejściu do „bezpiecznej przystani". Organizacja, która chce rozszerzyć przywilej „bezpiecznej przystani" na informacje osobowe o zasobach ludzkich, przekazywane z UE w celu wykorzystania w związku ze stosunkiem pracy musi to zaznaczyć, kiedy przedstawia swój certyfikat w Departamencie Handlu (albo osobie przez niego wyznaczonej) i spełnić wymagania podane w najczęściej zadawanych pytaniach dotyczących samocertyfikacji. Organizacje będą też mogły wprowadzić środki bezpieczeństwa wymagane na podstawie art. 26 dyrektywy, jeżeli włączą zasady do pisemnych umów ze stronami przekazującymi dane z UE w celu ustanowienia zasadniczych przepisów dotyczących ochrony prywatności z chwilą, gdy pozostałe przepisy takich wzorcowych umów zostaną zatwierdzone przez Komisję i Państwa Członkowskie.

Prawo USA będzie miało zastosowanie do pytań związanych z wykładnią i przestrzeganiem zasad „bezpiecznej przystani" (łącznie z najczęściej zadawanymi pytaniami) oraz stosownych polityk ochrony prywatności przez organizacje „bezpiecznej przystani", z wyjątkiem przypadków, gdy organizacje zobowiązały się współpracować z europejskimi organami ochrony danych. O ile nie stwierdzono inaczej, wszystkie przepisy zasad „bezpiecznej przystani" i najczęściej zadawanych pytań stosuje się we wszystkich przypadkach, których one dotyczą.

„Dane osobowe" i „informacje osobowe" są to dane o zidentyfikowanej albo możliwej do zidentyfikowania osobie, wchodzące w zakres dyrektywy, otrzymane przez organizację amerykańską z Unii Europejskiej i zarejestrowane w dowolnej formie.

## OGŁOSZENIE

Organizacja musi poinformować osoby o celach, w jakich zbiera i wykorzystuje informacje o nich, o sposobie kontaktowania się z organizacją w celu zasięgnięcia informacji albo złożenia skargi, o rodzajach stron trzecich, którym ujawnia te informacje, oraz o możliwościach wyboru i środkach ograniczenia korzystania i ujawnienia tych informacji, oferowanych przez organizację tym osobom. Ogłoszenie to musi być sformułowane jasno i jednoznacznie z chwilą, gdy osoby fizyczne są po raz pierwszy proszone o dostarczenie organizacji informacji osobowych lub też w jak krótszym terminie jak to możliwe, ale w każdym przypadku przed użyciem przez organizację takich informacji w celu innym niż ten, w którym były one pierwotnie zbierane albo przetwarzane przez organizację przekazującą lub zanim ujawni je po raz pierwszy stronie trzeciej ([1]).

## WYBÓR

Organizacja musi dać osobom możliwość wyboru (wyrażenie sprzeciwu), czy informacje osobowe ich dotyczące mają: a) być ujawnione stronie trzeciej ([1]) lub b) być wykorzystane w celu niezgodnym z celem(-ami), dla którego(-ych) były pierwotnie zbierane, lub na które osoba fizyczna wyraziła później zgodę. Procedury wyboru udostępnione osobom fizycznym muszą być jasne i jednoznaczne, łatwo dostępne i cenowo przystępne.

W przypadku informacji wrażliwych (tj. informacji osobowych określających warunki leczenia lub stan zdrowia, pochodzenie rasowe lub etniczne, przekonania polityczne, wierzenia religijne lub poglądy filozoficzne, członkostwo w związkach zawodowych, albo informacji określających życie seksualne danej osoby), muszą one mieć możliwość twierdzącego lub wyraźnego wyboru (wyrażenie zgody), jeżeli informacje mają być ujawnione stronie trzeciej lub mają być użyte w celu innym niż cele, dla których były pierwotnie zbierane, lub do których wykorzystania zainteresowana osoba później upoważniła poprzez wykorzystanie możliwości wyrażenia zgody. W każdym przypadku organizacja powinna traktować jako informację wrażliwą każdą informację otrzymaną od strony trzeciej, w przypadku gdy strona trzecia określa i traktuje je jako wrażliwe.

## DALSZE PRZEKAZYWANIE DANYCH

W celu ujawnienia informacji stronie trzeciej, organizacje muszą stosować zasady ogłoszenia i wyboru. W przypadku gdy organizacja chce przesłać informację stronie trzeciej, będącej przedstawicielem, jak opisano w przypisie końcowym, może to zrobić pod warunkiem uprzedniego upewnienia się, iż strona trzecia przystąpiła do zasad albo podlega dyrektywie albo ustaleniom dotyczącym adekwatności lub zawrze z taką stroną trzecią pisemną umowę wymagającą, aby strona trzecia zapewniła, co najmniej taki sam poziom ochrony prywatności, jaki jest wymagany przez odnośne zasady. Jeżeli organizacja będzie przestrzegać tych wymagań, to nie będzie ona ponosić odpowiedzialności (o ile organizacja nie postanowi inaczej) za to, że strona trzecia, do której przekazuje informacje, przetwarza je w sposób niezgodny z ograniczeniami albo oświadczeniami, chyba że organizacja ta wiedziała albo powinna była wiedzieć, że strona trzecia może przetwarzać dane w taki nieodpowiedni sposób i organizacja nie podjęła właściwych kroków, żeby zapobiec takiemu przetwarzaniu danych lub je powstrzymać.

([1]) Nie jest konieczne uprzedzanie ani oferowanie wyboru, gdy ujawnia się dane stronie trzeciej, która działa jako przedstawiciel powołany do wykonania zadania(-ń) w imieniu i na polecenie organizacji. Z drugiej strony, w takich przypadkach stosuje się zasadę dalszego przekazywania danych.

**BEZPIECZEŃSTWO**

Organizacje tworzące, przechowujące, używające albo rozpowszechniające informacje osobowe muszą podejmować rozsądne środki ostrożności w celu ich ochrony przed utratą, niewłaściwym wykorzystaniem oraz nieuprawnionym dostępem, ujawnieniem, zmianą i zniszczeniem.

**INTEGRALNOŚĆ DANYCH**

Zgodnie z zasadami, informacje osobowe muszą odpowiadać celom, do których mają być użyte. Organizacji nie wolno przetwarzać informacji osobowych w sposób niezgodny z celami, dla których były one zbierane lub celom, na które osoba udzieliła następnie zezwolenia. W zakresie niezbędnym do osiągnięcia tych celów, organizacja powinna podjąć właściwe kroki, aby zapewnić wiarygodność dla celów, jakim mają służyć, dokładność, kompletność i aktualność.

**DOSTĘP**

Osoby fizyczne muszą mieć dostęp do informacji osobowych ich dotyczących, które organizacja przechowuje i mieć możliwość poprawiania, zmieniania lub usuwania takich informacji, gdy są one nieprawidłowe, z wyjątkiem przypadków, gdy obciążenie kosztami udostępnienia informacji byłoby nieproporcjonalne w stosunku do zagrożenia dla ochrony prywatności danej osoby, lub w przypadku gdy prawa osób innych niż dana osoba zostałyby naruszone.

**ZAPEWNIANIE PRAWU SKUTECZNOŚCI**

Skuteczna ochrona prywatności musi obejmować procedury postępowania zapewniające przestrzeganie zasad, prawo odwoływania się osób, których dane dotyczą, które wskutek nieprzestrzegania zasad zostały poszkodowane, oraz konsekwencje wynikające dla organizacji z powodu nieprzestrzegania zasad. Procedury te muszą obejmować, co najmniej: a) łatwo dostępny i finansowo przystępny mechanizm niezależnej ochrony prawnej, dzięki któremu bada się i rozstrzyga skargi oraz spory poszczególnych osób w odniesieniu do zasad, a także przyznaje odszkodowania w przypadku gdy przewiduje to odnośne prawo lub inicjatywy sektora prywatnego; b) procedury kontrolne mające na celu sprawdzenie, że poświadczenia i zapewnienia dokonywane przez przedsiębiorstwa w odniesieniu do ich praktyk ochrony prywatności są prawdziwe oraz, że praktyki te zostały wdrożone zgodnie z deklaracjami; oraz c) obowiązki dotyczące zaradzenia problemom wynikającym z nieprzestrzegania zasad przez organizacje deklarujące ich przestrzeganie oraz konsekwencje dla organizacji. Sankcje muszą być dostatecznie surowe, by zapewnić przestrzeganie zasad przez organizacje.

*Załącznik*

**Wykaz ustawowych organów Stanów Zjednoczonych uznanych przez Unię Europejską**

Unia Europejska uznaje następujące organy rządowe Stanów Zjednoczonych za upoważnione do badania skarg i uwolnienia od nieuczciwych albo wprowadzających w błąd praktyk, a także uzyskiwania odszkodowania dla osób fizycznych w razie nieprzestrzegania zasad wprowadzonych w życie zgodnie z NZP:

— Federalna Komisja Handlu na podstawie uprawnień przyznanych jej na mocy sekcji 5 Ustawy o Federalnej Komisji Handlu,

— Departament Transportu na podstawie uprawnień przyznanych mu na mocy tytułu 49 sekcji 41712 Kodeksu Stanów Zjednoczonych.

*ZAŁĄCZNIK II*

NAJCZĘŚCIEJ ZADAWANE PYTANIA (NZP)

**NZP 1 — Dane wrażliwe**

P: *Czy w odniesieniu do danych wrażliwych organizacja zawsze musi zapewnić możliwość wyraźnego wyboru (wyrażenia zgody)?*

O: Nie, taka możliwość nie jest wymagana w przypadku gdy przetwarzanie danych jest: 1) w żywotnym interesie osoby, której dane dotyczą, lub innej osoby; 2) konieczne do ustalenia roszczeń prawnych lub obrony; 3) wymagane do zapewnienia opieki zdrowotnej lub dokonania diagnozy; 4) wykonywane w toku prawomocnych działań przez fundację, stowarzyszenie albo jakikolwiek podmiot typu non-profit prowadzący działalność polityczną, filozoficzną, religijną albo związkową, a także pod warunkiem że przetwarzanie danych dotyczy wyłącznie członków tego podmiotu albo osób mających z nim stały kontakt w związku z jego działalnością celową, a dane nie są ujawnione stronie trzeciej bez zgody osób, których te dane dotyczą; 5) konieczne w celu wykonywania zobowiązań organizacji w dziedzinie prawa pracy; lub 6) związane z danymi, które osoba w sposób oczywisty ujawnia publicznie.

**NZP 2 — Wyjątki dziennikarskie**

P: *Biorąc pod uwagę konstytucyjną ochronę wolności prasy w Stanach Zjednoczonych i wyłączenie spod dyrektywy materiałów dziennikarskich, czy zasady „bezpiecznej przystani" stosuje się do informacji gromadzonej, przechowywanej, albo rozpowszechnianej na potrzeby dziennikarstwa?*

O: W przypadku gdy prawa do wolnej prasy wyrażone w pierwszej poprawce do konstytucji Stanów Zjednoczonych kolidują z interesami ochrony prywatności, pierwsza poprawka musi regulować równoważenie tych interesów w odniesieniu do działań obywateli lub organizacji amerykańskich. Informacje osobowe zebrane w celu ich publikacji w prasie, radio lub telewizji albo w innej formie publicznego rozpowszechnienia materiału dziennikarskiego, niezależnie od tego, czy informacje te wykorzystano czy nie, a także informacje znajdujące się w uprzednio opublikowanym materiale rozpowszechnionym z archiwów środków masowego przekazu, nie podlegają wymaganiom zasad „bezpiecznej przystani".

**NZP 3 — Odpowiedzialność pośrednia**

P: *Czy dostawcy usług internetowych, operatorzy telekomunikacyjni lub inne organizacje podlegają odpowiedzialności w ramach zasad „bezpiecznej przystań" i, gdy w imieniu innej organizacji jedynie przekazują, kierują, przełączają lub przechowują w pamięci informacje, które mogą naruszać te zasady?*

O: Nie. Podobnie jak w przypadku samej dyrektywy, „bezpieczna przystań" nie powoduje odpowiedzialności pośredniej. W zakresie, w jakim organizacja działa jedynie jako kanał przekazywania danych przekazywanych przez strony trzecie i o ile nie decyduje ona o celach oraz sposobach przetwarzania tych danych osobowych, nie podlegałaby odpowiedzialności.

**NZP 4 — Bankowość inwestycyjna i kontrole**

P: *Działania audytorów i bankierów inwestycyjnych mogą obejmować przetwarzanie danych osobowych bez zgody lub wiedzy osoby, której dane dotyczą. W jakich okolicznościach jest to dozwolone przepisami zasad ogłoszenia, wyboru i dostępu?*

O: Bankierzy inwestycyjni lub audytorzy mogą przetwarzać informacje bez wiedzy osoby tylko w takim zakresie i przez taki okres, jaki jest konieczny do spełnienia wymagań ustawowych albo wymagań interesu publicznego oraz w innych okolicznościach, w których stosowanie niniejszych zasad naruszałoby uzasadnione interesy organizacji. Te uzasadnione interesy obejmują kontrolę przestrzegania przez przedsiębiorstwa ich obowiązków prawnych i uzasadnionych operacji księgowania, a także konieczność zachowania poufności w związku z ewentualnymi przejęciami, łączeniem się spółek, tworzeniem spółek joint venture albo innymi podobnymi transakcjami przeprowadzanymi przez bankierów inwestycyjnych lub audytorów.

**NZP 5 — Rola organów ochrony danych**

P: *W jaki sposób przedsiębiorstwa, które zobowiążą się współpracować z organami ochrony danych (OOD) Unii Europejskiej dokonają tych zobowiązań i jak będą one wykonywane?*

O: Zgodnie z zasadami „bezpiecznej przystani" organizacje amerykańskie otrzymujące dane osobowe z UE muszą zobowiązać się do stosowania skutecznych procedur dla zapewnienia przestrzegania zasad „bezpiecznej przystani". W szczególności, zgodnie z zasadą zapewniania prawu skuteczności, muszą one zapewnić a) mechanizm ochronny dla osób, których dane dotyczą, b) procedury kontrolne mające na celu sprawdzenie, że poświadczenia i zapewnienia przez nie dokonywane są prawdziwe, oraz c) zobowiązania zaradzenia problemom powstałym na skutek nieprzestrzegania zasad oraz konsekwencje dla takich organizacji. Organizacja może spełniać wymagania lit. a) i c) zasady zapewniania skuteczności prawa, jeżeli przestrzega wymagań niniejszych NZP w zakresie współpracy z OOD.

Organizacja może zobowiązać się do współpracy z OOD przez stwierdzenie w swoim certyfikacie w sprawie „bezpiecznej przystani" przedstawionym w Departamencie Handlu (patrz: NZP 6 dotyczące samocertyfikacji), że organizacja ta:

1. zamierza spełnić wymaganie podane w lit. a) i c) zasady zapewniania prawu skuteczności „bezpiecznej przystani" przez zobowiązuje się do współpracy z OOD;

2. będzie współpracowała z OOD przy badaniu i rozstrzyganiu skarg wniesionych na podstawie „bezpiecznej przystani" oraz

3. będzie postępować zgodnie z poradami udzielonymi przez OOD, w przypadkach, gdy OOD uzna, że organizacja powinna podjąć szczególne działania w celu przestrzegania zasad „bezpiecznej przystani", włącznie ze stosowaniem środków zaradczych albo odszkodowawczych na rzecz osób pokrzywdzonych przez każde nieprzestrzeganie zasad i dostarczy OOD pisemne potwierdzenie, iż takie działanie zostało podjęte.

Współpraca ze strony OOD będzie polegała na udzielaniu informacji i porad w następujący sposób:

— Porady OOD będą udzielane za pośrednictwem nieformalnej grupy OOD ustanowionej na poziomie Unii Europejskiej, która między innymi zapewni skoordynowane i spójne podejście.

— Grupa będzie udzielać porad zainteresowanym organizacjom amerykańskim w sprawie nierozstrzygniętych skarg osób fizycznych, dotyczących posługiwania się informacjami osobowymi, które zostały przekazane z UE w ramach „bezpiecznej przystani". Porady te będą miały na celu zapewnienie prawidłowego stosowania zasad „bezpiecznej przystani" i będą zawierać wszelkie środki zaradcze dla zainteresowanej(ych) osoby(ób), jakie OOD uznają za właściwe.

— Grupa będzie udzielać takich porad w odpowiedzi na odwołania zainteresowanych organizacji i/lub w odpowiedzi na skargi otrzymane bezpośrednio od osób fizycznych na organizacje, które zobowiązały się współpracować z OOD do celów „bezpiecznej przystani", jednocześnie zachęcając i w razie potrzeby pomagając takim osobom wykorzystać w pierwszej kolejności wewnętrzne procedury rozpatrywania skarg, które dana organizacja może oferować.

— Porady będą udzielone dopiero wtedy, gdy obie strony sporu miały należytą możliwość wypowiedzenia się i przedstawienia wszystkich dowodów zgodnie z własnym uznaniem. Grupa będzie starała się udzielić porad tak szybko jak niniejszy wymóg należytej procedury stanowi. Jako ogólną zasadę przyjmuje się, że grupa będzie starała się udzielić porady w ciągu 60 dni od otrzymania skargi lub odwołania, a w miarę możliwości wcześniej.

— Jeżeli grupa uzna to za stosowne, poda do publicznej wiadomości wyniki badania przedłożonych jej skarg.

— Udzielenie porad za pośrednictwem grupy nie będzie skutkowało powstaniem jakiejkolwiek odpowiedzialności ze strony grupy lub poszczególnych OOD.

Jak wspomniano powyżej, organizacje wybierające ten sposób rozstrzygania sporów muszą zobowiązać się do przestrzegania porad OOD. Jeżeli organizacja nie zastosuje się do porad w ciągu 25 dni od ich otrzymania i nie poda zadowalającego usprawiedliwienia takiego opóźnienia, to grupa zawiadamia ją o swoim zamiarze przedłożenia sprawy Federalnej Komisji Handlu albo innemu federalnemu lub stanowemu organowi USA posiadającemu ustawowe uprawnienia do podjęcia czynności zapewniających prawu skuteczność w przypadku wprowadzenia w błąd albo podania fałszywych informacji lub uznać, że porozumienie o współpracy zostało poważnie naruszone i w związku z powyższym musi zostać uznane za nieważne. W ostatnim przypadku, grupa poinformuje Departament Handlu (albo osobę przez niego wyznaczoną), w celu umożliwienia dokonania właściwej zmiany na liście uczestników „bezpiecznej przystani". Każdy przypadek niewypełnienia zobowiązania do współpracy z OOD, a także przypadki nieprzestrzegania zasad „bezpiecznej przystani" będą podlegały zaskarżeniu jako praktyka wprowadzająca w błąd na mocy sekcji 5 Ustawy o FKH albo innej podobnej ustawy.

Organizacje wybierające taką opcję będą musiały zapłacić roczną składkę przeznaczoną na sfinansowanie kosztów operacyjnych grupy i mogą zostać poproszone o pokrycie koniecznych wydatków związanych z tłumaczeniami wynikających z rozpatrywania przez grupę odwołań lub skarg przeciwko nim. Roczna składka nie przekroczy 500 USD, a w przypadku małych przedsiębiorstw będzie niższa.

Organizacje przystępujące do „bezpiecznej przystani" będą miały możliwość nawiązania współpracy z OOD przez okres trzech lat. Jeżeli liczba amerykańskich organizacji wybierających tę możliwość okaże się nadmierna, przed końcem tego okresu OOD ponownie rozpatrzą to ustalenie.

**NZP 6 — Samocertyfikacja**

P: *W jaki sposób organizacja może przedstawić certyfikat, że przystępuje do zasad „bezpiecznej przystani"?*

O: Przywileje „bezpiecznej przystani" przysługują od dnia, w którym organizacja przedstawia swój certyfikat w Departamencie Handlu (albo u osoby przez niego wyznaczonej), że będzie przestrzegać zasad zgodnie z instrukcjami podanymi poniżej.

W celu dokonania samocertyfikacji o przystąpienia do „bezpiecznej przystani" organizacje mogą dostarczyć do Departamentu Handlu (albo osoby przez niego wyznaczonej) list podpisany przez członka zarządu w imieniu organizacji, która przystępuje do „bezpiecznej przystani", zawierający, co najmniej następujące informacje:

1. nazwę organizacji, adres pocztowy, adres e-mail:, numery telefonu i faksu;

2. opis działalności organizacji w odniesieniu do informacji osobowych otrzymywanych z UE; oraz

3. opis obowiązującej w organizacji polityki ochrony prywatności w odniesieniu do takich informacji osobowych, obejmujący: a) gdzie polityka ochrony prywatności jest udostępniona do wglądu publicznego, b) jej data obowiązywania, c) biuro kontaktowe dla rozpatrywania skarg, wniosków o udzielenie dostępu i wszelkich innych zagadnień wynikających z uczestnictwa w „bezpiecznej przystani", d) określony organ ustawowy właściwy do rozpoznawania skarg przeciwko organizacji, dotyczących ewentualnych nieuczciwych lub wprowadzających w błąd praktyk oraz naruszenia przepisów ustawowych lub wykonawczych regulujących ochronę prywatności (wymieniony w Załączniku do zasad), e) nazwy wszelkich programów ochrony prywatności, których organizacja jest członkiem, f) metoda kontroli (np. wewnętrzna, przez stronę trzecią) [1] i g) mechanizm niezależnej ochrony prawnej, który umożliwia badanie nierozstrzygniętych skarg.

W przypadku gdy organizacja chce, aby jej przywileje „bezpiecznej przystani" obejmowały także informacje o zasobach ludzkich, przekazywanych z UE do wykorzystania w związku ze stosunkiem pracy, może tak uczynić w przypadku gdy istnieje ustawowy organ, wymieniony w Załączniku do zasad, właściwy do rozpoznawania skarg przeciwko organizacji wynikających z informacji o zasobach ludzkich, którą wymieniono w Załączniku do zasad. Ponadto organizacja musi zaznaczyć to w swoim piśmie i zobowiązać się do współpracy, gdzie stosownie, z zainteresowanym organem bądź organami UE zgodnie z NZP 9 i NZP 5 oraz że będzie postępować zgodnie z poradami otrzymanymi od takich organów.

Departament (albo wyznaczona przez niego osoba) będzie prowadzić wykaz wszystkich organizacji, które złożyły takie pisma, zapewniając sobie w ten sposób przywileje „bezpiecznej przystani" i będzie również aktualizować ten wykaz na podstawie corocznych pism i zawiadomień otrzymanych zgodnie z NZP 11. Takie listy samocertyfikujące powinny być składane nie rzadziej niż raz w roku. W przeciwnym przypadku organizacja zostanie wykreślona z wykazu i pozbawiona przywilejów „bezpiecznej przystani". Zarówno wykaz, jak i listy

[1] Patrz: NZP 7 w sprawie kontroli.

samocertyfikujące przedkładaneprzez organizacje będą podane do publicznej wiadomości. Wszystkie organizacje, które samocertyfikują o przystąpieniu do „bezpiecznej przystani" muszą także podać w opublikowanych przez siebie odnośnych oświadczeniach dotyczących polityki ochrony prywatności, że przystąpiły do zasad „bezpiecznej przystani".

Zobowiązanie do przystąpienia do zasad „bezpiecznej przystani" nie jest ograniczone czasowo w odniesieniu do danych otrzymanych w okresie, w którym organizacja korzysta z przywilejów „bezpiecznej przystani". Jej zobowiązanie oznacza, że będzie w dalszym ciągu stosować zasady w odniesieniu do takich danych, tak długo jak długo będzie je przechowywać, wykorzystywać, ujawniać, nawet jeżeli w późniejszym terminie z jakiegokolwiek powodu opuści „bezpieczną przystań".

Organizacja, która przestanie istnieć jako odrębna osoba prawna w wyniku łączenia się lub przejmowania przedsiębiorstw musi zawiadomić o tym z wyprzedzeniem Departament Handlu (albo osobę przez niego wyznaczoną). Zawiadomienie powinno także zawierać informację, czy podmiot przejmujący albo podmiot powstały w wyniku łączenia się przedsiębiorstw 1) będzie w dalszym ciągu związany zasadami „bezpiecznej przystani" na skutek działania prawa regulującego przejęcie bądź łączenie lub też 2) zamierza przedstawić certyfikat o przyjęciu przez siebie zasad „bezpiecznej przystani" bądź zastosuje inne środki ochrony, takie jak pisemną umowę, które zapewnią przyjęcie zasad „bezpiecznej przystani". W przypadku gdy ani pkt 1) ani 2), nie ma zastosowania wszelkie dane uzyskane w ramach „bezpiecznej przystani" muszą zostać bezzwłocznie usunięte.

Organizacja nie musi poddawać wszystkich danych osobowych zasadom „bezpiecznej przystani", ale musi poddać zasadom „bezpiecznej przystani" wszystkie dane osobowe otrzymane z UE po swoim przystąpieniu do „bezpiecznej przystani".

Każde podanie do publicznej wiadomości fałszywej informacji dotyczącej przyjęcia przez organizację zasad „bezpiecznej przystani" może podlegać zaskarżeniu przez Federalną Komisję Handlową albo inny odpowiedni organ rządowy. Podanie fałszywych informacji Departamentowi Handlu (albo osobie przez niego wyznaczonej) może podlegać wniesieniu powództwa na podstawie Ustawy o fałszywych oświadczeniach (18 U. S. C.§ 1001).

**NZP 7 — Kontrola**

P: *W jaki sposób organizacje zapewniają procedury kontrolne pozwalające sprawdzić, czy ich poświadczenia i zapewnienia dotyczące praktyk ochrony prywatności w ramach „bezpiecznej przystani" są prawdziwe, czy praktyki te zostały wprowadzone w życie tak, jak to zostało przedstawione i czy zgodnie z zasadami „bezpiecznej przystani"*?

O: W celu spełnienia wymagań kontrolnych zasady zapewniania prawu skuteczności organizacja może sprawdzać takie poświadczenia i zapewnienia albo na drodze samooceny albo zewnętrznych przeglądów zgodności z wymaganiami.

W ramach samooceny kontrola taka musiałaby wykazać, że opublikowana polityka ochrony prywatności danej organizacji, dotycząca informacji osobowych otrzymanych z UE jest właściwa, całościowa, umieszczona w wyraźnym miejscu, w pełni wprowadzona w życie i dostępna. Organizacja musiałaby także wykazać, że jej polityka ochrony prywatności jest zgodna z zasadami „bezpiecznej przystani"; że osoby fizyczne są informowane o wszelkich wewnętrznych niezależnych mechanizmach rozpatrywania skarg oraz niezależnych mechanizmach składania skarg; że stosuje ona odpowiednie procedury szkoleń pracowników we wprowadzaniu w życie polityki ochrony prywatności i karania pracowników w przypadku jej nieprzestrzegania; oraz że stosuje ona wewnętrzne procedury okresowego przeprowadzania przedmiotowych przeglądów zgodności z powyższym. Oświadczenie potwierdzające samoocenę powinno być podpisane przez członka zarządu lub innego upoważnionego przedstawiciela organizacji przynajmniej raz w roku i powinno być udostępnione na żądanie osobom fizycznym lub w kontekście badania lub skargi dotyczącej nieprzestrzegania zasad.

Organizacje powinny zachowywać swe dokumenty w sprawie wprowadzania w życie ich praktyk ochrony prywatności w ramach „bezpiecznej przystani" oraz udostępniać je na żądanie w kontekście badania lub skargi na nieprzestrzeganie zasad niezależnemu organowi odpowiedzialnemu za rozpatrywanie skarg bądź organowi właściwemu do badania nieuczciwych i wprowadzających w błąd praktyk.

W przypadku gdy organizacja wybrała zewnętrzny przegląd przestrzegania, taki przegląd musi wykazać, że polityka organizacji w zakresie ochrony prywatności dotycząca informacji osobowych otrzymanych z UE jest zgodna z zasadami „bezpiecznej przystani", zaś zasady są przestrzegane, a osoby informowane o procedurach wnoszenia skarg. Metody przeglądu mogą obejmować audyt bez ograniczeń, wyrywkowe przeglądy, używanie „przynęt" albo stosowanie narzędzi technicznych, gdy to jest odpowiednie. Oświadczenie potwierdzające przeprowadzenie z pozytywnym wynikiem zewnętrznego przegląduzgodnościpowinno być

podpisane przez osobę dokonującą przegląd, członka zarządu lub innego upoważnionego przedstawiciela organizacji przynajmniej raz w roku i powinno być udostępnione na żądanie osobom fizycznym lub w kontekście badania lub skargi dotyczącej nieprzestrzegania zasad.

**NZP 8 — Dostęp**

**Zasada dostępu:**

Osoby fizyczne muszą mieć dostęp do informacji osobowych, które ich dotyczą przechowywanych przez organizację oraz mieć możliwość poprawienia, zmiany lub usunięcia niedokładnych informacji z wyjątkiem przypadków, gdy obciążenie związane z kosztami lub udzieleniem dostępu byłoby nieproporcjonalne do zagrożenia ochrony prywatności danej osoby lub w przypadku gdy zostałyby naruszone prawa osób innych niż dana osoba.

1. P: *Czy prawo dostępu jest nieograniczone?*

1. O: Nie. Zgodnie z zasadami „bezpiecznej przystani" prawo dostępu ma fundamentalne znaczenie dla ochrony prywatności. W szczególności, pozwala ono osobom fizycznym na sprawdzenie poprawności przechowywanych o nich informacji. Niemniej jednak obowiązek zapewnienia przez organizację dostępu do informacji osobowych, jakie przechowuje ona o zainteresowanej osobie fizycznej, podlega zasadzie proporcjonalności lub zasadności i w pewnych przypadkach musi być ograniczony. Potwierdzają to uzasadnienia do Wytycznych OECD w sprawie ochrony prywatności z 1980 r., które jasno stwierdzają, że obowiązek udzielenia dostępu przez organizację nie jest nieograniczony. Nie wymaga on nadmiernie szczegółowego przeszukania nakazanego, na przykład, w wezwaniu sądowym, ani nie wymaga dostępu do informacji we wszystkich poszczególnych formach, w jakich może ona być przechowywana przez organizację.

Doświadczenie wykazało raczej, że odpowiadając na żądania dostępu zgłaszane przez osoby fizyczne, organizacje powinny mieć na uwadze przede wszystkim kwestię, która spowodowała zgłoszenie żądania. Jeżeli na przykład żądanie dostępu jest niejasne albo ma bardzo szeroki zakres, organizacja może porozumieć się z daną osobą, żeby lepiej zrozumieć jej powód żądania i zlokalizować właściwą informację. Organizacja może zapytać, z jaką częścią(częściami) jej struktury osoba miała do czynienia i/lub o charakter informacji (albo jej wykorzystania), która jest przedmiotem żądania dostępu. Jednakże osoby fizyczne nie muszą uzasadniać żądania dostępu do swoich własnych danych.

Koszt i obciążenia są istotnymi czynnikami i powinny być brane pod uwagę, ale nie rozstrzygają o tym, czy umożliwienie dostępu jest uzasadnione. Jeżeli na przykład informacja jest wykorzystywana do podejmowania decyzji, które w istotny sposób wpływają na życie osoby fizycznej (na przykład odmowa bądź przyznanie istotnych korzyści, takich jak ubezpieczenie, hipoteka lub praca), wówczas zgodnie z innymi przepisami niniejszych NZP organizacja musiałaby ujawnić te informacje, nawet gdyby to było stosunkowo kosztowne albo trudne do wykonania.

Jeżeli żądana informacja nie jest wrażliwa albo nie jest używana do podejmowania decyzji, które w istotny sposób wpłyną na osobę fizyczną (np. niewrażliwe dane marketingowe używane do ustalenia, czy danej osobie wysłać katalog), lecz jest łatwo dostępna i jej dostarczenie jest niedrogie, organizacja będzie musiała zapewnić dostęp do informacji o faktach przechowywanych na temat danej osoby. Informacja będąca przedmiotem zainteresowania mogłaby zawierać fakty uzyskane od danej osoby, fakty zebrane w trakcie dokonywania transakcji lub fakty dotyczące osoby fizycznej uzyskane od innych osób.

Zgodnie z fundamentalnym charakterem dostępu organizacje powinny zawsze w dobrej wierze starać się go zapewnić. W przypadku gdy na przykład niektóre informacje wymagają ochrony i mogą być łatwo oddzielone od innych informacji podlegających żądaniu dostępu, organizacja powinna odpowiednio przeredagować chronioną informację i udostępnić pozostałe informacje. Jeżeli organizacja zdecyduje, że należy odmówić dostępu w każdym określonym przypadku, to powinna ona osobie żądającej dostępu udzielić wyjaśnienia, dlaczego podjęła taką decyzję oraz poinformować o punkcie kontaktowym w razie dalszych zapytań.

2. P: *Co to jest poufna informacja handlowa i czy organizacje w celu jej ochrony mogą odmówić do niej dostępu?*

2. O: Poufna informacja handlowa (w rozumieniu „Federalnych zasad procedury" w sprawie odkrywania) jest informacją, w odniesieniu do której organizacja podjęła kroki w celu jej ochrony przed ujawnieniem w przypadku gdy ujawnienie byłoby pomocne dla konkurenta rynkowego. Informacją poufną może być określony program komputerowy używany przez organizację, na przykład program do komputerowego modelowania, albo szczegółowe dane na temat tego programu. W przypadku gdy poufna informacja handlowa może być oddzielona od innej informacji będącej przedmiotem żądaniadostępu, organizacja powinna

przeredagować poufną informację handlową i udostępnić
informację jawną. Organizacje mogą odmówić dostępu albo go ograniczyć w takim zakresie, w jakim udzielenie go ujawniłoby ich własne poufne informacje handlowe, jak zdefiniowano powyżej, na przykład klasyfikacje lub wnioski marketingowe wypracowane przez organizację, albo poufne informacje handlowe innych przedsiębiorstw, w przypadku gdy taka informacja jest przedmiotem umownego zobowiązania do poufności w okolicznościach, gdy takie zobowiązanie do poufności byłoby zwyczajowo podjęte lub nałożone.

3. P: *Czy zapewniając dostęp, organizacja może ujawnić osobom fizycznym jedynie informacje osobowe o nich pochodzące z jej baz danych czy też wymagany jest sam dostęp do takiej bazy?*

3. O: Dostęp można zapewnić w postaci ujawnienia danych osobie fizycznej przez organizację i nie wymaga to dostępu przez tę osobę fizyczną do samej bazy danych organizacji.

4. P: *Czy organizacja musi restrukturyzować swoje bazy danych, żeby móc zapewnić dostęp?*

4. O: Dostęp musi być zapewniony tylko w takim zakresie, w jakim organizacja przechowuje informację. Sama zasada dostępu nie stwarza obowiązku zachowania, przechowywania, reorganizacji bądź restrukturyzacji plików z informacjami osobowymi.

5. P: *W niniejszych odpowiedziach wyraźnie stwierdzono, że dostępu można odmówić w pewnych okolicznościach. W jakich innych okolicznościach organizacja może odmówić osobie fizycznej dostępu do informacji osobowych na jej temat?*

5. O: Takie okoliczności są ograniczone i każdy powód odmowy dostępu musi być szczególny. Organizacja może odmówić udzielenia dostępu do informacji w zakresie, w jakim ujawnienie prawdopodobnie kolidowałoby z ochroną ważnych, równoważnych interesów społecznych, takich jak bezpieczeństwo narodowe, obrona albo bezpieczeństwo publiczne. Ponadto dostępu można odmówić w przypadku gdy informacje osobowe przetwarzane są wyłącznie w celach naukowych albo statystycznych. Innymi powodami odmowy lub ograniczenia dostępu są:

a. ingerencja w wykonywanie lub przestrzeganie prawa łącznie z prewencją, dochodzeniem lub wykrywaniem wykroczeń albo prawem do uczciwego procesu;

b. ingerencja w prywatne podstawy roszczeń, łącznie z prewencją, dochodzeniem lub wykrywaniem roszczeń prawnych lub prawem do uczciwego procesu;

c. ujawnienie informacji osobowych odnoszących się do innej osoby bądź osób, w przypadku gdy takich odnośnych informacji nie da się przeredagować;

d. naruszenie prawnego albo innego zawodowego przywileju lub obowiązku;

e. naruszenie niezbędnej poufności przyszłych lub trwających negocjacji, takich jak negocjacje w sprawie przejęcia spółek notowanych na giełdzie;

f. uszczerbek dla badań bezpieczeństwa pracownika lub procedur rozpoznawania skarg;

g. uszczerbek dla poufności, która może być konieczna przez ograniczony okres czasu w związku z planami awansowania pracowników, reorganizacją przedsiębiorstwa; lub

h. uszczerbek dla poufności, która może być konieczna w związku z funkcjami kontrolnymi, nadzorczymi lub regulacyjnymi związanymi z należytym zarządzaniem gospodarką lub finansami; albo

i. inne okoliczności, w których ciężar lub koszt zapewnienia dostępu byłby niewspółmierny lub kiedy udzielenie dostępu powodowałoby naruszenie uzasadnionych praw lub interesów innych osób.

Ciężar wykazania, że zachodzą wyjątkowe okoliczności, spoczywa na organizacji powołującej się na nie (tak jak w normalnych okolicznościach). Jak stwierdzono powyżej, osobom należy podać powody odmowy lub ograniczenia dostępu oraz punkt kontaktowy w przypadku dalszych pytań.

6. P: *Czy organizacja może pobierać opłatę na pokrycie kosztów udzielenia dostępu?*

6. O: Tak. Wytyczne OECD uznają prawo organizacji do pobierania opłaty pod warunkiem że nie są one nadmierne. Tak, więc organizacje mogą pobierać uzasadnioną opłatę z tytułu udzielenia dostępu. Pobieranie opłaty może być korzystne w celu zniechęcania do zadawania powtarzających się i złośliwych pytań.

Organizacje, których działalność polega na sprzedaży publicznie dostępnych informacji, mogą zatem pobierać opłaty ustalone przez nie zwyczajowo przy udzielaniu odpowiedzi na żądania dostępu. Osoby mogą alternatywnie starać się o dostęp do swoich informacji w organizacji, która pierwotnie zebrała dane.

Dostępu nie można odmówić ze względu na koszty, jeżeli osoba fizyczna zgłasza gotowość ich pokrycia.

7. P: *Czy organizacja jest zobowiązana zapewnić dostęp do informacji osobowych uzyskanych z dokumentów urzędowych?*

7. O: Wyjaśnijmy najpierw, że dokumenty urzędowe są to dokumenty przechowywane przez agencje albo jednostki rządowe na dowolnym szczeblu, które są otwarte do konsultacji dla publiczności. Nie ma potrzeby stosowania zasady dostępu do takich informacji, o ile nie są one połączone z innymi informacjami osobowymi, z wyjątkiem przypadków, gdy niewielkie ilości informacji niepochodzących z dokumentów urzędowych są wykorzystywane do indeksowania albo porządkowania informacji pochodzących z dokumentów urzędowych. Należy jednak przestrzegać wszelkich warunków wglądu ustalonych przez właściwe organy. Jednakże w przypadkach, gdy informacje pochodzące z dokumentów urzędowych są połączone z informacjami niepochodzącymi z dokumentów urzędowych (innymi niż te szczegółowo określone powyżej), organizacja musi zapewnić dostęp do wszystkich tego rodzaju informacji zakładając, że nie podlegają one innym dopuszczalnym wyjątkom.

8. P: *Czy zasada dostępu musi być stosowana do powszechnie dostępnych informacji osobowych?*

8. O: Podobnie jak w przypadku informacji pochodzących z dokumentów urzędowych (patrz: P.7) nie ma potrzeby zapewniania dostępu do informacji, która są już powszechnie dostępne dla publiczności, o ile nie są one połączone z informacjami powszechnie niedostępnymi.

9. P: *Jak organizacja może się chronić przed powtarzającymi się lub złośliwymi żądaniami dostępu?*

9. O: Organizacja nie musi odpowiadać na takie żądania dostępu. Z tych powodów organizacje mogą pobierać uzasadnioną opłatę i mogą ustalać uzasadnione ograniczenia liczby żądań zgłaszanych przez poszczególne osoby fizyczne w danym okresie czasu, które zostaną zaspokojone. Ustanawiając takie ograniczenia organizacja powinna uwzględnić takie czynniki jak częstotliwość, z jaką informacje są aktualizowane, cel w jakim dane są wykorzystywane oraz charakter informacji.

10. P: *W jaki sposób organizacja może bronić się przed oszukańczymi żądaniami dostępu?*

10. O: Organizacja nie jest zobowiązana do zapewnienia dostępu, jeżeli nie otrzyma wystarczających informacji umożliwiających jej potwierdzenie tożsamości osoby zgłaszającej żądanie.

11. P: *Czy określono termin, w którym odpowiedzi na żądanie dostępu muszą zostać udzielone?*

11. O: Tak, organizacje powinny odpowiedzieć bez zbędnej zwłoki i w rozsądnym terminie. Jak podano w wyjaśnieniach do Wytycznych OECD w sprawie ochrony prywatności z 1980 r., wymaganie to może być spełnione na różne sposoby. Na przykład kontroler danych, który w regularnych odstępach czasu przekazuje informacje osobom, których dane dotyczą, może być zwolniony z obowiązku natychmiastowego odpowiadania na indywidualne żądania.

**NZP 9 — Zasoby ludzkie**

1. P: *Czy przekazywanie z UE do Stanów Zjednoczonych informacji osobowych zebranych w związku ze stosunkiem pracy jest objęte zasadami „bezpiecznej przystani"?*

1. O: Tak, w przypadkach, gdy informacje osobowe o pracownikach (byłych lub obecnych) zebrane w związku ze stosunkiem pracy, są przekazywane przez przedsiębiorstwo działające w UE do usługodawcy w Stanach Zjednoczonych, który będąc firmą matką, firmąpowiązaną lub nie powiązaną, uczestniczy

w „bezpiecznej przystani", wówczas przekazywanie jest objęte przywilejami „bezpiecznej przystani". W takich przypadkach zbieranie informacji i ich przetwarzanie przed przekazaniem będzie podlegało prawu krajowemu państwa UE, w którym dane zostały zebrane, a wszelkie warunki albo ograniczenia ich przekazywania będą musiały być przestrzegane zgodnie z tymi prawami.

Zasady „bezpiecznej przystani" mają zastosowanie jedynie wówczas, gdy przekazywane lub udostępniane są indywidualnie zidentyfikowane zapisy. Sprawozdawczość statystyczna opierająca się na zagregowanych danych zatrudnieniowych i/lub wykorzystaniu danych anonimowych lub pod postacią pseudonimów nie wiąże się z ochroną prywatności.

2. P: *W jaki sposób do takich informacji stosuje się zasady ogłoszenia i wyboru?*

2. O: Amerykańska organizacja, która w ramach „bezpiecznej przystani" otrzymała z UE informacje dotyczące pracowników, może ujawnić je stronom trzecim i/lub wykorzystać je do innych celów jedynie zgodnie z zasadami ogłoszenia i wyboru. W przypadku gdy na przykład dana organizacja zamierza wykorzystać informacje osobowe zebrane w związku ze stosunkiem pracy do celów nie związanych z zatrudnieniem, takich jak przekazywanie materiałów marketingowych, to zanim to zrobi, musi dać zainteresowanym osobom możliwość wyboru, chyba że osoby te już wcześniej wyraziły na zgodę na wykorzystanie informacji do takich celów. Ponadto, dokonywanie takiego wyboru nie może zostać wykorzystane do ograniczenia możliwości zatrudnienia albo wszczynania postępowania karnego wobec takich osób.

Należy zwrócić uwagę, że niektóre ogólnie stosowane warunki przekazywania danych z niektórych Państw Członkowskich mogą wykluczać odmienne wykorzystanie takich informacji nawet po ich przekazaniu poza terytorium UE i warunki te muszą być przestrzegane.

Ponadto pracodawcy muszą dołożyć należytych starań, w celu uwzględnienia preferencji pracowników dotyczących ochrony prywatności. Mogłoby to obejmować na przykład ograniczenie dostępu do danych, nadanie niektórym danym anonimowego charakteru albo nadanie kodów lub pseudonimów w przypadkach, kiedy w celu doraźnego zarządzania nie ma potrzeby posługiwania się rzeczywistymi imionami i nazwiskami.

W zakresie i w okresie czasu potrzebnym w celu uniknięcia naruszenia dla uzasadnionych interesów organizacji przy awansowaniu, mianowaniu lub dokonywaniu innych podobnych decyzji kadrowych, organizacja nie musi oferować ogłoszenia i wyboru.

3. P: *Jak stosuje się zasadę dostępu?*

3. O: NZP dotyczące dostępu zawierają wytyczne w sprawie przyczyn mogących usprawiedliwiać odmowę lub ograniczenie dostępu na żądanie dotyczące danych o zasobach ludzkich. Oczywiście pracodawcy w Unii Europejskiej muszą przestrzegać miejscowych przepisów i zapewnić pracownikom pochodzącym z państw UE dostęp do takich informacji zgodnie z wymogami prawa w ich państwach ojczystych niezależnie od miejsca przetwarzania i magazynowania danych. Zasada „bezpiecznej przystani" wymaga, żeby organizacja przetwarzająca takie dane w Stanach Zjednoczonych współpracowała w zapewnieniu takiego dostępu albo bezpośrednio albo za pośrednictwem unijnego pracodawcy.

4. P: *Jak zapewniana będzie prawu skuteczność w odniesieniu do danych o pracownikach objętych zasadami „bezpiecznej przystani"?*

4. O: W zakresie, w jakim informacja jest wykorzystywana wyłącznie w związku ze stosunkiem pracy, główna odpowiedzialność za dane o pracowniku spoczywa na przedsiębiorstwie w UE. Stąd w przypadkach, gdy europejscy pracownicy składają skargi na naruszenie ich praw do ochrony danych i nie są zadowoleni z wyników wewnętrznych przeglądów, skarg i procedur odwoławczych (lub wszelkich stosownych procedur rozpoznawania skarg na podstawie umowy ze związkiem zawodowym), należy ich skierować do państwowego lub krajowego organu ochrony danych albo organu ds. prawa pracy obejmującego swoją właściwością obszar, na którym pracownik jest zatrudniony. Obejmuje to także przypadki, gdy domniemane niewłaściwe traktowanie ich informacji osobowych miało miejsce w Stanach Zjednoczonych, za które odpowiedzialność spoczywa nie na pracodawcy, a na organizacji amerykańskiej, otrzymującej informacje od pracodawcy i w ten sposób stanowi domniemane naruszenie zasad „bezpiecznej przystani", a nie prawa krajowego wprowadzającego w życie dyrektywę. Będzie to najbardziej skuteczny sposób podejścia do często nakładających się na siebie praw i obowiązków nakładanych przez lokalne prawo pracy i układy zbiorowe, a także prawo o ochronie danych.

Jeżeli amerykańska organizacja uczestnicząca w „bezpiecznej przystani" i korzystająca z unijnych danych o zasobach ludzkich przekazywanych z Unii Europejskiej w związku ze stosunkiem pracy, życzy sobie, żeby przekazywanie takich danych odbywało się w ramach „bezpiecznej przystani", musi zobowiązać się do współpracy przy dochodzeniach prowadzonych w odnośnych sprawach przez właściwe władze UE oraz musi stosować się do ich wskazówek. OOD, które zgodziły się współpracować w ten sposób,zawiadomią o tym

Komisję Europejską i Departament Handlu. Jeżeli organizacja amerykańska uczestnicząca w „bezpiecznej przystani" chce przekazywać dane o zasobach ludzkich pracownikach z Państwa Członkowskiego, w którym OOD nie wyraziły na to zgody, stosuje się przepisy NZP 5.

**NZP 10 — Umowy na podstawie art. 17**

P: *Gdy dane są przekazywane z UE do Stanów Zjednoczonych tylko w celu przetwarzania, to czy wymagana jest umowa niezależnie od uczestnictwa podmiotu przetwarzającego w ramach „bezpiecznej przystani"?*

O: Tak. Od kontrolerów danych w Unii Europejskiej zawsze wymaga się zawarcia umowy, gdy dokonuje się przekazywania informacji jedynie w celu jej przetworzenia niezależnie od tego, czy przetwarzanie odbywa się na terytorium UE czy poza nim. Celem umowy jest ochrona interesów kontrolera danych, tj. osoby albo organu, który decyduje o celach i sposobach przetwarzania oraz ponosi pełną odpowiedzialność za te dane wobec zainteresowanej osoby bądź osób fizycznych. Tak, więc umowa określa rodzaj przetwarzania, które ma być wykonane oraz wszelkie środki niezbędne do zapewnienia, że dane przechowywane są w bezpieczny sposób.

Organizacja amerykańska, która uczestniczy w „bezpiecznej przystani" i otrzymuje informacje osobowe z UE jedynie w celu przetwarzania, nie musi stosować zasad do tych informacji, ponieważ kontroler w UE pozostaje bezpośrednio za nie odpowiedzialny wobec zainteresowanej osoby zgodnie z odnośnymi unijnymi przepisami, (które mogą być bardziej rygorystyczne niż odpowiadające im zasady „bezpiecznej przystani").

Ponieważ właściwą ochronę zapewniają uczestnicy „bezpiecznej przystani", umowy z uczestnikami „bezpiecznej przystani" o zwykłe przetwarzanie danych nie wymagają uprzedniego zezwolenia (albo zezwolenie takie zostanie udzielone przez Państwa Członkowskie automatycznie), jakie byłoby wymagane w przypadku umów z odbiorcami nie uczestniczącymi w „bezpiecznej przystani" lub nie zapewniającymi właściwej ochrony w inny sposób.

**NZP 11 — Rozstrzyganie sporów i zapewnianie prawu skuteczności**

P: *W jaki sposób powinny być wprowadzane w życie wymagania zasady zapewniania prawu skuteczności dotyczące rozstrzygania sporów i jak będzie traktowane uporczywe nieprzestrzeganie zasad przez organizację?*

O: Zasada zapewniania prawu skuteczności ustanawia wymagania dotyczące egzekwowania zasad „bezpiecznej przystani". W NZP dotyczącym kontroli (NZP 7) określono, jak spełnić wymagania lit. b) zasad. Niniejsze NZP 11 dotyczy lit. a) i c), które wymagają mechanizmów niezależnej ochrony prawnej. Mechanizmy te mogą przybierać różną postać, ale muszą spełniać wymagania zasady zapewniania prawu skuteczności. Organizacje mogą spełnić te wymagania w następujący sposób: 1) przez przestrzeganie programów ochrony prywatności opracowanych przez sektor prywatny, które włączają zasady „bezpiecznej przystani" do swoich zasad i które zawierają skuteczne mechanizmy zapewniania prawu skuteczności takiego rodzaju jak opisane w zasadzie zapewniania prawu skuteczności; 2) stosując się do wskazówek sądowych i wykonawczych organów nadzorczych, które rozpatrują indywidualne skargi i rozstrzygają spory; lub 3) przez zobowiązanie do współpracy z organami ochrony danych zlokalizowanymi na terytorium Unii Europejskiej lub ich upoważnionymi przedstawicielami. Wykaz ten ma charakter informacyjny, a nie ograniczający. Sektor prywatny może opracować inne mechanizmy zapewniające prawu skuteczność, o ile tylko spełniać one będą wymagania zasady zapewniania prawu skuteczności i NZP. Proszę zauważyć, że wymagania zasady zapewniania prawu skuteczności mają charakter uzupełniający wobec wymagań ustalonych w ust. 3 wstępu do zasad mówiących, że działania samoregulacyjne muszą być egzekwowalne na mocy art. 5 Ustawy o Federalnej Komisji Handlu albo podobnej ustawy.

Mechanizmy ochrony prawnej.

Powinno się zachęcać konsumentów do składania wszelkich skarg najpierw odnośnym organizacjom, zanim odwołają się do mechanizmów niezależnej ochrony prawnej. Pytanie o niezależność procedury jest pytaniem o fakty, które może być zadane w różny sposób, na przykład przez przejrzystość struktury i finansowania

lub udowodnione osiągnięcia. Zgodnie z wymogami zasady zapewniana prawu skuteczności, mechanizm ochronny przysługujący osobom fizycznym musi być dla nich łatwo dostępny i finansowo przystępny. Organy rozstrzygania sporów powinny rozpatrywać każdą skargę otrzymaną od osób fizycznych, chyba że jest ona w oczywisty sposób bezpodstawna lub niepoważna. Nie wyklucza to ustanowienia wymogów kwalifikacyjnych przez organizację stosującą mechanizm niezależnej ochrony prawnej, ale takie wymogi powinny być przejrzyste i uzasadnione (na przykład w celu wyłączenia skarg, które nie mieszczą się w zakresie programu albo kwalifikują się do rozpatrzenia na innym forum), i nie powinny skutkować podważeniem zobowiązania do rozpatrywania uzasadnionych skarg. Dodatkowo, mechanizmy niezależnej ochrony prawnej powinny umożliwiać osobom fizycznym pełną i łatwo dostępną informację o tym, jak działa procedura rozstrzygania sporów w momencie, gdy składają skargę. Taka informacja powinna zawierać informację o praktyce ochrony prywatności danego mechanizmu zgodnie z zasadami „bezpiecznej przystani" ([1]). Powinny one także współpracować przy opracowywaniu narzędzi takich jak znormalizowane formularze skargi w celu ułatwienia procesu rozpatrywania skarg

Środki zaradcze i sankcje.

Rezultatem wszelkich środków zaradczych, udostępnionych przez organ rozstrzygania sporów, powinno być, o ile to osiągalne, odwrócenie lub naprawienie przez organizację skutków nieprzestrzegania wymagań oraz zapewnienie, że w przyszłości organizacja będzie przetwarzała dane zgodne z zasadami oraz, gdzie stosownie, zaprzestanie przetwarzania danych osobowych osoby, która wniosła skargę. Sankcje powinny być dostatecznie surowe, aby zapewnić przestrzeganie zasad przez organizację. Zakres sankcji o różnym stopniu dolegliwości umożliwi organom rozstrzygającym spory reagować odpowiednio do stopnia nieprzestrzegania zasad. Sankcje powinny obejmować zarówno podanie do publicznej wiadomości stwierdzonych przypadków nieprzestrzegania zasad, jak i wymaganie usunięcia danych w pewnych okolicznościach ([2]). Inne sankcje mogą obejmować zawieszenie lub cofnięcie zezwolenia na prowadzenie działalności, odszkodowanie dla osób z tytułu strat poniesionych wskutek nieprzestrzegania zasad oraz zabezpieczenia roszczenia w określony sposób. Organy rozstrzygania sporów sektora prywatnego oraz organy samoregulacyjne muszą zgłaszać przypadki niewykonywania przez organizacje, które przystąpiły do „bezpiecznej przystani" ich orzeczeń organom rządowym o stosownej właściwości albo sądom, gdzie stosowne, oraz Departamentowi Handlu (albo osobie przez niego wyznaczonej).

Działanie Federalnej Komisji Handlu.

FKH (Federalna Komisja Handlu) podjęła się rozpatrywania na zasadzie pierwszeństwa wniosków wpływających od instytucji samoregulujących ochronę prywatności, takich jak BBBOnline i TRUSTe, oraz Państw Członkowskich podnoszących zarzuty nieprzestrzegania zasad „bezpiecznej przystani" w celu ustalenia, czy zostały naruszone przepisy sekcji 5 Ustawy o FKH zakazujące nieuczciwych bądź wprowadzających w błąd czynów lub praktyk handlowych. Jeżeli FKH stwierdzi, że ma powód bądź powody by uznać, że przepisy sekcji 5 zostały naruszone, może ona rozstrzygnąć sprawę wydając administracyjny nakaz zaprzestania stosowania kwestionowanych praktyk lub też składając w federalnym sądzie okręgowym skargę, która w przypadku jej uznania, może skutkować wydaniem takiego samego zakazu przez sąd federalny. Federalna Komisja Handlu może uzyskać nałożenie kary cywilnej za złamanie nakazu zaprzestania i może dochodzić stwierdzenia niewykonania polecenia sądu lub obrazy sądu za złamanie nakazu sądowego. FKH powiadomi Departament Handlu o wszystkich takich działaniach, które podjęła. Departament Handlu zachęca inne organy rządowe do powiadamiania go o ostatecznych przepisach wszelkich tego rodzaju wniosków lub innych orzeczeń stwierdzających przyjęcie zasad „bezpiecznej przystani".

Uporczywe nieprzestrzeganie zasad

Jeżeli organizacja uporczywie nie przestrzega zasad, to traci ona uprawnienia do korzystania z przywilejów „bezpiecznej przystani". Z uporczywym nieprzestrzeganiem mamy do czynienia wtedy przypadku, gdy organizacja, która złożyła oświadczenie w Departamencie Handlu (albo u osoby przez niego wyznaczonej) odmawia zastosowania się do ostatecznego przepisy jakiegokolwiek samoregulacyjnego albo rządowego organu, lub w przypadku gdy dany organ stwierdzi, że organizacja nie przestrzega zasad tak często, że jej twierdzenie o przestrzeganiu tych zasad przestaje być wiarygodne. W takich przypadkach organizacja musi niezwłocznie powiadomić Departament Handlu (albo osobę przez niego wyznaczoną) o tego rodzaju faktach. Niewykonanie tego może być powodem wszczęcia postępowania na podstawie Ustawy o fałszywych oświadczeniach (18 U. S. C. § 1001).

Departament (albo osoba przez niego wyznaczona) zamieści w prowadzonym przez siebie publicznym wykazie organizacji zaświadczających o przyjęciu zasad „bezpiecznej przystani" wszelkie zawiadomienia, jakie do niego wpłynął dotyczące uporczywego nieprzestrzegania zasad, niezależnie od tego czy wpłynie ono od samej organizacji, organu samoregulacji czy też organu rządowego, jednak dopiero po 30 dniach od zawiadomienia o tym organizacji, która nie stosowała zasad, dając jej jednocześnie możliwość udzielenia wyjaśnień. Stosownie do powyższego, w publicznym wykazie prowadzonym przez Departament Handlu (lub osobę przez niego wyznaczoną) zostanie wyraźnie podane, którym podmiotom przysługują przywileje „bezpiecznej przystani", a które je utraciły.

([1]) Organy rozstrzygające spory nie muszą przestrzegać zasady zapewniania prawu skuteczności. Mogą także odstępować od zasad w przypadku gdy napotykają na sprzeczne zobowiązania albo wyraźne upoważnienia przy wykonywaniu swoich szczególnych zadań.

([2]) Organy rozstrzygania sporów posiadają uprawnienia uznaniowe w zakresie okoliczności, w których stosują one te sankcje. Sensytywność odnośnych danych jest jednym z czynników, które należy wziąć pod uwagę, podejmując decyzję czy należy wymagać usunięcia danych, jak również czy organizacja zbierała, wykorzystywała lub ujawniła informacje z rażącym naruszeniem zasad.

Organizacja ubiegająca się o uczestnictwo w instytucji samoregulacji w celu ponownego zakwalifikowania się do „bezpiecznej przystani" musi dostarczyć temu organowi wszystkie informacje o swoim wcześniejszym uczestnictwie w „bezpiecznej przystani".

**NZP 12 — Możliwość wyboru — termin wyrażenia sprzeciwu**

P: *Czy zasada możliwości wyboru pozwala osobie fizycznej na dokonywanie wyboru tylko z chwilą powstania zależności czy w dowolnym czasie?*

O: Ogólnie rzecz biorąc, celem zasady możliwości wyboru jest zapewnienie, że informacja osobowa będzie wykorzystywana i ujawniana w sposób zgodny z oczekiwaniami i wyborem osoby, której dotyczy. Stosownie do tego, osoba fizyczna powinna móc skorzystać w dowolnym czasie z możliwości wyrażenia sprzeciwu (albo dokonania wyboru) wobec wykorzystania informacji osobowych w marketingu bezpośrednim w każdej chwili, przy uzasadnionych ograniczeniach ustalonych przez organizację, takich jak wyznaczenie terminu, w którym sprzeciw staje się skuteczny. Organizacja może też wymagać odpowiednich informacji pozwalających na potwierdzenie tożsamości osoby zgłaszającej sprzeciw. W Stanach Zjednoczonych osoby fizyczne mogą korzystać z takiego prawa dzięki centralnemu programowi zgłaszania sprzeciwu, takiemu jak (Mail Preference Service(Stowarzyszenie Marketingu Bezpośredniego). Organizacje biorące udział w Mail Preference Service powinny promować możliwość jego wykorzystania wśród konsumentów, którzy nie chcą otrzymywać informacji handlowych. W każdym razie osoby fizyczne powinny mieć do dyspozycji łatwo dostępną i finansowo przystępną procedurę, w celu dokonania takiego wyboru.

Podobnie, organizacja może wykorzystywać informacje do określonych celów związanych z marketingiem bezpośrednim, gdy umożliwienie osobie zainteresowanej zgłoszenia sprzeciwu przed użyciem informacji byłoby niewykonalne, jeżeli jednocześnie (oraz na żądanie w każdej chwili) dana organizacja bezzwłocznie umożliwi danej osobie rezygnację (bezpłatnie) z przyjmowania wszelkich dalszych materiałów marketingu bezpośredniego i organizacja zastosuje się do życzeń osoby fizycznej.

**NZP 13 — Informacje dotyczące podróży**

P: *Kiedy rezerwacja pasażera linii lotniczej i inne informacje związane z podróżą, takie jak informacje związane z programem „frequent flyer" lub rezerwacją hotelową oraz o potrzebie zapewnienia specjalnej obsługi, na przykład wyżywienia spełniającego wymagania religijne czy pomocy fizycznej, mogą być przekazywane organizacjom spoza terytorium UE?*

O: Takie informacje mogą być przekazywane w kilku różnych okolicznościach. Zgodnie z art. 26 dyrektywy dane osobowe mogą być przekazywane „do państwa trzeciego, które nie zapewnia adekwatnego poziomu ochrony w rozumieniu art. 25 ust. 2" pod warunkiem że 1) są one niezbędne do świadczenia usług żądanych przez konsumenta albo do spełnienia warunków umowy, takiej jak umowa „frequent flyer"; lub 2) konsument jednoznacznie wyraził na to zgodę. Amerykańskie organizacje uczestniczące w „bezpiecznej przystani" gwarantują właściwą ochronę danych osobowych i dlatego mogą otrzymywać dane przekazywane z UE bez konieczności spełnienia tych warunków bądź innych ustanowionych w art. 26 dyrektywy. Ponieważ „bezpieczna przystań" obejmuje szczególne zasady odnoszące się do informacji wrażliwych, takie informacje (której gromadzenie może być konieczne na przykład w związku z potrzebą zapewnienia klientowi pomocy fizycznej) może być zawarta w przekazach do uczestników „bezpiecznej przystani". Jednak we wszystkich przypadkach organizacja przekazująca informację musi przestrzegać prawa obowiązującego w Państwie Członkowskim UE, na terytorium, którego działa i które może między innymi nakładać specjalne warunki dotyczące posługiwania się danymi wrażliwymi.

**NZP 14 — Produkty farmaceutyczne i medyczne**

1. P: *Jeżeli dane osobowe są zbierane w UE i przekazywane do Stanów Zjednoczonych w celu prowadzenia badań farmaceutycznych i/lub w innych celach, to czy stosuje się ustawodawstwo Państwa Członkowskiego czy zasady „bezpiecznej przystani"?*

1 O: Ustawodawstwo Państwa Członkowskiego stosuje się do zbierania danych osobowych i do wszelkiego przetwarzania, które ma miejsce przed przekazaniem do Stanów Zjednoczonych. Do danych przekazanych już do Stanów Zjednoczonych stosuje się zasady „bezpiecznej przystani". W stosownych przypadkach dane używane do badań farmaceutycznych i do innych celów powinny zostać pozbawione cech identyfikacyjnych.

2. P: *Dane osobowe opracowane podczas szczególnych badań medycznych lub farmaceutycznych często odgrywają ważną rolę w przyszłych badaniach naukowych. W przypadku gdy dane osobowe zebrane dla jednego projektu badawczego zostaną przekazane do amerykańskiej organizacji w „bezpiecznej przystani", czy organizacja ta może wykorzystać te dane do innych badań naukowych?*

2. O: Tak, jeżeli na początku zapewniono właściwe ogłoszenie i wybór. Takie ogłoszenie powinno zawierać informację o wszelkich przyszłych sposobach użycia danych, takich jak kontrole okresowe, badania pokrewne albo marketing. Oczywistym jest to, że nie można wyszczególnić wszystkich przyszłych sposobów wykorzystania danych, ponieważ nowy sposób wykorzystania w badaniach może wyłonić się z nowego spojrzenia na pierwotne dane, nowych odkryć i postępów w medycynie, rozwoju w dziedzinie zdrowia publicznego i regulacjach. W stosownych przypadkach ogłoszenie powinno, więc zawierać wyjaśnienie, że dane osobowe mogą być wykorzystane w przyszłej medycznej i farmaceutycznej działalności badawczej, której nie da się przewidzieć. Jeżeli sposób wykorzystania jest niezgodne z ogólnym celem(ami) badawczymi, dla których dane były pierwotnie zbierane, albo na które osoba fizyczna wyraziła następnie zgodę, należy uzyskać nową zgodę.

3. P: *Co stanie się z danymi osoby fizycznej, jeżeli uczestnik zdecyduje sam albo na żądanie sponsora o wycofaniu się z prób klinicznych?*

3. O: Uczestnicy mogą sami zdecydować albo mogą zostać poproszeni o wycofanie się z badań klinicznych w każdej chwili. Wszelkie dane zebrane przed ich wycofaniem się mogą nadal być przetwarzane razem z innymi danymi zebranymi w ramach prób klinicznych, jednakże pod warunkiem że uczestnik został o tym wyraźnie poinformowany w ogłoszeniu w chwili, gdy on lub ona wyrażali zgodę na uczestnictwo.

4. P: *Firmy farmaceutyczne i producenci wyrobów medycznych są upoważnieni do przekazywania danych osobowych z prób klinicznych prowadzonych w UE organom regulacyjnym w Stanach Zjednoczonych do celów nadzoru i regulacji. Czy dozwolone jest podobne przekazywanie danych do stron innych niż organy regulacyjne, takich jak siedziby przedsiębiorstw i inne jednostki badawcze?*

4. O: Tak, zgodnie z zasadami ogłoszenia i wyboru.

5. P: *W celu zapewnienia obiektywności w szeregu prób klinicznych uczestnicy, a często także badacze, nie mogą mieć dostępu do informacji o tym, jakiemu leczeniu poddawany jest każdy uczestnik. Zagroziłoby to ważności badania i wyników. Czy osoby biorące udział w takich próbach klinicznych (zwanych „ślepymi" próbami) będą miały dostęp do danych o ich leczeniu w czasie trwania próby?*

5. O: Nie, taki dostęp nie musi być zapewniony uczestnikowi, jeżeli ograniczenie to zostało wyjaśnione, gdy uczestnik przystępował do próby, a ujawnienie takich informacji zagrażałoby integralności wysiłków badawczych. Zgoda na udział w próbie na tych warunkach stanowi uzasadnioną przyczynę rezygnacji z prawa dostępu. Po zakończeniu próby i przeanalizowaniu wyników uczestnicy powinni mieć dostęp do swoich danych, jeżeli tego zażądają. Powinni oni starać się o dostęp przede wszystkim u lekarza albo w placówce usług medycznych, która przeprowadziła leczenie w ramach próby klinicznej, lub w drugiej kolejności w firmie sponsorującej.

6. P: *Czy firma farmaceutyczna lub producent wyrobów medycznych musi stosować zasady „bezpiecznej przystani" w odniesieniu do ogłoszenia, wyboru, dalszego przekazywania danych i dostępu do nich w swoich działaniach monitorujących bezpieczeństwo i wydajność produktu, łącznie ze składaniem sprawozdań dotyczących niekorzystnych zdarzeń i obserwacji pacjentów/obiektów badawczych stosujących określone leki lub wyrobów medycznych (np. rozrusznik)?*

6. O: Nie, w zakresie, w którym przestrzeganie zasad koliduje z przestrzeganiem wymagań regulacyjnych. Odnosi się to zarówno do sprawozdań np. podmiotów świadczących usługi ochrony zdrowotnej, do firm farmaceutycznych i producentów wyrobów medycznych oraz do sprawozdań firm farmaceutycznych oraz do sprawozdań firm farmaceutycznych i producentów wyrobów medycznych sporządzanych dla agencji rządowych, jak Food and Drug Administration (Urząd ds. Żywności i Leków).

7. P: *Dane badawcze są zawsze szyfrowane na wstępie za pośrednictwem unikalnego klucza przez głównego badacza, tak żeby nie ujawniać tożsamości poszczególnych osób, których dane dotyczą. Spółki farmaceutyczne sponsorujące takie badania nie otrzymują klucza do szyfru. Unikalny klucz jest znany tylko badaczowi tak, że tylko on/ona może zidentyfikować obiekt badań, gdy zajdą szczególne okoliczności (np. jeżeli potrzebne jest badanie kontrolne). Czy przekazywanie z UE do Stanów Zjednoczonych danych osobowych zaszyfrowanych w ten sposób stanowi przekazanie danych osobowych podlegające zasadom „bezpiecznej przystani"?*

7. O: Nie. Nie stanowiłoby to przekazywania danych osobowych, które podlegałoby zasadom.

**NZP 15 — Dokumenty urzędowe i powszechnie dostępna informacja**

P: *Czy konieczne jest stosowanie zasad ogłoszenia, wyboru oraz dalszego przekazywania danych w odniesieniu do informacji pochodzących z dokumentów urzędowych albo informacji powszechnie dostępnej?*

O: Nie ma konieczności stosowania zasad ogłoszenia, wyboru i dalszego przekazywania danych w odniesieniu do informacji pochodzących z dokumentów urzędowych, dopóki nie jest ona połączona z informacją niepochodzącą z dokumentów urzędowych oraz dopóki są przestrzegane wszelkie warunki konsultacji ustanowione w ramach właściwej właściwości.

Nie jest także zasadniczo konieczne stosowanie zasad ogłoszenia, wyboru i dalszego przekazywania danych w odniesieniu do informacji powszechnie dostępnych, chyba że europejski nadawca zaznaczy, że takie informacje podlegają ograniczeniom, które wymagają stosowania tych zasad w przypadku zamierzonych przez organizację sposobów wykorzystania danych. Organizacje nie będą ponosić odpowiedzialności za to, jak takie informacje będą wykorzystywane przez tych, którzy uzyskają je z opublikowanych materiałów.

W przypadku gdy zostanie stwierdzone, że organizacja celowo podała do publicznej wiadomości informacje osobowe z naruszeniem zasad tak, aby sama mogła lub by inni mogli skorzystać z tych wyjątków, to utraci ona prawo do przywilejów „bezpiecznej przystani".

*ZAŁĄCZNIK III*

**Przegląd egzekwowania „bezpiecznej przystani"**

**Uprawnienia federalnych i stanowych organów w sprawach „nieuczciwych i wprowadzających w błąd praktyk" a ochrona prywatności**

Niniejsze memorandum nakreśla uprawnienia Federalnej Komisji Handlu (FKH) wynikające z sekcji 5 Ustawy o Federalnej Komisji Handlu (15 U. S. C. §§ 41-58, ze zmianami) do podejmowania działań przeciwko tym, którzy nie chronią prywatności informacji osobowych zgodnie ze swoimi oświadczeniami i/lub zobowiązaniami do takich działań. Zajmuje się także wyłączeniami spod tych uprawnień i zdolnością innych federalnych i stanowych agencji do podejmowania działania w przypadkach, gdy FKH nie posiada uprawnień ([1]).

**Uprawnienia FKH w sprawach nieuczciwych albo wprowadzających w błąd praktyk**

Sekcja 5 Ustawy o Federalnej Komisji Handlu uznaje „nieuczciwe albo wprowadzające w błąd czyny lub praktyki handlowe lub wpływające w handel" za niezgodne z prawem.15 U. S. C. § 45 lit. a) pkt 1. Sekcja 5 przyznaje FKH pełną władzę w zakresie zapobiegania takim czynom i praktykom. 15 U. S. C. § 45 lit. a) pkt 2. Stosownie do tego, FKH może po przeprowadzeniu formalnego przesłuchania wydać nakaz zaprzestania w celu powstrzymania zachowania naruszającego prawo. 15 U. S. C. § 45 lit. b). Jeżeli leżałoby to w interesie publicznym, FKH może także starać się o nakaz czasowego powstrzymania się od działania albo czasowego lub stałego zakazu wydanego przez amerykański sąd okręgowy. 15 U. S. C. § 53 lit. b). W przypadkach, gdy nieuczciwe albo wprowadzające w błąd czyny bądź praktyki występują powszechnie lub w przypadkach, gdy FKH wydała już nakaz zaprzestania działania w danej sprawie, może ona ogłosić przepis administracyjny przedawniający odnośne czyny lub praktyki. 15 U. S. C. § 57a.

Każdy, kto nie zastosuje się do nakazu FKH podlega karze cywilnej w wysokości do 11 000 USD, przy czym każdy dzień trwającego wykroczenia stanowi oddzielne wykroczenie ([2]). 15 U. S. C. § 45 ust. 1. Podobnie każdy, kto świadomie narusza którąkolwiek z zasad FKH podlega karze 11 000 USD za każde wykroczenie. 15 U. S. C. § 45 lit. m). Działania zapewniające prawu skuteczność mogą zostać wszczęte albo przez Departament Sprawiedliwości albo, jeśli tego odmówi, przez FKH. 15 U. S. C. § 56.

**Uprawnienia FKH a ochrona prywatności**

Wykorzystując swoje uprawnienia na mocy sekcji 5, FKH stoi na stanowisku, że podawanie fałszywych informacji w odniesieniu do powodu zbierania informacji od konsumentów albo sposobu, w jaki te informacje będą wykorzystane, stanowi wprowadzającą w błąd praktykę ([3]). Na przykład w 1998 r. FKH złożyła skargę przeciwko GeoCities z powodu ujawnienia informacji, które ta spółka zebrała w swojej witrynie internetowej, stronom trzecim w celu zabiegania o klientów bez uprzedniej zgody, pomimo przeciwnych oświadczeń ([4]). FKH stwierdziła także stanowczo, że zbieranie informacji osobowych od dzieci oraz sprzedaż i ujawnianie tych informacji bez zgody rodziców może być nieuczciwą praktyką ([5]).

---

([1]) Nie omawiamy tutaj wszystkich rozmaitych ustaw federalnych, które zajmują się ochroną prywatności w szczególnych kontekstach lub ustaw stanowych i prawa zwyczajowego, które może mieć tutaj zastosowanie. Ustawy na szczeblu federalnym, które regulują zbieranie i wykorzystanie informacji osobowej do celów handlowych, obejmują między innymi Cable Communications Policy Act (Ustawę o polityce łączności kablowej) (47 U. S. C. § 551), Driver's Privacy Protection Act (Ustawę o ochronie prywatności kierowcy) (18 U. S. C. § 2721), Electronic Communications Privacy Act (Ustawę o ochronie prywatności w łączności elektronicznej) (18 U. S. C. § 2701 i następny), Electronic Funds Transfer Act (Ustawę o elektronicznym przekazywaniu środków pieniężnych) (15 U. S. C. §§ 1693 z 1693m), Fair Credit Reporting Act (Ustawę o rzetelnej sprawozdawczości kredytowej) (15 U. S. C. § 1681 i następny), Right to Financial Privacy Act (Ustawę o prawie do ochrony prywatności finansowej) (12 U. S. C. § 3401 i następny), Telephone Consumer Protection Act (Ustawę o ochronie konsumentów usług telefonicznych) (47 U. S. C. § 227) i Video Privacy Protection Act (Ustawę o ochronie prywatności nagrań video) (18 U. S. C. § 2710). Wiele stanów ma w tych dziedzinach analogiczne prawodawstwo. Patrz: np. Mass. Gen. Laws rozdział 167B, § 16 (zakazujący instytucjom finansowym ujawniania dokumentów finansowych stronie trzeciej bez zgody klienta albo postępowania sądowego) N. Y. Pub. Health Law § 17 (ograniczający wykorzystanie i ujawnianie dokumentów medycznych lub dotyczących zdrowia psychicznego oraz dający pacjentom prawo dostępu do nich).

([2]) W takim postępowaniu amerykański sąd okręgowy może także orzec o zastosowaniu słusznych środków zabezpieczających odpowiednich do wykonania nakazu FTC (15 U. S. C. § 45 ust. 1).

([3]) „Wprowadzająca w błąd praktyka" jest definiowana jako informowanie, zaniechanie albo praktyka, które mogą w istotny sposób wprowadzić w błąd rozsądnych konsumentów.

([4]) Patrz: www.ftc.gov/opa/1998/9808/geocitie.htm.

([5]) Patrz interpretacja dla Center for Media Education (Centrum Edukacji Medialnej), w: www.ftc.gov/os/1997/9707/cenmed.htm. Ponadto, Ustawa o ochronie prywatności dzieci w systemie online z 1998 r. Udziela FTC szczególnej kompetencji prawnej w zakresie regulowania zbierania informacji osobowych od dzieci przez operatorów witryn internetowych i serwisów interaktywnych Patrz: 15 U. S. C. §§ 6501-6506. W szczególności ustawa wymaga od operatorów internetowych zawiadamiania i uzyskiwania sprawdzalnej zgody rodzicielskiej przed zebraniem, wykorzystaniem lub ujawnieniem informacji osobowych pozyskanych od dzieci. Id.,, § 6502 lit b). Ustawa daje także rodzicom prawo dostępu i prawo odmowy zezwolenia na dalsze wykorzystanie informacji. Id.,.

W liście do Johna Mogga, dyrektora Generalnego Komisji Europejskiej, Przewodniczący FKH Pitofsky zwrócił uwagę na ograniczenia uprawnień FKH do ochrony prywatności w przypadkach, gdy nie doszło do podania fałszywych informacji (albo nie dokonano oświadczenia) w odniesieniu do sposobu, w jaki sposób zebrane informacje będą wykorzystywane. List Przewodniczącego FKH Pitofsky'ego do Johna Mogga z dnia 23 września 1998 r. Jednakże przedsiębiorstwa, które chcą korzystać z proponowanej „bezpiecznej przystani" będą musiały złożyć oświadczenie o objęciu ochroną zebranych przez siebie informacji zgodnie z określonymi wytycznymi. W konsekwencji, w przypadkach, gdy przedsiębiorstwo oświadczy, że będzie chronić prywatność informacji, a następnie nie wykona tego, takie działanie byłoby podaniem fałszywych informacji i „praktyką wprowadzającą w błąd" w rozumieniu sekcji 5.

Ponieważ właściwość FKH rozciąga się na nieuczciwe albo wprowadzające w błąd czyny bądź praktyki „handlowe lub godzące w handel", FKH nie będzie posiadać właściwości nad zbieraniem i wykorzystywaniem informacji osobowych w celach niehandlowych, na przykład dotyczących charytatywnej zbiórki pieniędzy. Patrz list Pitofsky'ego, str. 3. Jednakże wykorzystanie informacji osobowych w dowolnej transakcji handlowej spełni warunki takiego predykatu sądowego. Zatem na przykład sprzedaż przez pracodawcę informacji osobowych o jego pracownikach organizacji zajmującej się sprzedażą bezpośrednią spowoduje, że taka transakcja wchodzić będzie w zakres sekcji 5.

**Wyjątki od sekcji 5**

Sekcja 5 ustanowiła wyjątki od uprawnień FKH w sprawach nieuczciwych albo wprowadzających w błąd czynów lub praktyk w odniesieniu do:

— instytucji finansowych, w tym banków, instytucji oszczędnościowo — kredytowych oraz spółdzielni kredytowych;

— telekomunikacji i międzystanowych przewoźników publicznych;

— przewoźników lotniczych; oraz

— zakładów rzeźnych i punktów skupu bydła rzeźnego

Patrz: 15 U. S. C. § 45 lit. a) pkt 2. Poniżej omawiamy każdy wyjątek i organ regulacyjny przejmujący jego rolę.

*Instytucje finansowe* ([1])

Pierwszy wyjątek stosuje się do „banków, instytucji oszczędnościowo-kredytowych określonych w sekcji 18 lit. f) pkt 3 (15 U. S. C. § 57a lit. f) pkt 3)" oraz „federalnych spółdzielni kredytowych określonych w sekcji 18, lit. f) pkt 4, (15 U. S. C. § 57a, lit. f), pkt 4)" ([2]). Te instytucje finansowe podlegają w zamian przepisom wykonawczym wydanym przez odpowiednio Federal Reserve Board (Radę Rezerwy Federalnej), Office of Thrift Supervision (Urząd Nadzoru Oszczędności) ([3]) i National Credit Union Administration Board (Radę Administracyjną Krajowej Spółdzielni Kredytowej). Patrz: 15 U. S. C. §§ 57a lit. f). Wymienione organy regulacyjne mają za zadanie wydawanie przepisów wykonawczych koniecznych do zapobiegania nieuczciwym i wprowadzającym w błąd praktykom tych instytucji finansowych ([4]) i ustanowienie oddzielnego wydziału, który będzie zajmował się skargami konsumentów. 15 U. S. C. § 57a lit. f) pkt 1. Wreszcie, uprawnienie do zapewniania prawu skuteczności wynika z sekcji 8 Federal Deposit Insurance Act (Ustawy o ubezpieczeniu federalnych depozytów) (12 U. S. C. § 1818) dla banków i instytucji oszczędnościowo — kredytowych oraz sekcji 120 i 206 Federal Credit Union Act (Ustawy o federalnej spółdzielni kredytowej) (15 U. S. C. §§ 57a lit. f) pkt 2-4).

Chociaż branża ubezpieczeniowa nie jest w sposób szczególny włączona do wykazu wyjątków w sekcji 5, Ustawa McCarran — Fergusson (15 U. S. C. § 1011 i następny) zasadniczo pozostawia regulację działalności

([1]) W dniu 12 listopada 1999 r. prezydent Clinton podpisał ustawę Gramm — Leach — Bliley (Pub. L. 106-102, skodyfikowana w 15 U. S. C. § 6801 et seq.). Ustawa ogranicza ujawnianie przez instytucje finansowe informacji osobowych o ich klientach. Ustawa nakłada na instytucje finansowe obowiązek między innymi powiadamiania wszystkich klientów o swojej polityce ochrony prywatności i praktykach odnoszących się do dzielenia się informacjami osobowymi z osobami współpracującymi i niewspółpracującymi. Ustawa upoważnia FTC, federalne władze bankowe i inne organy do urzędowego ogłaszania regulacji w celu wdrożenia ochrony prywatności wymaganej przez ustawę. W tym celu wspomniane agencje wydały wnioskowane przepisy.

([2]) Zgodnie z jego warunkami, wyjątek ten nie ma zastosowania do sektora papierów wartościowych. Dlatego też maklerzy, dealerzy i inne osoby działające w branży papierów wartościowych podlegają równocześnie właściwości Securities and Exchange Commission (Komisji Papierów Wartościowych i Giełd) i FTC w odniesieniu do nieuczciwych albo wprowadzających w błąd czynów lub praktyk.

([3]) Ten wyjątek w sekcji 5 pierwotnie odnosił się do Federal Home Loan Bank Board (Federalnej Bankowej Rady Hipotecznej), która została zniesiona w sierpniu 1989 r. przez Financial Institutions Reform, Recovery and Enforcement Act (Ustawą o reformie, odbudowie i egzekwowaniu prawa przez instytucje finansowe) z 1989 r. Jej zadania zostały przeniesione do Office of Thrift Supervision (Urzędu Nadzoru Oszczędności), Resolution Trust Corporation (Powierniczej Korporacji Upadłościowej), Federal Deposit Insurance Corporation (Federalnej Korporacji Ubezpieczeń Depozytów) i Housing Finance Board (Rady Finansowania Budownictwa).

([4]) Wyłączając instytucje finansowe spod właściwości FTC, sekcja 5 przewiduje także, że kiedykolwiek FTC wydaje rozstrzygnięcie w sprawie nieuczciwych albo wprowadzających w błąd czynów i praktyk, Rady ds. regulacji finansowych powinny przyjąć równoległe przepisy w ciągu 60 dni. Patrz 15 U. S. C. § 57a lit. f) pkt 1.

ubezpieczeniowejposzczególnym stanom ([1]). Ponadto na podstawie sekcji 2 lit. b) Ustawy McCarran — Fergusson, żadne prawo federalne nie może unieważnić, ograniczyć ani zastąpić regulacji stanowej, „chyba że taka ustawa wyraźnie odnosi się do działalności ubezpieczeniowej" (15 U. S. C. § 1012 lit. b)). Jednakże przepisy Ustawy o FKH stosuje się do branży ubezpieczeniowej „w takim zakresie, w jakim taka działalność nie jest regulowana przez prawo stanowe". Id.,. Należy także zauważyć, że McCarran — Fergusson odsyła do prawa stanowego tylko w odniesieniu do „działalności ubezpieczeniowej". Zatem FKH zachowuje pozostałe uprawnienia w zakresie nieuczciwych lub wprowadzających w błąd praktyk stosowanych przez firmy ubezpieczeniowe, gdy ich działalność nie dotyczy ubezpieczeń. Może to obejmować na przykład przypadki, gdy ubezpieczyciele sprzedają informacje osobowe o swych posiadaczach polis ubezpieczeniowych firmom zajmującym się sprzedażą bezpośrednią produktów innych niż ubezpieczeniowe ([2]).

*Przewoźnicy publiczni*

Drugi wyjątek od sekcji 5 obejmuje tych przewoźników publicznych, którzy „podlegają ustawom regulującym handel". 15 U. S. C. § 45 lit. a) pkt 2. W tym przypadku „ustawy regulujące handel" odnoszą się do tytułu 49 podtytuł IV United States Code (Kodeksu Stanów Zjednoczonych) i Communications Act (Ustawy o łączności) z 1934 r. (47 U. S. C. § 151 i nast. Communications Act (Ustawa o łączności). Patrz: 15 U. S. C. § 44.

49 U. S. C. podtytuł IV (Transport międzystanowy) obejmuje przewoźników kolejowych, samochodowych i wodnych, pośredników, spedytorów i operatorów rurociągów (49 U. S. C. § 10101 i następny). Wymienieni poszczególni przewoźnicy publiczni podlegają przepisom wydanym przez Surface Transportation Board (Radę Transportu Lądowego), niezależną agencję działającą w ramach Department of Transportation (Departamencie Transportu). 49 U. S. C. §§ 10501, 13501 i 15301. W każdym przypadku przewoźnikowi nie wolno ujawniać informacji o rodzaju, przeznaczeniu i innych aspektach ładunku, które mogłyby być użyte na szkodę nadawcy ładunku. Patrz: 49 U. S. C. §§ 11904, 14908 i 16103. Zwracamy uwagę, że powyższe przepisy odnoszą się do informacji dotyczącej ładunku nadawcy, a zatem nie obejmują raczej informacji osobowych o nadawcy ładunku, które nie są związane z daną wysyłką.

Jeżeli chodzi o Communications Act (Ustawę o łączności), wprowadza ona regulację „międzystanowego i zagranicznego handlu w zakresie łączności radiowej i kablowej" przez Federal Communications Commission (Federalną Komisję Łączności, FKŁ). Patrz: 47 U. S. C. §§ 151 i 152. Oprócz przedsiębiorstw telekomunikacyjnych będących publicznymi operatorami, Ustawę o łączności stosuje się także do takich przedsiębiorstw, jak nadawcy telewizyjni i radiowi oraz dostawcy sieci kablowych, nie będący operatorami publicznymi. Te ostatnie przedsiębiorstwa jako takie nie kwalifikują się do tego wyjątku na mocy sekcji 5 Ustawy o FKH. Zatem FKH posiada właściwość do badania tych przedsiębiorstw w zakresie prowadzonych przez nie nieuczciwych lub wprowadzających w błąd praktyk, podczas gdy FKŁ posiada równoległą właściwość w celu egzekwowania swoich niezależnych uprawnień w tej dziedzinie jak opisano wyżej.

Zgodnie z Communications Act, „każdy operator telekomunikacyjny", łącznie z lokalnymi operatorami telekomunikacyjnymi, ma obowiązek ochrony prywatności prawnie zastrzeżonych informacji o klientach ([3]). 47 U. S. C. § 222 lit a). Oprócz tych ogólnych uprawnień w zakresie ochrony prywatności Ustawa o łączności została zmieniona Cable Communications Policy Act, (Ustawą o polityce łączności kablowej) z 1984 r., zwana Cable Act. 47 U. S. C. § 521 i następny, w celu szczególnego upoważnienia operatorów sieci kablowych do ochrony prywatności „informacji identyfikowalnych osobowo" dotyczących abonentów sieci kablowych. 47 U. S. C. § 551 ([4]). Cable Act ogranicza zbieranie informacji osobowych przez operatorów sieci kablowych i wymaga, żeby operatorzy kablowi zawiadamiali abonentów o rodzaju zebranych informacji i o tym, jak te informacje będą wykorzystane. Cable Act daje abonentom prawo dostępu do informacji o nich i wymaga od operatorów sieci kablowych, żeby niszczyli informacje, kiedy nie są już potrzebne.

Communications Act upoważnia Federalną Komisję Łączności do egzekwowania tych dwóch przepisów o prywatności, albo z własnej inicjatywy, albo w odpowiedzi na skargę z zewnątrz ([5]). 47 U. S. C. §§ 205, 403; Id., § 208. Jeżeli FKŁ stwierdzi, że operator telekomunikacyjny (łącznie z operatorem sieci kablowej) naruszył przepisy o

---

([1]) „Działalność ubezpieczeniowa i każda wykonująca ją osoba podlegają prawu kilku stanów, które odnosi się do regulowania lub opodatkowywania takiej działalności". 15 U. S. C. § 1012 lit. a).

([2]) Zakłady ubezpieczeniowe podlegają właściwości FTC w różnych kontekstach. W jednym przypadku FTC wszczęła postępowanie przeciwko pewnej firmie w sprawie o wprowadzającą w błąd reklamę w stanie, w którym nie miała ona koncesji na wykonywanie działalności. Właściwość FTC została podtrzymana przez sąd na tej podstawie, że nie było skutecznej regulacji stanowej, ponieważ firma pozostawała faktycznie poza zasięgiem przepisów stanowych. Patrz: FTC przeciwko Travellers Health Association, 362 U. S. 293 (1960).

Jeżeli chodzi o stany to siedemnaście z nich przyjęło wzorcową Insurance Information and Privacy Protection Act (Ustawę o informacji ubezpieczeniowej i ochronie prywatności) opracowaną przez National Association of Insurance Commissioners, NAIC (Krajowe Zrzeszenie Komisarzy Ubezpieczonych, KZKU). Ustawa zawiera przepisy o zawiadamianiu, wykorzystaniu i ujawnianiu oraz dostępie. Ponadto, prawie wszystkie stany przyjęły opracowaną przez KZKU wzorcową Unfair Insurance Practices Act (Ustawę o nieuczciwych praktykach ubezpieczeniowych), która szczegółowo identyfikuje nieuczciwe praktyki handlowe w branży ubezpieczeniowej.

([3]) Termin „prawnie zastrzeżona informacja o kliencie pochodząca z sieci" oznacza informację, która dotyczy ilości, technicznej konfiguracji, rodzaju, miejsca i częstości korzystania z usługi telekomunikacyjnej przez klienta oraz informację o bilingu telefonicznym. 47 U. S. C. § 222 lit. f) pkt 1. Jednakże termin ten nie obejmuje informacji ze spisu abonentów. Id.,.

([4]) Ustawodawstwo nie definiuje wyraźnie „informacji identyfikujących osobowo".

([5]) Uprawnienie to obejmuje prawo do odszkodowania za naruszenie prywatności na mocy zarówno sekcji 222 Ustawy o łączności lub w odniesieniu do abonentów sieci kablowych sekcji 551 poprawki do Ustawy o łączności kablowej. Patrz też 47 U. S. C. § 551 lit f) pkt 3 (powództwo cywilne w federalnym sądzie okręgowym jest środkiem niewyłącznym, oferowanym „w uzupełnieniu do każdego innego środka prawnego dostępnego dla abonenta sieci kablowej)."

prywatności zawarte w sekcji 222 albo 551, to istnieją trzy podstawowe działania, jakie może podjąć. Po pierwsze, po przesłuchaniu i stwierdzeniu naruszenia prawa, Komisja może nakazać operatorowi zapłacenie odszkodowania pieniężnego [1]. 47 U. S. C. § 209. Alternatywnie, FKŁ może nakazać operatorowi zaprzestanie dalszego zaniechania albo niedozwolonej praktyki. 47 U. S. C. § 205 lit. a). W końcu, Komisja może także nakazać operatorowi dokonującemu naruszenia „podporządkowanie się [wszelkim] przepisom wykonawczym lub praktykom", jakie FKŁ może zalecić oraz „przestrzeganie ich". *Id*.

Osoby prywatne, które uznają, że operator telekomunikacyjny albo operator sieci kablowej naruszył odnośne przepisy Communications Act lub Cable Act (Ustawy o łączności albo Ustawy o polityce łączności kablowej) może albo złożyć skargę do FKŁ, albo wystąpić z roszczeniem do federalnego sądu okręgowego. 47 U. S. C. § 207. Skarżący, który wygra w postępowaniu przed sądem federalnym przeciwko operatorowi telekomunikacyjnemu w sprawie z tytułu niezapewnienia ochrony prawnie zastrzeżonej informacji o kliencie na podstawie szerszej sekcji 222 Communications Act może otrzymać odszkodowanie za szkody rzeczywiste i zwrot honorariów adwokackich. 47 U. S. C. § 206. Skarżący, który złoży pozew o naruszenie ochrony prywatności na podstawie szczególnych przepisów dotyczących łączności kablowej sekcji 551 Cable Act, może oprócz odszkodowania za szkody rzeczywiste i zwrotu honorariów adwokackich otrzymać także odszkodowanie za straty moralne i zwrot uzasadnionych kosztów procesowych. 47 U. S. C. § 551 lit. f).

FCC przyjęła szczegółowe zasady wykonania przepisów sekcji 222. Patrz: 47 CFR 64.2001-2009. Zasady te określają szczególne środki ochronne w celu ochrony przed nieuprawnionym dostępem do prawnie zastrzeżonej informacjach o klientach pochodzących z sieci. Przepisy te wymagają od operatorów telekomunikacyjnych, żeby:

— opracowywali i wdrażali systemy komputerowe, które „oflagowują" status powiadomienia/zgody klienta, gdy zapis dotyczący obsługi klienta po raz pierwszy pojawia się na ekranie;

— prowadzili elektroniczny „ślad kontrolny" pozwalający śledzić dostęp do konta klienta, w tym, kiedy otwierany jest zapis dotyczący obsługi klienta, przez kogo i w jakim celu;

— przeszkolili swoich pracowników na temat uprawnionego wykorzystania prawnie zastrzeżonej informacji o kliencie pochodzącej z sieci, z zachowaniem odpowiednich procedur dyscyplinarnych;

— ustanowili przeglądowy proces nadzoru w celu zapewnienia zgodności przy prowadzenie marketingu zewnętrznego; oraz

— składali coroczne oświadczenie do FKŁ o sposobie przestrzegania tych przepisów.

*Przewoźnicy lotniczy*

Amerykańscy i zagraniczni przewoźnicy lotniczy, którzy podlegają Federal Aviation Act (federalnej Ustawie o lotnictwie) z 1958 r. są także wyłączeni z sekcji 5 Ustawy o FKH. Patrz: 15 U. S. C. § 45 lit. a) pkt 2. Dotyczy to każdego, kto świadczy usługi międzystanowego lub zagranicznego lotniczego transportu towarów lub pasażerów bądź przewozu poczty. Patrz: 49 U. S. C. § 40102. Przewoźnicy lotniczy podlegają uprawnieniom Departamentu Transportu. W tym względzie Sekretarz Transportu jest upoważniony do podejmowania działań „zapobiegających nieuczciwym, wprowadzającymi w błąd, rabunkowym, albo sprzecznym z zasadami konkurencji praktykom w transporcie lotniczym". 49 U. S. C. § 40101 lit. a) pkt 9. Jeżeli leży to w interesie publicznym, Sekretarz Transportu może dociekać, czy amerykański albo zagraniczny przewoźnik lotniczy bądź sprzedawca biletów stosuje nieuczciwą albo wprowadzającą w błąd praktykę. 49 U. S. C. § 41712. Po przesłuchaniu stron Sekretarz Transportu może wydać nakaz zaniechania nielegalnej praktyki. Id. O ile wiadomo, Sekretarz Transportu nie korzystał z tych uprawnień w celu zajęcia się sprawą ochrony prywatności informacji osobowych dotyczących klientów linii lotniczych [2].

Istnieją dwa przepisy chroniące prywatność informacji osobowych, mające zastosowanie do przewoźników lotniczych w szczególnych sytuacjach. Po pierwsze, Federal Aviation Act (federalna Ustawa o lotnictwie) chroni prywatność kandydatów na pilotów. Patrz: 49 U. S. C. § 44936 lit. f). Zezwalając przewoźnikom lotniczym na uzyskanie akt osobowych kandydatów na pilotów, ustawa daje kandydatowi prawo do otrzymania zawiadomienia, że zażądano jego akt oraz do wyrażenia przez niego na to zgody, do poprawiania nieścisłości, a także do udostępniania danych tylko osobom zaangażowanym w podejmowanie decyzji o zatrudnieniu. Po drugie, przepisy Departamentu Transportu wymagają, aby informacje o liście pasażerów zbierane do wykorzystania przez rząd na wypadek katastrofy lotniczej były „zachowane w tajemnicy i ujawnione tylko Departamentowi Stanu USA, National Transportation Board (Krajowej Radzie ds. Transportu) (na żądanie National Transport Security Board, Krajowej Rady Bezpieczeństwa Transportu) i Departamentowi Transportu USA". 14 CFR część 243 § 243.9 lit. c), (uzupełniona przez 63 FR 8258).

---

[1] Jednakże nie wystąpienie szkody bezpośredniej u skarżącego nie stanowi podstawy do oddalenia skargi. 47 U. S. C. § 208 lit. a).

[2] Rozumiemy, że w branży trwają prace nad problemem ochrony prywatności. Przedstawiciele branży omawiali proponowane zasady „bezpiecznej przystani" i ich ewentualne zastosowanie w odniesieniu do przewoźników lotniczych. Omawiano także propozycję przyjęcia branżowej polityki ochrony prywatności, w ramach której uczestniczące przedsiębiorstwa wyraźnie poddałyby się uprawnieniom Departamentu Transportu.

*Zakłady rzeźne i punkty skupu bydła rzeźnego*

W odniesieniu do Packers and Stockyards Act (Ustawy o zakładach rzeźnych i punktach skupu bydła rzeźnego) z 1921 r. (7 U. S. C. § 181 i następny), ustawa zakazuje „każdemu zakładowi rzeźnemu w odniesieniu do żywca, mięs, mięsnych produktów żywnościowych albo nieprzetworzonych produktów z żywca bądź każdemu pośrednikowi handlującego żywym drobiem w odniesieniu do żywego drobiu, stosowania lub brania udziału we wszelkich nieuczciwych, niesprawiedliwie dyskryminujących lub wprowadzających w błąd praktykach lub środkach". 7 U. S. C. § 192 lit. a); patrz też: 7 U. S. C. § 213 lit. a) (zakazujący „wszelkich nieuczciwych, niesprawiedliwie dyskryminujących lub wprowadzających w błąd praktyk lub środków" w odniesieniu do inwentarza żywego. Podstawowym obowiązkiem Sekretarza Rolnictwa jest egzekwowanie tych przepisów, podczas gdy FKH zachowuje właściwość w odniesieniu do transakcji detalicznych oraz tych związanych z branżą drobiową. 7 U. S. C. § 227 lit. b) pkt 2.

Nie jest jasne, czy Sekretarz Rolnictwa będzie interpretował zaniedbanie ochrony prywatności ze strony zakładu rzeźnego lub punktu skupu bydła rzeźnego zgodnie z rzeczoną polityką jako praktykę „wprowadzającą w błąd" zgodnie z Ustawą o zakładach rzeźnych i punktach skupu bydła rzeźnego. Jednakże wyjątek od sekcji 5 stosuje się do osób, spółek osobowych i korporacji jedynie w zakresie, w jakim podlegają one Ustawie o zakładach rzeźnych i punktach skupu bydła rzeźnego. W związku z powyższym, jeżeli ochrona prywatności osób nie jest kwestią sporną w rozumieniu Ustawy o zakładach rzeźnych i punktach skupu bydła rzeźnego, wówczas ten wyjątek w sekcji 5 może właściwie nie mieć zastosowania i zakłady rzeźne i punkty skupu bydła rzeźnego podlegałyby w tym zakresie uprawnieniom FKH.

**Stanowe uprawnienia w zakresie „nieuczciwych i wprowadzających w błąd praktyk"**

Zgodnie z analizą opracowaną przez FKH, „wszystkie 50 stanów oraz dystrykt Kolumbia, Guam, Puerto Rico i Wyspy Dziewicze USA uchwaliły prawa mniej więcej zbliżone do Federal Trade Commission Act, FTCA (Ustawy o Federalnej Komisji Handlu," UFKH „) w celu zapobiegania nieuczciwym albo wprowadzającym w błąd praktykom w handlu" Raport FKH, przedrukowany w „Comment, Consummer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation", 59 Tul, L. Rev. 427 (1984 ). We wszystkich przypadkach organ przestrzegania prawa posiada uprawnienia „do prowadzenia dochodzeń poprzez stosowanie wezwań do stawiennictwa w sądzie lub cywilnych roszczeń prawnych, uzyskiwania gwarancji dobrowolnego przestrzegania, wydawania nakazów zaprzestania albo uzyskiwania sądowych przepisów o zabezpieczeniu roszczeń zapobiegających stosowaniu nieuczciwych, sprzecznych z zasadami współżycia społecznego albo wprowadzających w błąd praktyk handlowych. Tamże. W 46 jurysdykcjach prawo dopuszcza prywatne powództwa o odszkodowania za rzeczywiste, podwójne lub potrójne szkody lub nazwiązki, a w niektórych przypadkach zwrot kosztów i honorariów adwokackich. *Id*."

Na przykład, Deceptive and Unfair Trade Practices Act (Ustawa o wprowadzających w błąd i nieuczciwych praktykach handlowych) stanu Floryda upoważnia Prokuratora Generalnego do prowadzenia dochodzenia i wnoszenia powództwa cywilnego przeciwko „nieuczciwym metodom konkurencji, nieuczciwym i niezgodnym z zasadami współżycia społecznego albo wprowadzającym w błąd praktykom handlowym", łącznie z fałszywymi lub wprowadzającymi w błąd reklamami, wprowadzającymi w błąd ofertami prowadzenia działalności franszyzowej albo gospodarczej, oszukańczym telemarketingiem i piramidami finansowymi Patrz także: N. Y. General Business Law § 349 (zakazujący nieuczciwych czynów i wprowadzających w błąd praktyk stosowanych w trakcie prowadzenia działalności gospodarczej).

Badanie przeprowadzone w bieżącym roku przez National Association of Attorneys General, NAAG (Krajowe Zrzeszenie Prokuratorów Generalnych, KZPG) potwierdza te ustalenia. Spośród 43 stanów, które udzieliły odpowiedzi, wszystkie posiadają „mini — ustawy o FKH" lub inne ustawy, które zapewniają porównywalną ochronę. Także według badania KZPG, 39 stanów poinformowało, że mają uprawnienia do rozpatrywania skarg wnoszonych przez nierezydentów. W odniesieniu do ochrony prywatności konsumentów, w szczególności, 37 spośród 41 stanów, które udzieliły odpowiedzi, poinformowało, że zareagują na skargi o nieprzestrzeganiu przez przedsiębiorstwo podlegające ich właściwości zadeklarowanej przez nie polityki ochrony prywatności.

*ZAŁĄCZNIK IV*

**Odszkodowania z tytułu naruszenia prywatności, prawne upoważnienia oraz łączenia i przejęcia przedsiębiorstw w prawie amerykańskim**

Niniejszy Załącznik jest odpowiedzią na zgłoszony przez Komisję Europejską wniosek objaśnienia amerykańskiego prawa dotyczącego a) roszczeń odszkodowawczych z tytułu naruszenia prywatności, b) „wyraźnych upoważnień" w prawie amerykańskim do wykorzystania informacji osobowej w sposób niezgodny z zasadami „bezpiecznej przystani", i c) łączenia się i przejęć przedsiębiorstw wpływających na zobowiązania podjęte zgodnie z zasadami „bezpiecznej przystani".

A. **Odszkodowania z tytułu naruszenia prywatności**

Nieprzestrzeganie zasad „bezpiecznej przystani" może stanowić podstawę do szeregu prywatnych roszczeń w zależności od stosownych okoliczności. W szczególności, organizacje „bezpiecznej przystani" mogą zostać pociągnięte do odpowiedzialności za wprowadzenie w błąd z powodu nieprzestrzegania własnych procedur ochrony prywatności przez nie określonych. Prywatne powództwa o odszkodowania za naruszenie prywatności są także dostępne w systemie prawa powszechnego. Wiele federalnych i stanowych ustaw w sprawie ochrony prywatności daje także możliwość uzyskania przez osoby prywatne odszkodowań za naruszenia.

*Prawo do otrzymania odszkodowania za naruszenie prywatności osobistej jest dobrze ugruntowane w amerykańskim prawie powszechnym.*

Wykorzystanie informacji osobowych w sposób niezgodny z zasadami „bezpiecznej przystani" może powodować powstanie odpowiedzialności prawnej na podstawie szeregu różnych teorii prawnych. Na przykład zarówno przekazujący kontroler danych, jak i osoby fizyczne poszkodowane mogą zaskarżyć organizację „bezpiecznej przystani", która nie honoruje swoich zobowiązań wynikających z „bezpiecznej przystani", za wprowadzenie w błąd. Drugi zbiór prawa USA, czyny niedozwolone ([1]) stanowi, że:

> Kto w sposób oszukańczy podaje fałszywą informację w odniesieniu do faktu, opinii, zamiaru albo prawa w celu nakłonienia drugiej osoby do działania albo powstrzymania się od działania w oparciu o to, podlega odpowiedzialności wobec tej osoby z tytułu oszustwa za stratę pieniężną poniesioną przez nią z powodu jej usprawiedliwionego zawierzenia takiej fałszywej informacji.

Zbiór prawa cywilnego, § 525. Podanie fałszywych informacji jest „oszukańcze", jeżeli zostało popełnione ze świadomością albo w przekonaniu, że jest fałszywe. Id.,, § 526. Jako generalną zasadę przyjmuje się, że ten kto podaje fałszywe informacje jest potencjalnie odpowiedzialny wobec każdej osoby, która zgodnie z jego zamiarem albo oczekiwaniami zawierzy jego fałszywej informacji, za stratę pieniężną jaką w wyniku owego zawierzenia osoba ta mogłaby ponieść. *Id.*, 531. Ponadto, strona podająca fałszywą informację drugiej stronie może być odpowiedzialna wobec strony trzeciej, jeżeli osoba dopuszczająca się czynu niedozwolonego zamierza albo oczekuje, że fałszywa informacja zostanie powtórzona osobie trzeciej, która podejmie działanie na jej podstawie. Id., § 533.

W kontekście „bezpiecznej przystani" odnośną informacją jest publiczna deklaracja organizacji, że przyjmie zasady „bezpiecznej przystani". Po podjęciu takiego zobowiązania przypadek świadomego nieprzestrzegania tych zasad może stanowić podstawę do wniesienia powództwa z tytułu podania fałszywych informacji przez osoby, które zawierzyły fałszywej informacji. Ponieważ zobowiązanie przestrzegania tych zasad jest dokonywane jest wobec publiczności, osoby będące przedmiotem tej informacji, jak również kontroler danych w Europie, który przekazuje informacje osobowe amerykańskiej organizacji, mogą mieć podstawy do wytoczenia powództwa przeciwko amerykańskiej organizacji z tytułu podania fałszywych informacji ([2]). Ponadto amerykańska organizacja pozostaje odpowiedzialna wobec nich za stałe podawanie fałszywych informacji tak długo, jak długo osoby te polegają na fałszywej informacji na swoją szkodę. Zbiór prawa cywilnego, § 535.

([1]) Second Restatement of the Law — Torts (Drugi zbiór prawa — czyny niedozwolone); American Law Institute (1997).

([2]) Taki przypadek może mieć miejsce na przykład, kiedy osoby fizyczne polegały na zobowiązaniach „bezpiecznej przystani" składanych przez amerykańską organizację, kiedy dawały zgodę kontrolerowi danych na przesłanie ich informacji osobowych do Stanów Zjednoczonych.

Osoby, które polegają na oszukańczym podaniu fałszywych informacji mają prawo do uzyskania odszkodowania. Według zbioru prawa:

> Osoba poszkodowana przez podanie fałszywych informacji, w powództwie z tytułu wprowadzenia w błąd, jest uprawniona do dochodzenia od sprawcy w formie odszkodowania poniesionej przez nią straty pieniężnej, której przyczyną prawną było podanie fałszywych informacji.

Zbiór prawa, § 549. Dopuszczalne odszkodowanie obejmuje rzeczywiste straty bieżące, a także utraconą „korzyść z transakcji" przy transakcji handlowej. *Id.;* patrz: np. Boling przeciwko Tennessee State Bank, 890 S. W.2d 32 (1994) (odszkodowanie wyrównawcze w wysokości 14 825 USD z tytułu odpowiedzialności banku wobec kredytobiorców za ujawnienie informacji osobowej i biznes planu kredytobiorców prezesowi banku uwikłanego w konflikt interesów).

Oszukańcze podanie fałszywych informacji wymaga albo rzeczywistej wiedzy albo przynajmniej przekonania, że informacja jest fałszywa, odpowiedzialność może także wiązać się z podaniem fałszywych informacji na skutek niedbalstwa. Zgodnie ze zbiorem prawa każdy, kto podaje fałszywe informacje podczas wykonywania swojej działalności gospodarczej, zawodu albo pracy najemnej, bądź w toku przeprowadzania jakiejkolwiek transakcji pieniężnej, może być pociągnięty do odpowiedzialności, „jeżeli nie dochowa należytej staranności lub fachowości przy uzyskiwaniu albo udzielaniu informacji". Zbiór prawa cywilnego, § 552 ust. 1. W przeciwieństwie do oszukańczego podania fałszywych informacji, odszkodowanie z tytułu podania fałszywych informacji na skutek niedbalstwa jest ograniczone do strat bieżących. *Id.,* § 552B ust. 1).

Na przykład w niedawno rozpatrywanej sprawie Sąd Najwyższy stanu Connecticut orzekł, że nieujawnienie przez elektrownię faktu przekazania informacji o płatnościach klienta krajowym agencjom kredytowym stanowi podstawę wniesienia powództwa z tytułu podania fałszywych informacji. Patrz: Bouillard przeciwko United Illuminating Co., 1999 Conn. Super. LEXIS 1754. W omawianym przypadku powodowi odmówiono kredytu, ponieważ pozwany zgłosił płatności nieuzyskane w ciągu trzydziestu dni od daty wystawienia rachunku jako „spóźnione". Powód podnosił, że nie został poinformowany o tej polityce, kiedy otwierał u pozwanego rachunek do rozliczeń opłat za dostawę energii elektrycznej do domu. Sąd wyraźnie orzekł, że „roszczenie z tytułu podania fałszywych informacji na skutek niedbalstwa może się opierać na tym, że pozwany nie udziela informacji wtedy, gdy jest to jego obowiązkiem". Ten przypadek pokazuje także, iż „świadomy" albo oszukańczy zamiar nie jest koniecznym elementem do wniesienia powództwa z tytułu podania fałszywych informacji na skutek niedbalstwa. Zatem amerykańska organizacja, która na skutek niedbalstwa nie ujawni w pełni, w jaki sposób będzie wykorzystywać informację osobową otrzymaną w ramach „bezpiecznej przystani", może zostać pociągnięta do odpowiedzialności za podanie fałszywych informacji.

W zakresie, w jakim naruszenie zasad „bezpiecznej przystani" obejmowało niewłaściwe wykorzystanie informacji osobowych, mogło także stanowić podstawę roszczenia ze strony osoby, której dane dotyczą, z tytułu deliktu naruszenia prywatności na podstawie prawa powszechnego. Prawo amerykańskie od dawna uznaje powództwa związane z naruszeniem prywatności. W sprawie z 1905 r. ([1]) Sąd Najwyższy stanu Georgia orzekł na korzyść obywatela, którego fotografia została użyta bez jego zgody i wiedzy przez zakład ubezpieczeń na życie do zilustrowania reklamy handlowej, że prawo do prywatności wynika z prawa naturalnego i twierdzeń prawa precedensów. Wyrażając znane obecnie wątki amerykańskiego orzecznictwa dotyczącego ochrony prywatności, sąd uznał, że takie wykorzystanie fotografii było „złośliwe", „kłamliwe" i zmierzało do „publicznego ośmieszenia powoda". ([2]) Podstawy wyroku w sprawie Pavesich pozostają z niewielkimi zmianami fundamentem amerykańskiego prawa w tym zakresie. Sądy stanowe konsekwentnie uznają naruszenia w dziedzinie prywatności jako podstawę powództwa; obecnie co najmniej 48 stanów uznaje tego rodzaju podstawę powództwa w swoim orzecznictwie ([3]). Ponadto, w co najmniej 12 stanach obowiązują przepisy konstytucyjne chroniące prawa ich obywateli przed działaniami naruszającymi prywatność ([4]), które w pewnych przypadkach mogą się rozszerzać na ochronę przed naruszeniem prywatności przez podmioty pozarządowe. Patrz: np. Hill przeciwko NCAA, 865 P.2d 633 (Ca. 1994); patrz także: S. Ginder, Lost and Found in Cyberspace: Information Privacy in the age of the internet, 34 S. D. L. Rev. 1153 (1997) („Niektóre konstytucje stanowe zawierają lepsze przepisy ochrony prywatności niż przepisy zawarte w konstytucji Stanów Zjednoczonych. Stany Alaska, Arizona, Kalifornia, Floryda, Hawaje, Illinois, Luizjana, Montana, Południowa Karolina i Waszyngton posiadają szerszą ochronę prywatności").

Drugi zbiór prawa dotyczący czynów niedozwolonych daje autorytatywny przegląd prawa w tej dziedzinie. Odzwierciedlając powszechną praktykę sądów, zbiór wyjaśnia, że „prawo do prywatności" obejmuje cztery różne podstawy powództwa z tytułu szkody wyrządzonej czynem niedozwolonym. Patrz: Zbiór, § 652A. Po pierwsze podstawa powództwa z tytułu naruszenia prywatności i miru domowego może przysługiwać przeciwko pozwanemu, który umyślnie narusza, fizycznie albo w inny sposób, prywatność i mir domowy innejosoby bądź jej spraw

([1]) Pavesich przeciwko New England Life Ins. Co., 50 S. E. 68 (Ga. 1905).

([2]) Id., w 69.

([3]) Elektroniczne przeszukanie bazy danych Westlaw wykazało 2 703 zgłoszonych przypadków powództwa cywilnego w sądach stanowych, które odnosiły się do „ochrony prywatności" od 1995 r. Wcześniej przekazaliśmy wyniki tego wyszukiwania Komisji.

([4]) Patrz np. Konstytucja stanu Alaska sekcja 22 art. 1; stanu Arizona sekcja 8 art. 2; stanu Kalifornia sekcja 1 art. 1; stanu Floryda sekcja 23 art. 1; stanu Hawaje sekcja 5 art. 1; stanu Illinois sekcja 6 art. 1, stanu Luizjana sekcja 5 art. 1; stanu Montana sekcja 10 art. 2; stanu Nowy York sekcja 12 art. 1; stanu Pensylwania sekcja 1 art. 1; stanu Południowa Karolina sekcja 10 art. 1; i stanu Waszyngton sekcja 7 art. 1.

prywatnych ([1]). Po drugie może zaistnieć przypadek „przywłaszczenia", gdy ktoś używa imienia i nazwiska albo podobizny dla swojego własnego użytku lub korzyści ([2]). Po trzecie „opublikowanie faktów dotyczących życia prywatnego" podlega zaskarżeniu, gdy opublikowana informacja ma taki charakter, że jej opublikowanie byłoby wysoce obraźliwe dla rozsądnej osoby, a nie jest ona przedmiotem uzasadnionego zainteresowania ogółu ([3]). Wreszcie, powództwo z tytułu rozpowszechniania o kimś oszczerczych informacji jest zasadne, gdy pozwany świadomie lub lekkomyślnie stawia kogoś publicznie w fałszywym świetle, które byłoby wysoce obraźliwe dla rozsądnej osoby ([4]).

W kontekście „bezpiecznej przystani", „naruszenie miru domowego" mogłoby obejmować nieuprawnione zbieranie informacji osobowych, podczas, gdy nieuprawnione wykorzystanie informacji osobowych do celów handlowych mogłoby stanowić przyczynę powództwa z tytułu przywłaszczenia. Podobnie ujawnienie informacji osobowych, które są nieścisłe, stanowiłoby czyn niedozwolony w postaci rozpowszechnienia oszczerczych informacji, jeżeli informacja spełnia kryteria wysokiej obraźliwości dla rozsądnej osoby. Wreszcie, naruszenie prywatności, którego przyczyną jest opublikowanie lub ujawnienie informacji osobowych zawierających dane wrażliwe, mogłoby stanowić podstawę do powództwa z tytułu „opublikowania faktów dotyczących życia prywatnego". Patrz przykładowe spraw poniżej.

W zakresie odszkodowań, naruszenia prywatności upoważniają stronę poszkodowaną do dochodzenia odszkodowania za:

a) naruszenie jej prawa do prywatności powstałe na skutek naruszenia;

b) zakłócenie czynności psychicznych, które u niego stwierdzono, jeżeli mają one taki charakter, że zwykle wynikają z takiego naruszenia;

c) szczególną szkodę, której przyczyną prawną jest naruszenie.

Zbiór prawa, § 652H. Biorąc pod uwagę ogólne stosowanie prawa o czynach niedozwolonych i wielość podstaw powództwa obejmujących rozmaite aspekty interesów prywatnych, na odszkodowanie pieniężne mogą liczyć osoby, których dotknęło naruszenie ich interesów związanych z prywatnością w wyniku nieprzestrzegania zasad „bezpiecznej przystani".

Sądy stanowe faktycznie są przepełnione sprawami o wtargnięcie w prywatność w analogicznych sytuacjach. Postępowanie *ex parte* AmSouth Bancorporation et al., 717 So. 2d 357 obejmowało na przykład pozew grupowy, w którym zarzucono pozwanemu, że „wykorzystał zaufanie posiadaczy kont do Banku, udzielając poufnych informacji dotyczących posiadaczy kont w banku i ich rachunków", w celu umożliwienia osobom upoważnionym przez bank sprzedaży funduszy wzajemnych i innych inwestycji. W takich przypadkach często przyznawane są odszkodowania. W sprawie Vassiliades przeciwko Garfinckel's, Brooks Bros., 492 A.2d 580 (D. C. App. 1958) sąd apelacyjny uchylił wyrok sądu niższej instancji orzekając, że użycie fotografii powoda „przed" i „po" operacji plastycznej do prezentacji w domu towarowym stanowiło wtargnięcie w prywatność poprzez publikację faktów dotyczących życia prywatnego. W sprawie Candebat przeciwko Flanagan, 487 So.2d 207 (Miss. 1986) pozwany zakład ubezpieczeń wykorzystał w kampanii reklamowej wypadek, w którym poważne obrażenia odniosła żona powoda. Powód wytoczył powództwo o naruszenie prywatności. Sąd orzekł, że powód może dochodzić odszkodowania za zakłócenie czynności psychicznych i przywłaszczenie tożsamości. Roszczenia o nieuprawnione użycie mogą zostać uznane nawet wtedy, gdy osoba powoda nie jest sławna Patrz, np. Staruski przeciwko Continental Telephone Co., 154 Vt. 568 (1990) (pozwany uzyskał korzyść handlową wykorzystując imię i nazwisko oraz zdjęcie pracownika w reklamie w gazecie). W sprawie Pulla przeciwko Amoco Oil Co., 882 F. Supp. 836 (S. D Iowa 1995) pracodawca naruszył prywatność pracownika pozwanego przez to, że zlecił innemu pracownikowi zbadanie historii jego karty kredytowej w celu zweryfikowania jego nieobecności w pracy z tytułu choroby. Sąd podtrzymał rozstrzygnięcie ławy przysięgłych o przyznaniu odszkodowania w wysokości 2 USD za szkody rzeczywiste i 500 000 USD za straty moralne. Inny pracodawca został pociągnięty do odpowiedzialności za opublikowanie w gazecie zakładowej artykułu o pracowniku, który został zwolniony za domniemane fałszowanie swoich dokumentów dotyczących zatrudnienia Patrz Zinda przeciwko Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis. App. 1987). Artykuł naruszył prywatność powoda przez opublikowanie prywatnej sprawy, ponieważ gazeta była rozpowszechniania w społeczności, której był członkiem. Wreszcie uczelnia, która przebadała studentów pod kątem zarażenia wirusem HIV twierdząc, że badanie krwi miało na celu wykrycie jedynie różyczki, została uznana za odpowiedzialną za naruszenie prywatności. Patrz: Doe przeciwko High-Tech Institute, Inc., 972 P.2d 1060 (Colo. App. 1998). Inne zgłoszone sprawy — patrz Zbiór prawa, § 652H, Dodatek.

Stany Zjednoczone są często krytykowane za nadmierną skłonność do wchodzenia na drogę sądową, ale oznacza to także, iż osoby fizyczne mogą i faktycznie korzystają z możliwości sądowego dochodzenia swoich praw, kiedy czują się pokrzywdzone. Wiele aspektów amerykańskiego systemu sądowego ułatwia powodom wnoszenie powództwa

([1]) Id., sekcja 62B rozdział 28.
([2]) Id., sekcja 652C rozdział 28.
([3]) Id., sekcja 652D rozdział 28.
([4]) Id., sekcja 652E rozdział 28.

indywidualnie lub grupowo. Adwokatura porównywalnie liczniejsza niż w większości innych krajów zapewnia łatwy dostęp do przedstawicielstwa ustawowego. Adwokat powoda, występujący jako przedstawiciel osób fizycznych w powództwach prywatnych najczęściej pracuje za wynagrodzeniem uzależnionym od wygrania sprawy, co pozwala nawet ludziom biednym ubiegać się o odszkodowanie. Podnosi to ważną kwestię — w Stanach Zjednoczonych każda strona zwykle ponosi koszty honorariów swojego adwokata i pozostałe koszty. Kontrastuje to z przeważającą w Europie zasadą, zgodnie, z którą strona przegrywająca musi zwrócić koszty drugiej stronie. Nie rozważając względnych zalet obu systemów, przyjęta w USA zasada w mniejszym stopniu zniechęca do dochodzenia uzasadnionych roszczeń osoby fizyczne, które nie byłyby w stanie zapłacić kosztów poniesionych przez obie strony w przypadku przegrania procesu.

Osoby fizyczne mogą dochodzić sądownie odszkodowań nawet wówczas, gdy ich roszczenia są stosunkowo niewielkie. Większość, jeżeli nie wszystkie jurysdykcje w USA, posiadają sądy dla rozpoznawania drobnych roszczeń, które zapewniają uproszczone i mniej kosztowne procedury dla sporów nie mieszczących się w granicach ustawowych ([1]). Dzięki możliwościom stwarzanym przez nawiązkę, także osoby, które poniosły niewielką szkodę bezpośrednią mogą wnosić powództwo z tytułu wykroczenia. Wreszcie, osoby fizyczne, które zostały pokrzywdzone w ten sam sposób mogą zebrać razem swoje środki i roszczenia w celu wniesienia powództwa grupowego.

Dobrym przykładem możliwości osób fizycznych w zakresie wnoszenia powództwa w celu uzyskania odszkodowania jest będąca w toku sprawa sądowa przeciwko Amazon.com o naruszenie prywatności. Amazon.com, wielki detalista internetowy, jest przedmiotem pozwu grupowego, w którym powodowie utrzymują, że nie zostali poinformowani i nie wyrazili zgody na zbieranie informacji osobowych ich dotyczących, gdy korzystali z programu komputerowego o nazwie „Alexa" będącego własnością Amazon.com. W tym przypadku powodowie zarzucili naruszenie Computer Fraud and Abuse Act (Ustawy o oszustwach i nadużyciach komputerowych) poprzez bezprawny dostęp do przechowywanej przez nich korespondencji oraz Electronic Communications Privacy Act (Ustawy o ochronie prywatności w łączności elektronicznej) przez bezprawne przechwytywanie ich korespondencji elektronicznej i przewodowej. Zgłaszają także roszczenie z tytułu naruszenia prywatności na podstawie prawa powszechnego. Wynika ono ze skargi złożonej w grudniu przez specjalistę ds. bezpieczeństwa w sieci. Powodowie domagają się odszkodowania w wysokości 1 000 USD na uczestnika grupy pozywającej plus honoraria adwokackie i zyski osiągnięte w wyniku naruszeń prawa. Biorąc pod uwagę, że ilość uczestników grup może sięgać milionów, odszkodowanie może wynieść łącznie miliardy dolarów. Zarzuty bada także FKH.

*Ustawodawstwo federalne i stanowe często uznaje możliwość wytoczenia prywatnego powództwa o odszkodowanie pieniężne.*

Oprócz tytułu do odpowiedzialności cywilnej na podstawie prawa o czynach niedozwolonych, nieprzestrzeganie zasad „bezpiecznej przystani" może także stanowić naruszenie któregoś spośród setek federalnych i stanowych przepisów prawa dotyczącego prywatności. Wiele z tych przepisów, które podnoszą kwestię posługiwania się informacjami osobowymi zarówno przez sektor rządowy, jak i prywatny, pozwala osobom fizycznym dochodzić odszkodowania w przypadku naruszenia prawa. Na przykład:

*Electronic Communications Privacy Act, ECPA (Ustawa o ochronie prywatności w łączności elektronicznej) z 1986 r.* Zakazuje ona nieuprawnionego przechwytywania rozmów w sieci telefonii komórkowej i danych przekazywanych między komputerami. Naruszenia mogą skutkować odpowiedzialnością cywilną nie mniejszą niż 100 USD za każdy dzień naruszania prawa. Ochrona ECPA obejmuje także nieuprawniony dostęp do przechowywanej korespondencji elektronicznej lub jej ujawnienie. Osoby naruszające prawo zobowiązane są do wynagrodzenia poniesionej szkody albo narażają się na utratę zysków osiągniętych w drodze naruszenia.

*Telecomunications Act (Ustawa o telekomunikacji) z 1996 r.* Zgodnie z sekcją 702 customer proprietary network information, CPNI (prawnie zastrzeżona informacja o klientach pochodząca z sieci) nie może być wykorzystana w żadnym innym celu, jak tylko świadczenie usług telekomunikacyjnych. Abonenci usług mogą złożyć skargę do Federalnej Komisji Łączności lub wnieść pozew w federalnym sądzie okręgowym w celu uzyskania odszkodowania i zwrotu honorariów adwokackich.

*Consumer Credit Reporting Reform Act (Ustawa o reformie sprawozdawczości dotyczącej kredytów konsumeckich) z 1996 r.* Ustawa z 1996 r. zmieniła Fair Credit Reporting Act, FCRA (Ustawę o rzetelnej sprawozdawczości kredytowej) z 1970 r. ustanawiając wymóg lepszego ogłaszania i prawa dostępu dla osób, będących przedmiotem informacji kredytowych. Zmieniona ustawa nałożyła także nowe ograniczenia na podmioty odsprzedające informacje o sytuacji kredytowej konsumentów. Konsumenci mogą uzyskać odszkodowanie i zwrot kosztów adwokackich za naruszenia.

([1]) Informowaliśmy wcześniej Komisję na temat powództw w sprawach dotyczących drobnych roszczeń.

Prawa stanowe chronią także prywatność osób w wielu różnorodnych okolicznościach. Obszary, w których stany podjęły działania obejmują zapisy bankowe, abonamenty telewizji kablowych, sprawozdania kredytowe, akta osobowe pracowników, akta rządowe, informację genetyczną i dokumentację medyczną, dokumentację ubezpieczeniową, dokumentację szkolną, korespondencję elektroniczną i wypożyczalnie kaset video ([1]).

B. **Wyraźne upoważnienia prawne**

Zasady „bezpiecznej przystani" zawierają wyjątek w przypadku gdy, przepisy prawa stanowionego albo precedensy stwarzają „sprzeczne obowiązki albo wyraźne upoważnienia, pod warunkiem że stosując każde takie upoważnienie, organizacja może wykazać, że nie przestrzeganie przez nią zasad ogranicza się jedynie do poziomu koniecznego do zaspokojenia nadrzędnych, uzasadnionych interesów popartych takim upoważnieniem". Najwyraźniej w przypadkach, gdy prawo amerykańskie nakłada sprzeczny obowiązek na organizacje amerykańskie, czy to działające w ramach „bezpiecznej przystani" czy poza nią, muszą one przestrzegać tego prawa. Jeżeli chodzi o wyraźne upoważnienia, podczas, gdy celem zasad „bezpiecznej przystani" jest zatarcie różnic między amerykańskimi a europejskimi systemami ochrony prywatności, ustawodawczym prerogatywom naszych wybranych ustawodawców należne jest poważanie. Ograniczony wyjątek od ścisłego przestrzegania zasad „bezpiecznej przystani" stanowi próbę zachowania równowagi w celu pogodzenia uzasadnionych interesów każdej ze stron.

Wyjątek jest ograniczony do przypadków, w których istnieje wyraźne upoważnienie. Zatem jako kryterium kwalifikujące odnośne przepisy prawa stanowionego albo orzeczenie sądowe muszą upoważniać organizację „bezpiecznej przystani" do określonego postępowania ([2]). Innymi słowy, wyjątku nie stosuje się tam, gdzie prawo tego nie reguluje. Ponadto wyjątek będzie stosowany tylko wtedy, gdy wyraźne upoważnienie jest sprzeczne z przestrzeganiem zasad „bezpiecznej przystani". Nawet wówczas wyjątek „jest ograniczony do zakresu koniecznego do zaspokojenia nadrzędnych, uzasadnionych interesów popartych takim upoważnieniem". Dla przykładu, w przypadku gdy prawo po prostu upoważnia przedsiębiorstwo do przekazywania informacji osobowych organom rządowym, wyjątek nie ma zastosowania. I odwrotnie, w przypadku gdy prawo wyraźnie upoważnia przedsiębiorstwo do przekazywania informacji osobowych organom rządowym bez zgody osoby fizycznej, stanowiłoby to „wyraźny upoważnienie" do działania w sposób sprzeczny z zasadami „bezpiecznej przystani". Alternatywnie, szczególne wyjątki od wymogów dotyczących twierdzącego ogłoszenia i zgody wchodziłyby w zakres wyjątku (ponieważ byłoby to równoważne z wyraźnym upoważnieniem do ujawnienia informacji bez ogłoszenia i zgody). Na przykład ustawa, która upoważnia lekarzy do przekazywania dokumentacji medycznej ich pacjentów urzędnikom służby zdrowia bez uprzedniej zgody pacjenta, może dopuszczać wyjątek od zasad ogłoszenia i wyboru. To upoważnienie nie zezwalałoby lekarzowi na udostępnienie tej samej dokumentacji medycznej zakładom opieki zdrowotnej lub komercyjnym farmaceutycznym laboratoriom badawczym, co wykraczałoby poza zakres celów upoważnionych z mocy prawa, a tym samym poza zakres wyjątku ([3]). Omawiane upoważnienie prawne może być „autonomicznym" upoważnieniem do wykonywania konkretnych czynności z informacjami osobowymi, ale jak pokazują podane niżej przykłady, należy się spodziewać, że będzie to wyjątek od prawa o szerszym zakresie, które zakazuje zbierania, wykorzystywania lub ujawniania informacji osobowych.

*Telecommunications Act z 1996 r.*

W większości przypadków zatwierdzone sposoby wykorzystywania danych są albo zgodne z wymaganiami dyrektywy i zasad, albo byłyby dozwolone przez jeden z pozostałych dopuszczalnych wyjątków. Na przykład sekcja 702 Telecommunications Act (skodyfikowana w 47 U. S. C. § 222) nakłada na operatorów telekomunikacyjnych obowiązek zachowania poufności informacji osobowych, które uzyskali w toku świadczenia swych usług na rzecz swoich klientów. Przepis ten wyraźnie zezwala operatorom telekomunikacyjnym na:

1) wykorzystywanie informacji o klientach w celu świadczenia usług telekomunikacyjnych, łącznie z publikacją spisów abonentów;

2) przekazywanie informacji o kliencie innym osobom na pisemny wniosek klienta; oraz

3) przekazywanie informacji o klientach w postaci zbiorczej.

([1]) Niedawne przeszukanie bazy danych Westlaw ujawniło 994 zgłoszonych procesów stanowych, które dotyczyły odszkodowań i pogwałcenia prywatności.

([2]) Dla wyjaśnienia, odnośny organ prawny nie będzie musiał wymieniać wprost zasad „bezpiecznej przystani".

([3]) Podobnie, lekarz w tym przykładzie nie może polegać na ustawowym upoważnieniu, w celu pominięcia prawa osoby fizycznej do wyrażenia sprzeciwu wobec marketingu bezpośredniego, przyznanego przez NZP 12. Zakres każdego wyjątku od „wyraźnego upoważnienia" jest z konieczności ograniczony do zakresu upoważnienia na podstawie odnośnego prawa.

Patrz 47 U. S. C. § 222 lit. c) pkt 1-3. Ustawa dopuszcza także wyjątek zezwalając operatorom telekomunikacyjnym na wykorzystanie informacji o kliencie:

1) do zapoczątkowania i świadczenia usług, wystawiania rachunków i inkasowania należności za nie;

2) do zabezpieczania się przed oszukańczym, niewłaściwym albo niezgodnym z prawem postępowaniem, oraz

3) do świadczenia telemarketingu, usług administracyjnych lub przekierowań w trakcie połączenia zapoczątkowanego przez klienta ([1]).

*Id.,* § 222 lit. d) pkt 1-3. Wreszcie, operatorzy telekomunikacyjni są zobowiązani do podawania wydawcom książek telefonicznych informacji ze spisu abonentów, która może zawierać tylko imiona i nazwiska, adresy, numery telefonów i rodzaj działalności w przypadku klientów komercyjnych., *Id.,* § 222 lit. e).

Wyjątek na rzecz „wyraźnego upoważnienia" może wchodzić w grę w przypadku gdy operatorzy telekomunikacyjni stosują CPNI w celu zapobieżenia oszustwu lub innemu bezprawnemu postępowaniu. Nawet w tym przypadku takie działania można by zakwalifikować jako podejmowane w „interesie publicznym" i z tego powodu dozwolone przez zasady.

*Zasady proponowane przez Department of Health and Human Services*

Department of Health and Human Services, HHS (Departament Zdrowia i Usług Społecznych) zaproponował zasady odnoszące się do norm ochrony prywatności informacji zdrowotnych identyfikowalnych osobowo. Patrz: 64 Fed. Reg. 59.918 (dnia 2 listopada 1999 r.) (do skodyfikowania w 45 C. F. R. pkt 160-164). Zasady wprowadzałyby w życie wymagania dotyczące ochrony prywatności, wynikające z Health Insurance Portability and Accountability Act (Ustawy o przenoszeniu i odpowiedzialności za ubezpieczenia zdrowotne)z 1996 r., Pub. L. 104-191. Proponowane zasady generalnie zakazywałyby podmiotom im podległym (tj. programom zdrowotnym, bankom informacji zdrowotnej i zakładom opieki zdrowotnej, które przekazują informacje medyczne w formie elektronicznej) wykorzystywania albo ujawniania chronionych informacji medycznych bez indywidualnego upoważnienia. Patrz: proponowane 45 C. F. R. § 164.506. Proponowane zasady wymagałyby ujawnienia chronionych informacji zdrowotnych jedynie w dwóch celach: 1) w celu umożliwienia osobom fizycznym zapoznania się i skopiowania informacji zdrowotnych ich dotyczących. Patrz: *Id.,* w § 164.514; oraz 2) w celu wprowadzenia w życie zasad. Patrz: *Id.,* w § 164.522.

Proponowane zasady pozwoliłyby na wykorzystanie lub ujawnienie w ograniczonych przypadkach chronionych informacji zdrowotnych bez wyraźnego upoważnienia osoby fizycznej. Do przypadków takich należy na przykład nadzór nad systemem opieki zdrowotnej, egzekwowanie prawa oraz nagłe przypadki. Patrz: *Id.,* w § 164510. Proponowane zasady określają szczegółowo granice takiego wykorzystania i ujawnienia. Ponadto dozwolone wykorzystanie i ujawnienie chronionych informacji zdrowotnych byłoby ograniczone do niezbędnego minimum koniecznych informacji. *Patrz id.,* w § 164506.

Dopuszczalne przez proponowane regulacje sposoby korzystania z informacji na mocy wyraźnego upoważnienia są w zasadzie zgodne z zasadami „bezpiecznej przystani" lub są dopuszczalne innym wyjątkiem. Na przykład organy przestrzegania prawa i organy sądowe są dopuszczalne tak jak badania w zakresie medycyny. Wykorzystanie informacji w inny sposób, taki jak nadzór nad systemem opieki zdrowotnej, funkcje związane ze zdrowiem publicznym oraz rządowe systemy danych zdrowotnych służą interesowi publicznemu. Ujawnienia dokonywane w celu obsługi płatności za opiekę zdrowotną i płatności składek ubezpieczeniowych są konieczne dla zapewnienia opieki zdrowotnej. Wykorzystanie w nagłych przypadkach w celu zasięgnięcia opinii najbliższej rodziny w sprawie leczenia, w przypadku gdy zgoda pacjenta „nie może być w sposób wykonalny i rozsądny uzyskana" albo w celu ustalenia tożsamości lub przyczyny śmierci zmarłego, chroni żywotne interesy osób, których dane dotyczą i osób trzecich. Wykorzystanie danych w celu zarządzania żołnierzami w służbie czynnej i innymi specjalnymi grupami osób fizycznych pomaga we właściwej realizacji zadań wojskowych i w podobnych wymagających sytuacjach; a w każdym przypadku takie wykorzystanie będzie tylko w niewielkim stopniu miało zastosowanie do ogółu konsumentów, jeśli będzie ich dotyczyć w ogóle.

Pozostaje tylko wykorzystanie informacji osobowych przez zakłady opieki zdrowotnej do tworzenia spisów pacjentów. Wprawdzie takie wykorzystanie może nie sięgać poziomu „żywotnych" interesów, jednak spisy przynoszą korzyść pacjentom oraz ich przyjaciołom i bliskim. Także ten zakres dozwolonego wykorzystania jest z natury

([1]) Zakres tego wyjątku jest bardzo ograniczony. Zgodnie z jego warunkami, operator telekomunikacyjny może stosować CPNI wyłącznie podczas połączenia zainicjowanego przez klienta. Ponadto FTC poinformowała nas, że operatorowi telekomunikacyjnemu nie wolno stosować CPNI do oferowania usług wychodzących poza zakres zapytania klienta. Wreszcie, ponieważ klient musi wyrazić zgodę na zastosowanie CPNI w tym celu, przepis ten właściwie wcale nie jest „wyjątkiem".

ograniczony. Dlatego też stosowanie wyjątku od zasad do celów, do których odnosi się „wyraźne upoważnienie" przyznane na mocy prawa stwarza minimalne ryzyko dla prywatności pacjentów.

*Fair Credit Reporting Act (Ustawa o rzetelnej sprawozdawczości kredytowej)*

Komisja Europejska wyraziła zaniepokojenie, że wyjątek „wyraźnego upoważnienia" mógłby „faktyczne stworzyć konieczność ustalania adekwatności" dla Fair Credit Reporting Act (Ustawy o rzetelnej sprawozdawczości kredytowej). Taka sytuacja nie mogłaby mieć miejsca. W przypadku braku szczególnego ustalenia dotyczącego adekwatności dla FCRA, amerykańskie organizacje, które w przeciwnym przypadku polegałyby na takim ustaleniu, musiałyby zobowiązać się do pełnego przestrzegania zasad „bezpiecznej przystani". Oznacza to, że w przypadku gdy wymagania FCRA przekraczają poziom ochrony zawarty w zasadach, organizacje amerykańskie muszą przestrzegać tylko przepisów FCRA. W sytuacji odwrotnej, w przypadku gdy wymagania FCRA byłyby niewystarczające, wówczas organizacje musiałyby dostosować swoje praktyki postępowania z informacjami do zasad. Wyjątek nie zmieniłby tej podstawowej oceny. Zgodnie z zawartymi w nim warunkami stosuje się go tylko w przypadku gdy prawo wyraźnie upoważnia do postępowania, które byłoby niezgodne z zasadami „bezpiecznej przystani". Wyjątek nie obejmowałby przypadków, w których wymagania FCRA jedynie w nieznacznym stopniu nie spełniają zasad „bezpiecznej przystani" ([1]).

Inaczej mówiąc, naszą intencją nie jest utożsamianie wyjątku z założeniem, że jeżeli coś nie jest wymagane, to jest ono „wyraźnie upoważnione". Ponadto wyjątek stosuje się tylko wtedy, gdy wyraźne upoważnienie przez prawo amerykańskie jest sprzeczne z wymaganiami zasad „bezpiecznej przystani". Odnośne prawo musi spełnić oba te kryteria, zanim dozwolone zostanie odstępstwo od zasad.

Sekcja 604 FCRA wyraźnie upoważnia na przykład agencje sporządzające sprawozdania dotyczące konsumentów do publikowania sprawozdań dotyczących konsumpcji w poszczególnych określonych sytuacjach. *Patrz* FCRA, § 604. Jeżeli przy tym sekcja 604 upoważnia agencje sporządzające sprawozdania dotyczące kredytów do działania sprzecznego z zasadami „bezpiecznej przystani", wówczas agencje te musiałyby opierać się na wyjątku (o ile, oczywiście, nie miałby zastosowania jakiś inny wyjątek). Agencje sporządzające sprawozdania dotyczące kredytów muszą stosować się do nakazów sądowych i wezwań wielkiej ławy przysięgłych, a wykorzystanie sprawozdań przez rządowe organy przestrzegania prawa działające w zakresie udzielania zezwoleń, opieki społecznej i pomocy dzieciom służy interesowi publicznemu. *Id.,* § 604 lit. a) pkt 1, pkt 3 lit. D, i pkt 4). Zatem, agencja sporządzająca sprawozdania dotyczące kredytów nie musiałaby polegać na wyjątku „wyraźnego upoważnienia" dla tych celów. W przypadku gdy działa zgodnie z pisemnymi dyspozycjami konsumenta, agencja sporządzająca sprawozdania dotyczące konsumentów pozostawałaby całkowicie w zgodzie z zasadami „bezpiecznej przystani". *Id.,* § 604 lit. a) pkt 2. Podobnie sprawozdania o konsumentach mogą być zdobywane do celów związanych z zatrudnieniem tylko za pisemnym upoważnieniem konsumenta. (*id.,* § 604 lit. a) pkt 3 lit. B) i lit. b) pkt 2 lit. A) pkt ii)), a także do transakcji kredytowych i ubezpieczeniowych nie inicjowanych przez konsumenta, tylko w przypadku gdy konsument nie wyraził sprzeciwu na otrzymywanie takich ofert. (*id.,* § 604 lit. c) pkt 1 lit. B)). FCRA zakazuje także agencjom sporządzającym sprawozdania dotyczące kredytów przekazywania informacji zdrowotnych bez zgody konsumenta do celów związanych z zatrudnieniem. *Id.,* § 604 lit. g). Takie sposoby wykorzystania są zgodne z zasadami ogłoszenia i wyboru. Inne cele, do których upoważnia sekcja 604, dotyczą transakcji z udziałem konsumenta i z tego powodu mogą być dozwolone przez zasady. Patrz: *id.,* § 604 lit. a) pkt 3 lit. A) i F).

Pozostałe sposoby wykorzystania, do których „upoważnia" sekcja 604 dotyczą wtórnych rynków kredytowych. *Id.,* § 604 lit. a) pkt 3 lit. E). Nie ma sprzeczności między wykorzystaniem raportów o konsumentach do tego celu a zasadami „bezpiecznej przystani" *per se*. Prawdą jest, że FCRA nie wymaga od agencji sporządzającej sprawozdania dotyczące kredytów na przykład ogłoszenia i otrzymywania zgody konsumentów, gdy publikują sprawozdania do tych celów. Jednakże należy podkreślić raz jeszcze, że brak wymogu nie stanowi „wyraźnego upoważnienia" do działania w inny sposób niż jest to wymagane. Podobnie, sekcja 608 pozwala agencjom sporządzającym sprawozdania dotyczące kredytów przekazywać niektóre informacje osobowe agencjom rządowym. „Upoważnienie" to nie usprawiedliwiałoby ignorowania przez agencję sporządzającą sprawozdania dotyczące kredytów jej zobowiązań do przestrzegania zasad „bezpiecznej przystani". Kontrastuje to z innymi naszymi przykładami, w których wyjątki od wymagań dotyczących twierdzącego ogłoszenia i wyboru działają w ten sposób, że wyraźnie upoważniają do wykorzystania informacji osobowych bez ogłoszenia i wyboru.

*Wnioski*

Nawet z ograniczonego przeglądu wyżej wymienionych ustaw wyłania się wyraźny schemat:

— „Wyraźne upoważnienie" przewidziane prawem zasadniczo pozwala na wykorzystanie i ujawnienie informacji osobowej bez uprzedniej zgody osoby fizycznej; zatem wyjątek byłby ograniczony do zasad ogłoszenia i wyboru.

([1]) Z tych rozważań nie należy wyciągać wniosku, że FCRA nie zapewnia „adekwatnej" ochrony. Każda ocena niniejszej ustawy musi uwzględniać ochronę zapewnianą przez jej pełny tekst, a nie skupiać się tylko na wyjątkach, tak jak czynione jest tutaj.

— W większości przypadków wyjątki dopuszczone przez prawo są ściśle określone do stosowania w szczególnych sytuacjach dla szczególnych celów. We wszystkich przypadkach, w innych sytuacjach prawo zakazuje nieuprawnionego wykorzystania albo ujawniania informacji osobowych, które nie mieszczą się w tych granicach.

— W większości przypadków odzwierciedlających ich charakter legislacyjny, dozwolone wykorzystanie albo ujawnienie służy interesowi publicznemu.

— Prawie we wszystkich przypadkach uprawnione sposoby wykorzystania są albo w pełni zgodne z zasadami „bezpiecznej przystani" albo mieszczą się w granicach innych dopuszczalnych wyjątków.

Podsumowując, wyjątek „wyraźnego upoważnienia" przewidziany w prawie będzie z natury rzeczy miał raczej ograniczony zakres.

C. **Łączenie się i przejęcia przedsiębiorstw**

Grupa robocza ustanowiona w art. 29 wyraziła zaniepokojenie sytuacjami, do jakich dochodzi w przypadku gdy organizacja będąca członkiem „bezpiecznej przystani" zostaje przejęta albo łączy się z przedsiębiorstwem, które nie zobowiązało się do przestrzegania zasad „bezpiecznej przystani". Wydaje się jednak, że grupa robocza przyjęła, iż przedsiębiorstwo pozostające na rynku nie byłoby zobowiązane do stosowania zasad „bezpiecznej przystani" w odniesieniu do informacji przechowywanych przez przejętą firmę, ale zgodnie z amerykańskim prawem niekoniecznie tak musi się zdarzyć. Generalna zasada w Stanach Zjednoczonych dotycząca połączeń i przejęć mówi, że przedsiębiorstwo, które nabywa akcje będące w obrocie publicznym innego przedsiębiorstwa zasadniczo przejmuje odpowiedzialność i zobowiązania przejmowanej firmy. *Patrz 15 Fletcher Cyclopedia of the Law of Private Corporations* § 7117, 1990; *patrz także: Model Bus Corp*. Act § 11.06 ust. 3, (1979) („przedsiębiorstwo pozostałe po połączeniu posiada wszystkie zobowiązania każdego przedsiębiorstwa będącego stroną połączenia"). Innymi słowy, zgodnie z powyższym przedsiębiorstwo pozostające na rynku po połączeniu albo przejęciu organizacji „bezpiecznej przystani" będzie związane zobowiązaniami dotyczącymi „bezpiecznej przystani" tego ostatniego.

Ponadto nawet, jeżeli do połączenia albo przejęcia doszło w wyniku nabycia aktywów, zobowiązania nabytego przedsiębiorstwa mogą pomimo to w pewnych okolicznościach wiązać nabywcę. 15 Fletcher § 7122. Jednakże nawet w przypadku gdy zobowiązania ustaną po połączeniu, warto zaznaczyć, że ustałyby one także po połączeniu, gdy dane byłyby przekazane z Europy zgodnie z umową — co jest jedyną realną alternatywą „bezpiecznej przystani" w przypadku przekazywania danych do Stanów Zjednoczonych. Ponadto, po ostatnich zmianach dokumenty „bezpiecznej przystani" wymagają, żeby każda organizacja „bezpiecznej przystani" zawiadamiała Departament Handlu o wszystkich przejęciach i zezwalają na dalsze przekazywanie danych do nowo powstałej organizacji pod warunkiem że przystąpi ona do „bezpiecznej przystani". Patrz NZP 6. Stany Zjednoczone istotnie zmieniły obecnie strukturę „bezpiecznej przystani" i wymagają od organizacji amerykańskich w takiej sytuacji usunięcia informacji, jaką otrzymały w ramach „bezpiecznej przystani", jeżeli zobowiązania „bezpiecznej przystani" nie będą w dalszym ciągu przestrzegane lub, jeżeli nie zostaną zastosowane inne odpowiednie środki ochronne.

*ZAŁĄCZNIK V*

Dnia 14 lipca 2000 r.

John Mogg
Dyrektor, DG XV
Komisja Europejska
Biuro C 107–6/72
Rue de la Loi/Westraat 200
B—1049 Bruksela

Szanowny Panie Mogg,

Rozumiem, że w związku z moim listem przesłanym do Pana z dnia 29 marca 2000 r. powstało wiele wątpliwości. W celu wyjaśnienia kwestii naszych uprawnień w tych dziedzinach, w odniesieniu do których powstały te wątpliwości, przesyłam niniejszy list, uzupełniający i podsumowujący tekst dotychczasowej korespondencji w celu ułatwienia późniejszych odniesień.

W trakcie Pańskich wizyt w siedzibie naszego biura oraz w swojej korespondencji podniósł Pan kilka problemów dotyczących uprawnień Federalnej Komisji Handlu Stanów Zjednoczonych (FKH) w dziedzinie ochrony prywatności w systemie online. Myślę, że warto byłoby podsumować moje wcześniejsze odpowiedzi dotyczące działań FKH w tej dziedzinie i w odpowiedzi na poruszone przez Pana kwestie przekazać dodatkowe informacje o właściwości agencji w sprawach ochrony prywatności konsumentów. W szczególności pyta Pan czy: 1) FKH jest właściwa w zakresie przekazywania danych związanych z zatrudnieniem, jeżeli jest ono dokonywane z naruszeniem amerykańskich zasad „bezpiecznej przystani"; 2) FKH jest właściwa w zakresie programów ochrony prywatności typu non — profit opartych na zezwoleniu; 3) FTC Act (Ustawa o FKH) stosuje się jednakowo do systemu online jak i offline; oraz 4) co dzieje się, gdy właściwość FKH nakłada się na kompetencje innych organów przestrzegania prawa.

*Stosowanie Ustawy o FKH w odniesieniu do ochrony prywatności*

Jak Panu wiadomo, w ciągu ostatnich pięciu lat FKH przyjęła wiodącą rolę we wspieraniu starań amerykańskiego przemysłu i grup konsumenckich w celu wypracowania całościowej odpowiedzi na problemy ochrony prywatności konsumentów, włącznie z zbieraniem i wykorzystywaniem informacji osobowych w Internecie. Poprzez publiczne warsztaty i ciągłe konsultacje z członkami branży, przedstawicielami konsumentów i naszymi kolegami w Departamencie Handlu oraz Rządem Stanów Zjednoczonych, pomogliśmy wskazać kluczowe kwestie polityki i opracować rozsądne rozwiązania.

Uprawnienia Federalnej Komisji Handlu w tej dziedzinie określone są w sekcji 5 Ustawy o Federalnej Komisji Handlu („Ustawa o FKH"), która zakazuje „nieuczciwych lub wprowadzających w błąd czynów lub praktyk" handlowych albo wpływających na handel [1]. „Praktyka wprowadzająca w błąd" zdefiniowana jest jako podanie informacji, zaniechanie lub działanie, które może w istotny sposób wprowadzić w błąd rozsądnego konsumenta. Praktyka jest nieuczciwa, jeżeli powoduje albo może powodować u konsumentów znaczną szkodę, której w sposób rozsądny nie da się uniknąć, a której jednocześnie nie równoważą korzyści osiągane przez konsumentów lub konkurencję [2].

Niektóre praktyki zbierania informacji mogą naruszyć Ustawę o FKH. Na przykład, jeżeli w witrynie internetowej fałszywie informuje się, że jej właściciel przestrzega podanej polityki ochrony prywatności lub zestawu samoregulacyjnych wytycznych, sekcja 5 Ustawy o FKH zapewnia prawną podstawę zaskarżenia takiego podania fałszywych informacji jako wprowadzenia w błąd. Udało nam się wprowadzić w życie ustawę w celu ustanowienia tej zasady [3]. Ponadto Komisja stanęła na stanowisku, że może zaskarżać szczególnie rażące praktyki dotyczące ochrony prywatności jako nieuczciwe na podstawie sekcji 5, jeżeli praktyki takie dotyczą dzieci albo wykorzystania informacji wysoce wrażliwych, takich jak dokumentacja finansowa [4] i medyczna. Federalna Komisja Handlu będzie w dalszym ciągu, tak jak dotychczas to czyniła, wykonywać tego rodzaju działania na rzecz zapewniania prawu skuteczności poprzez nasze aktywne działania nadzorcze i śledcze, a także dzięki wnioskom, jakie otrzymujemy od instytucji samoregulacji i innych, w tym Państw Członkowskich Unii Europejskiej.

---

[1] 15 U. S. C. § 45. Fair Credit Reporting Act (Ustawa o rzetelnej sprawozdawczości kredytowej) odnosiłaby się także do zbierania w Internecie i sprzedaży odpowiadającej ustawowym definicjom „sprawozdania o konsumentach" i „agencji sporządzającej sprawozdania dotyczące konsumentów".

[2] 15 U. S. C. § 45 lit. n).

[3] Patrz: GeoCities, nr rej. C-3849 (orzeczenie ostateczne z 12.2.1999) (dostępne pod adresem www.ftc.gov/os/1999/9902/9823015d %26o.htm); Liberty Financial Cos., nr rej. C-3891 (orzeczenie ostateczne z 12.8.1999) (dostępne pod adresem www.ftc.gov/opa/1999/9905/younginvestor.htm). Patrz także: Children's Online Privacy Protection Act Rule, COPPA (przepis Ustawy o ochronie prywatności dzieci w systemie online), 16 C. F. R. Część 312 (dostępny pod adresem www.ftc.gov/opa/1999/9910/childfinal.htm). Przepis ustawy COPPA, który stał się skuteczny w zeszłym miesiącu, wymaga od operatorów witryn internetowych skierowanych do dzieci poniżej 13 roku życia lub tych, które świadomie zbierają informacje osobowe od dzieci poniżej 13 roku życia, wprowadzenia w życie norm uczciwej praktyki informacyjnej zawartych w przepisie.

[4] Patrz: FTC przeciwko Touch Tone Inc., Pozew cywilny nr 99-WM-783 (D. Co.) (złożony dnia 21 kwietnia 1999 r.) pod adresem www.ftc.gov/opa/1999/9904/touchtone.htm. Pismo interpretacyjne z dnia 17 lipca 1997 r. wydane w odpowiedzi na podanie złożone przez Center for Media Education, pod adresem www.ftc.gov/os/1997/9707/cenmed.htm.

*Wsparcie FKH dla samoregulacji*

Od dawna FKH wspiera starania branży zmierzające do opracowania skutecznych programów samoregulacji w celu zapewnienia klientom ochrony w Internecie. Jeżeli jednak starania te mają odnieść skutek, potrzebny jest masowy udział przedstawicieli branży. Jednocześnie samoregulacja musi mieć oparcie w organy przestrzegania prawa. Z tych powodów FKH da pierwszeństwo wnioskom dotyczącym nieprzestrzegania wytycznych samoregulacyjnych, otrzymywanym od takich podmiotów jak BBBOnline i TRUSTe. To podejście będzie spójne z naszymi wieloletnimi powiązaniami z National Advertising Review Board, NARB (Krajową Radą Przeglądu Reklamy) Better Business Bureau, która kieruje skargi dotyczące reklamy do FKH. National Advertising Division, NAD (Krajowy Oddział ds. Reklamy) NARB rozpatruje skargi dotyczące krajowej reklamy w trybie postępowania kontradyktoryjnego. Gdy jedna ze stron odmawia podporządkowania się decyzji NAD, sprawa jest kierowana do FKH. Pracownicy FKH zaskarżoną reklamę poddają analizie w trybie pilnym, żeby stwierdzić, czy narusza ona Ustawę o FKH i często udaje im się wstrzymać zaskarżone działanie albo przekonać daną stronę, aby powróciła na drogę postępowania wyznaczoną przez NARB.

Podobnie, FKH nada pierwszeństwo wnioskom pochodzącym z Państw Członkowskich UE w sprawach o nieprzestrzeganie zasad „bezpiecznej przystani". Podobnie jak w przypadku wniosków amerykańskich instytucji samoregulacji, nasi pracownicy rozważą każdą informację mającą związek z tym, czy zaskarżone postępowanie narusza sekcję 5 Ustawy o FKH. Zobowiązanie takie znajduje się także w zasadach „bezpiecznej przystani" w najczęściej zadawanych pytaniach (NZP 11) w sprawie zapewniania prawu skuteczności

*GeoCities: pierwsza prowadzona przez FKH sprawa o ochronie prywatności w systemie online*

Pierwsza prowadzona przez Federalną Komisję Handlu sprawa dotycząca ochrony prywatności w sieci, tj. sprawa GeoCities, opierała się na uprawnieniach Komisji wynikających z sekcji 5 [1]. W tym przypadku FKH zarzuciła GeoCities podawanie fałszywych informacji zarówno dorosłym, jak i dzieciom o tym, w jaki sposób zostaną użyte ich informacje osobowe. Skarga Federalnej Komisji Handlu stwierdzała, że GeoCities podała informację, iż określone informacje identyfikujące osobowo zbierane na stronach internetowych, miały być wykorzystane jedynie do wewnętrznych celów lub po to, żeby przekazywać konsumentom szczególne oferty reklamowe oraz żądane przez nich produkty i usługi, a także że niektóre dodatkowe, pozostawione klientowi do wyboru, informacje nie zostaną ujawnione nikomu bez jego zgody. W rzeczywistości, informacje te zostały ujawnione stronom trzecim, które wykorzystywały je w celu skierowania do członków grupy docelowej ofert wykraczających poza to, na co ci wyrazili zgodę. W skardze zarzucono też GeoCities, że uprawiała wprowadzające w błąd praktyki dotyczące zbierania przez nią informacji od dzieci. Zgodnie z treścią skargi FKH, GeoCities podawała informację o utrzymywaniu na swoich stronach internetowych miejsca przeznaczonego dla dzieci, w którym zebrane informacje były przechowywane przez GeoCities. W rzeczywistości operatorem tych obszarów na stronach internetowych były strony trzecie, które zbierały i przechowywały informacje.

Ugoda zabrania GeoCities podawania fałszywych informacji w zakresie celu, w jakim zbiera ona od konsumentów albo o konsumentach, łącznie z dziećmi, informacje identyfikujące osobowo lub w jakim celu je wykorzystuje. Zgodnie z nakazem spółka musi umieścić w swojej witrynie internetowej jednoznaczne, dobrze widoczne zawiadomienie o ochronie prywatności, mówiące konsumentom, jakie informacje są zbierane i w jakim celu, komu będą ujawnione, w jaki sposób konsumenci mogą uzyskać do nich dostęp oraz usunąć je. W celu zapewnienia kontroli rodzicielskiej ugoda nakłada także na GeoCities obowiązek uzyskania zgody rodziców przed zbieraniem od dzieci poniżej 12 roku życia informacji identyfikujących osobowo. Zgodnie z nakazem GeoCities musi uprzedzać swoich członków i dać im możliwość usunięcia informacji o sobie z baz danych GeoCities oraz wszelkich stron trzecich. Ugoda wyraźnie nakłada na GeoCities obowiązek ogłaszania rodziców dzieci w wieku lat 12 i młodszych oraz usuwania informacji o nich, o ile rodzic nie wyrazi zgody na zachowanie i wykorzystanie danych. Wreszcie, GeoCities musi także skontaktować się ze stronami trzecimi, którym wcześniej ujawniła informacje i zażądać także od nich usunięcia tych informacji [2].

*ReverseAuction.com*

Ostatnio nasza agencja wniosła sprawę przeciwko naruszeniu prywatności przez inną spółkę działającą w systemie online. W styczniu 2000 r. Komisja uznała skargę przeciwko ReverseAuction. Com, witryną WWW prowadząca aukcje w sieci, i zaakceptowała ugodę w związku z domniemanym pozyskiwaniem przez nią informacji identyfikujących osobowo o konsumentach od konkurencyjnej witryny (eBay.com), a następnie wysyłała podstępnie niezamówione wiadomości drogą elekroniczną do tych konsumentów w celach handlowych [3].Wskardzezarzuciliśmy ReverseAuction naruszenie przepisów sekcji 5 Ustawy o FKH przez

---

[1] GeoCities, nr rejestracyjny C-3849 (orzeczenie ostateczne z 12.2.1999 — dostępne pod adresem www.ftc.gov/os/1999/9902/9823015d %26o.htm).

[2] Komisja następnie doprowadziła do ugody w innej sprawie, dotyczącej zbierania w sieci informacji osobowych od dzieci. Liberty Financial Companies, Inc., była operatorem witryny internetowej Young Investor skierowanej do dzieci i nastolatków, a jej działalność skupiała się na kwestiach związanych z pieniędzmi i inwestowaniem. Komisja zarzuciła spółce podawanie fałszywych informacji, iż informacje osobowe zebrane od dzieci w ankiecie pozostaną anonimowe oraz że do uczestników zostanie przesłany pocztą elektroniczną biuletyn informacyjny i nagrody. W rzeczywistości, informacje osobowe na temat dzieci i sytuacji finansowej ich rodziny były przechowywane w sposób pozwalający na ustalenie tożsamości, a żadnego biuletynu informacyjnego ani nagród nie wysłano. Ugoda zabrania takiego wprowadzania w błąd w przyszłości i żąda od Liberty Financial zamieszczenia informacji o ochronie prywatności w swoich witrynach internetowych skierowanych do dzieci, a także uzyskania możliwej do sprawdzenia zgody rodziców przed zbieraniem od dzieci informacji identyfikujących osoby. Liberty Financial Cos., nr rejestracyjny C-3891 (orzeczenie ostateczne z 12.8.1999). (dostępne pod adresem ww.ftc.gov/opa/1999/9905/younginvestor.htm).

[3] Patrz: ReverseAuction.com, Inc., Civil Action (pozew cywilny) nr 000032 (D. D. C.) (złożony w dniu 6 stycznia 2000 r.) (informacje prasowe i wystąpienia stron pod adresem www.ftc.gov/opa/2000/01/reverse4.htm).

pozyskiwanie indywidualnie identyfikujących informacji osobowych, obejmujących adresy e-mail: użytkowników eBay i spersonalizowane nazwy użytkowników („nazwy użytkownika") oraz przez wysyłanie wprowadzających w błąd wiadomości e-mail:.

Jak przedstawiono w skardze, przed pozyskaniem informacji ReverseAuction zarejestrowała się jako użytkownik eBay i zgodziła się przestrzegać „Umowy użytkownika eBay" oraz jej „polityki ochrony prywatności". Umowa i polityka chronią prywatność konsumentów w ten sposób, że zabraniają użytkownikom eBay gromadzenia i wykorzystywania informacji identyfikujących osobowo w niedozwolonych celach, takich jak wysyłanie niezamówionych komercyjnych wiadomości e-mail:. Zatem w naszej skardze, po pierwsze, zarzuciliśmy ReverseAuction podawanie fałszywych informacji, że będzie przestrzegać „Umowy użytkownika eBay" i jej „polityki ochrony prywatności", co zgodnie z sekcją 5 stanowi wprowadzającą w błąd praktykę. Alternatywnie, w skardze zarzucono ReverseAuction, że wykorzystanie przez nią tych informacji do wysyłania niezamówionych komercyjnych wiadomości e-mail: z naruszeniem „Umowy użytkownika" i „polityki ochrony prywatności" stanowiło, zgodnie z sekcją 5, nieuczciwą praktykę handlową.

Po drugie, w skardze twierdzono, że w tytule wysyłanych do konsumentów wiadomości e-mail: umieszczano wprowadzający w błąd wiersz, w którym informowano każdego z konsumentów, że jego nazwa użytkownika eBay „wkrótce straci ważność". Ostatni z zarzutów skargi na ReverseAuction dotyczył nieprawdziwych informacji zawartych w wiadomościach e-mail: mówiących o tym, że eBay bezpośrednio albo pośrednio dostarczyła ReverseAuction informacje identyfikowalne osobowo albo w inny sposób brała udział w rozpowszechnianiu niezamówionych wiadomości e-mail:.

Ugoda uzyskana przez FKH zabrania ReverseAuction dopuszczania się powyższych naruszeń w przyszłości. Wymaga także od, ReverseAuction aby zawiadomiła konsumentów, którzy w wyniku otrzymania wiadomości e-mail: od ReverseAuction zarejestrowali się lub zarejestrują w ReverseAuction. Zawiadomienie informuje tych konsumentów, że ich nazwy użytkowników eBay nie miały w najbliższej przyszłości stracić ważności w witrynie eBay oraz, że eBay nie wiedziała o rozsyłaniu przez ReverseAuction niezamówionej poczty e-mail: ani na to nie zezwoliła. Zawiadomienie umożliwia także tym konsumentom anulowanie rejestracji w ReverseAuction i nakazanie usunięcia informacji identyfikujących osobowo z bazy danych ReverseAuction. Ponadto nakaz wymaga, żeby ReverseAuction skasowała i powstrzymała się od użycia lub ujawniania informacji identyfikujących osobowo członków eBay, którzy otrzymali wiadomości e-mail: od ReverseAuction, lecz którzy nie zarejestrowali się w ReverseAuction. Wreszcie, podobnie jak w przypadku wcześniejszych nakazów dotyczących ochrony prywatności uzyskanych przez naszą agencję, ugoda wymaga od ReverseAuction ujawnienia własnej polityki ochrony prywatności w jej witrynie internetowej i zawiera całościowe przepisy dotyczące przechowywania dokumentacji, co ma umożliwić FKH nadzór nad przestrzeganiem.

Sprawa ReverseAuction pokazuje, że FKH zdecydowana jest wykorzystywać zapewnianie skuteczności prawa do popierania samoregulacyjnych wysiłków branży w dziedzinie ochrony prywatności konsumenta w sieci. Sprawa ta rzeczywiście bezpośrednio zakwestionowała działanie, które podważało „politykę ochrony prywatności" i „Umowę z użytkownikiem" chroniące prywatność konsumentów, i które mogło zachwiać wiarę konsumenta w środki ochrony prywatności podejmowane przez spółki działające w systemie online. Ponieważ w tym przypadku chodziło o przywłaszczenie sobie przez jedno przedsiębiorstwo informacji o konsumentach chronionych przez politykę prywatności innego, sprawa ta może mieć znaczenie dla wyjaśnienia wątpliwości powstających przy przekazywaniu danych między przedsiębiorstwami w różnych krajach.

Bez względu na działania zapewniające prawu skuteczność prowadzone przez Federalną Komisję Handlu w odniesieniu do GeoCities, Liberty Financial Cos. i ReverseAuction uprawnienia agencji w niektórych obszarach ochrony prywatności w systemie online są bardziej ograniczone. Jak stwierdzono powyżej, aby móc postawić dany podmiot w stan oskarżenia na podstawie Ustawy o FKH, zbieranie i wykorzystanie informacji osobowych bez zgody zainteresowanych musi stanowić wprowadzającą w błąd albo nieuczciwą praktykę handlową. Zatem Ustawa o FKH raczej nie zajęłaby się praktykami witryny internetowej, która zbierała informacje identyfikowalne osobowo od konsumentów, ale ani nie wprowadzała w błąd w zakresie celu, dla jakiego zbierała informacje, ani nie używała lub nie ujawniała informacji w sposób mogący spowodować istotną szkodę dla konsumentów. Podobnie FKH nie może mieć prawa do wprowadzenia powszechnego wymogu, aby jednostki zbierające informacje w Internecie przestrzegały określonej lub jakiejkolwiek polityki ochrony prywatności ([1]). Jak jednak stwierdzono powyżej, nieprzestrzeganie przez spółkę ogłoszonej przez siebie polityki ochrony prywatności będzie miało wszelkie cechy wprowadzającej w błąd praktyki.

---

([1]) Z tego powodu Federalna Komisja Handlu w swoim zeznaniu przed Kongresem stwierdziła, że prawdopodobnie będzie potrzebna dodatkowa ustawa, żeby zobowiązać wszystkie amerykańskie komercyjne witryny internetowe skierowane do konsumentów do przestrzegania określonych uczciwych praktyk informacyjnych („Prywatność konsumentów w sieci WWW". — zeznanie przed Podkomitetem ds. Telekomunikacji, Handlu i Ochrony Konsumentów senackiego Komitetu Izby Reprezentantów USA ds. handlu, dnia 21 lipca 1998 r. Z zeznaniem można zapoznać się pod adresem www.ftc.gov/os/9807/privac98.htm). FTC wstrzymywała wezwanie do tworzenia takiego ustawodawstwa po to, żeby dać działaniom samoregulującym możliwość pokazania, że uczciwe praktyki informacyjne zostały powszechnie przyjęte w witrynach internetowych. W sprawozdaniu Federalnej Komisji Handlu dla Kongresu na temat prywatności w sieci („Prywatność w sieci: Sprawozdanie dla Kongresu", czerwiec 1998; sprawozdanie znajduje się pod adresem www.ftc.gov/reports/privacy3/toc.htm) FTC zaleciła przyjęcie ustawodawstwa nakładającego na komercyjne witryny internetowe obowiązku uzyskania zgody rodziców przed zbieraniem informacji identyfikujących osobowo od dzieci poniżej 13 roku życia. Patrz: przypis 46 powyżej. W ubiegłym roku w sprawozdaniu „Samoregulacja i prywatność w sieci: Sprawozdanie Federalnej Komisji Handlu dla Kongresu", lipiec 1999 r. (sprawozdanie jest zamieszczone pod adresem www.ftc.gov/os/1999/9907/index.htm#13) Komisja stwierdziła, że są dostateczne postępy w działalności samoregulacyjnej, w związku z tym, nie zaleciła wówczas unormowań prawnych. W najbliższych tygodniach Komisja będzie znowu składać sprawozdanie Kongresowi na temat rozwoju samoregulacji.

Ponadto, właściwość FKH w tym obszarze obejmuje nieuczciwe bądź wprowadzające w błąd czyny lub praktyki tylko wtedy, gdy dotyczą one „handlu albo wpływają na handel". Zbieranie informacji przez podmioty prowadzące działalność gospodarczą, które promują produkty lub usługi, łącznie ze zbieraniem i wykorzystywaniem informacji do celów handlowych, prawdopodobnie spełnia wymaganie relewantności w handlu. Z drugiej strony wiele osób fizycznych lub podmiotów może zbierać w sieci informacje nie w celach handlowych i tym samym może znajdować się poza właściwością Federalnej Komisji Handlu. Przykładem takiego ograniczenia są „chat rooms" (pogawędki internetowe), jeżeli ich operatorem są podmioty nieprowadzące działalności gospodarczej, np. organizacje charytatywne.

Wreszcie, istnieje szereg pełnych albo częściowych wyjątków ustawowych od podstawowej właściwości FKH w sprawie praktyk handlowych, które ograniczają możliwość podjęcia przez FKH całościowych działań w odpowiedzi na podnoszone kwestie ochrony prywatności w Internecie. Obejmują one wyjątki dotyczące wielu dziedzin działalności, w których istnieje duże zapotrzebowanie na informacje o konsumentach, takich jak banki, zakłady ubezpieczeniowe i linie lotnicze. Jak Panu wiadomo, jednostki te podlegałyby właściwości innych federalnych bądź stanowych organów, takich jak federalne agencje ds. bankowości lub Departament Transportu

W przypadkach, gdy posiada ona właściwość, FKH przyjmuje i, w miarę jak zasoby jej na to pozwalają, podejmuje działania w sprawie skarg konsumentów otrzymywanych pocztą i telefonicznie w swoim Consumer Response Center („CRC"), a od niedawna w swojej witrynie internetowej ([1]). CRC przyjmuje skargi od wszystkich konsumentów, także od posiadających miejsce zamieszkania w Państwach Członkowskich Unii Europejskiej. Ustawa o FKH nadaje Federalnej Komisji Handlu uprawnienia do uzyskania opartego na prawie słuszności zabezpieczenia na wypadek

przyszłych naruszeń Ustawy o FKH, a także zadośćuczynienia dla pokrzywdzonych konsumentów. Sprawdzamy jednak, czy firma przyjęła stały wzorzec niewłaściwego postępowania, ponieważ nie rozstrzygamy indywidualnych sporów konsumenckich. W przeszłości Federalna Komisja Handlu zapewniała zadośćuczynienie obywatelom zarówno Stanów Zjednoczonych, jak i innych krajów ([2]). FKH będzie nadal wykorzystywała swoje uprawnienia we właściwych sprawach w celu zapewnienia zadośćuczynienia obywatelom innych krajów, którzy zostali pokrzywdzeni na skutek wprowadzających w błąd praktyk w obszarze podlegającym jej właściwości.

*Dane o zatrudnieniu*

Pański ostatni list wyrażał potrzebę uzyskania dodatkowych wyjaśnień dotyczących właściwości FKH w dziedzinie danych o zatrudnieniu. Po pierwsze, stawia Pan pytanie, czy FKH mogłaby podjąć działanie na podstawie sekcji 5 przeciwko spółce, która twierdzi, że przestrzega amerykańskich zasad „bezpiecznej przystani", ale przekazuje albo wykorzystuje dane o zatrudnieniu w sposób, który narusza te zasady. Chcemy Pana zapewnić, że dokładnie przeanalizowaliśmy przepisy, z których wynikają uprawnienia FKH, odnośne dokumenty oraz odpowiednie precedensy i doszliśmy do wniosku, że FKH posiada taką samą właściwość w sytuacjach dotyczących danych o zatrudnieniu, jakie ogólnie wynikają przepisów sekcji 5 Ustawy o FKH ([3]). Oznacza to, że zakładając, iż dana sprawa spełni nasze istniejące kryteria (nieuczciwość lub wprowadzenie w błąd) dotyczące podejmowania działań zapewniających prawu skuteczność w zakresie ochrony prywatności, moglibyśmy podjąć działania również w sytuacjach, dotyczących danych o zatrudnieniu.

Chcielibyśmy także położyć kres wszelkim opiniom, zgodnie z którymi zdolności FKH do podejmowania działań zapewniających prawu skuteczność w zakresie ochrony prywatności ograniczona jest do przypadków, gdy spółka oszukała indywidualnych konsumentów. W rzeczywistości, jak pokazują niedawne działania Komisji w sprawie ReverseAuction ([4]), FKH podejmie działania zapewniające prawu skuteczność związane z ochroną prywatności w sytuacjach związanych z przekazywaniem danych między przedsiębiorstwami w przypadku gdy istnieje domniemanie, że jedna firma postępowała bezprawnie wobec drugiej firmy, co mogło doprowadzić do pokrzywdzenia zarówno konsumentów, jak i firm. Przypuszczamy, że najbardziej prawdopodobne jest pojawienie się kwestii związanych z zatrudnieniem właśnie w tego typu sytuacjach, ponieważ dane o zatrudnieniu Europejczyków przekazywane są z firm europejskich do firm amerykańskich, które zobowiązały się przestrzegać zasad „bezpiecznej przystani".

Chcielibyśmy jednakże wskazać jedną okoliczność, w której działanie FKH byłoby ograniczone. Byłaby to sytuacja, w której sprawa jest skierowana do rozpatrzenia zgodnie z procedurą tradycyjnego rozstrzygania sporów w dziedzinie prawa pracy, najprawdopodobniej jako roszczenie zgłoszone w Komisji ds. zażaleń lub arbitrażowej albo skarga na nieuczciwą praktykę w ramach stosunku pracy do National Labor Relations Board (Krajowej Rady ds.

([1]) Internetowy formularz skargi do Federalnej Komisji Handlu można znaleźć pod adresem http://www.ftc.gov/ftc/complaint.htm.

([2]) W niedawnej sprawie internetowej piramidy finansowej Komisja uzyskała dla 15 622 konsumentów zwrot sumy w przybliżeniu, 5,5 miliona USD. Konsumenci, których to dotyczy, mieszkają w Stanach Zjednoczonych i 70 innych krajach. Patrz www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

([3]) Z wyjątkiem szczególnych wykluczeń ściśle określonych w ustawie o uprawnieniach FTC, właściwość FTC w odniesieniu do praktyk handlowych lub wpływających na handel jest zgodna z konstytucyjną władzą Kongresu na mocy Klauzuli Handlowej, Stany Zjednoczone przeciwko American Building Maintenance Industries, 422 U. S. 271 z 277 n. 6 (1975). Tak więc właściwość FTC obejmuje praktyki odnoszące się do zatrudnienia w firmach i branżach handlu międzynarodowego.

([4]) Patrz: „Online Auction Site Settles FTC Privacy Charges", FTC News Release (6.1.2000) dostępne pod adresem http://www.ftc.gov/opa/2000/01/reverse4.htm.

stosunków pracy). Taka sytuacja miałaby miejsce, na przykład, gdyby w układzie zbiorowym pracy pracodawca przyjął na siebie określone zobowiązanie dotyczące wykorzystania danych osobowych, a pracownik lub związek zgłosił skargę, że pracodawca złamał ten układ. Komisja prawdopodobnie wstrzymałaby się od udziału w tym postępowaniu ([1]).

*Właściwość w zakresie programów opartych na zezwoleniu*

Po drugie, pyta Pan, czy FKH byłaby właściwa w zakresie programów opartych na zezwoleniu administrujących mechanizmami rozstrzygania sporów w Stanach Zjednoczonych, które podały fałszywe informacje w zakresie swej roli w egzekwowaniu zasad „bezpiecznej przystani" i rozpatrywaniu indywidualnych skarg, nawet jeżeli takie podmioty są formalnie typu non — profit. Starając się określić, czy naszej właściwości podlega podmiot, który utrzymuje, że ma status non — profit, Komisja dokładnie analizuje, czy podmiot ten, nie osiągając zysku dla siebie, nie pomaga jednak w osiąganiu zysku swoim członkom. Komisji udało się objąć swoją właściwością takie podmioty i w dniu 24 maja 1999 r. Sąd Najwyższy Stanów Zjednoczonych w sprawie antytrustowej California Detal Association przeciwko Federalnej Komisji Handlu jednogłośnie potwierdził, że właściwość Komisji obejmuje dobrowolne stowarzyszenie lokalnych towarzystw dentystycznych typu non — profit. Sąd orzekł:

> FKH stara się o włączenie do ustawy nie tylko podmiotu „zorganizowanego w celu prowadzenia działalności gospodarczej dla osiągnięcia własnego zysku", 15 U. S. C. § 44, ale także takiego, który prowadzi działalność dla osiągnięcia zysku przez „swoich członków"..... Rzeczywiście trudno byłoby zakładać, że Kongres miał na myśli takie ograniczone pojęcie organizacji wspierających w powiązaniu z możliwością, jaką by to stwarzało do unikania właściwości tam, gdzie cele Ustawy o FKH w sposób oczywisty się jej domagają.

Podsumowując, stwierdzenie, że posiada się właściwość nad określonym podmiotem typu non — profit, administrującym programem opartym na zezwoleniu, wymagałoby rzeczowego przeglądu zakresu, w jakim dany podmiot przynosił korzyści gospodarcze swoim nastawionym na osiąganie zysku członkom. Jeżeli taki podmiot zarządzałby swoim programem opartym na zezwoleniu w sposób, który przynosiłby korzyści gospodarcze jego członkom, to FKH prawdopodobnie objąłby go swoją właściwością. Oddzielną sprawą jest to, że FKH prawdopodobnie posiadałaby właściwość nad oszukańczym programem opartym na zezwoleniu, który podaje fałszywe informacje w odniesieniu do swojego statusu jako podmiotu typu non — profit.

*Ochrona prywatności w systemie offline*

Po trzecie, zauważa Pan, że nasza wcześniejsza korespondencja skupiła się na prywatności w systemie online. Chociaż ochrona prywatności w systemie online stanowiła główny przedmiot zainteresowania FKH jako krytyczny element rozwoju elektronicznego handlu, Ustawa o FKH sięga swoim rodowodem roku 1914 i stosuje się w jednakowym stopniu do systemu offline. Tak więc możemy ścigać firmy działające w systemie offline, które stosują nieuczciwe albo wprowadzające w błąd praktyki handlowe w odniesieniu do prywatności konsumentów ([2]). Faktycznie, w sprawie wytoczonej przez Komisję w zeszłym roku, FKH przeciwko Touchtone Information, Inc. ([3]), „pośrednik w obrocie informacjami" został oskarżony o nielegalne uzyskanie i sprzedaż prywatnych informacji finansowych konsumentów. Komisja twierdziła, że Touch Tone uzyskała informacje o konsumentach przez „pozorowanie", co jest żargonowym terminem ukutym w prywatnej branży detektywistycznej dla opisania praktyki zdobywania informacji osobowych o innych osobach pod fałszywym pozorem, zwykle przez telefon. W pozwie wniesionym dnia 21 kwietnia 1999 r. do sądu federalnego stanu Kolorado Komisja domaga się wydania zakazu oraz zajęcia wszelkich bezprawnie uzyskanych korzyści.

*Nakładanie się właściwości*

Pana ostatnie pytanie dotyczy wzajemnego oddziaływania właściwością FKH i innych organów przestrzegania prawa w szczególności w przypadkach, gdy mamy do czynienia z możliwością nakładania się właściwości. Wypracowaliśmy bliskie stosunki robocze z wieloma innymi organami przestrzegania prawa, włącznie z federalnymi organami ds.

---

([1]) Ustalenie, czy postępowanie jest „nieuczciwą praktyką w ramach stosunku pracy", czy też stanowi pogwałcenie układu zbiorowego pracy ma charakter techniczny i jest zwykle zastrzeżone dla wyspecjalizowanych sądów pracy, które rozpoznają skargi, takich jak sady arbitrażowe i NRLB.

([2]) Jak Panu wiadomo z wcześniejszych dyskusji, Fair Credit Reporting Act (Ustawa o rzetelnej sprawozdawczości kredytowej) nadaje FTC także uprawnienia do ochrony prywatności finansowej konsumentów w granicach ustawy, a Komisja niedawno przyjęła decyzję dotyczącą tej sprawy. Patrz: In the Matter of Trans Union, nr rej. 9255 (z 1.3.2000) (informacja prasowa i opinia dostępne pod adresem www.ftc.gov/os/2000/03/index.htm#1).

([3]) Pozew cywilny 99-WM-783 (D. Colo.) (dostępny pod adresem www.ftc.gov/opa/1999/9904/touchtone.htm) (orzeczenie w sprawie tymczasowej zgody której termin obowiązywania jeszcze nie upłynął).

bankowości i stanowymi prokuratorami generalnymi. Bardzo często w przypadku nakładających się właściwości koordynujemy dochodzenie w celu wykorzystania naszych zasobów w maksymalnym stopniu. Często także przekazujemy sprawy do właściwych agencji federalnych albo stanowych, w celu przeprowadzenia przez nie dochodzenia.

Mam nadzieję, że niniejszy przegląd okaże się przydatny. Proszę mnie powiadomić, jeżeli będzie Pan potrzebował jakichkolwiek dalszych informacji.

Z poważaniem,

Robert Pitofsky

*ZAŁĄCZNIK VI*

John Mogg
Dyrektor, DG XV
Komisja Europejska
Biuro C 107–6/72
Rue de la Loi/Westraat 200
B—1049 Brussels

Szanowny Panie Dyrektorze Generalny Mogg,

Piszę do Pana niniejszy list na prośbę Departamentu Handlu USA, w celu wyjaśnienia roli Departamentu Transportu w ochronie prywatności konsumentów w związku z informacjami przekazywanymi przez nich liniom lotniczym.

Departament Transportu popiera samoregulację jako najbardziej pożądany i skuteczny środek służący zapewnieniu ochrony prywatności informacji przekazywanych liniom lotniczym przez konsumentów, a co za tym idzie, wspiera ustanowienie systemu „bezpiecznej przystani", który pozwoliłby liniom lotniczym postępować zgodnie z wymaganiami dyrektywy Unii Europejskiej w sprawie ochrony prywatności w odniesieniu do przekazywania informacji poza UE. Departament uznaje jednak, że w celu przynoszenia efektów przez wysiłki samoregulacyjne, niezbędne jest, aby linie lotnicze, które zobowiążą się do przestrzegania zasad prywatności przyjętych w systemie „bezpiecznej przystani", rzeczywiście się do nich stosowały. Z tego względu, samoregulacja powinna mieć poparcie ze strony organów przestrzegania prawa. Zatem, wykorzystując swoje istniejące uprawnienia ustawowe w zakresie ochrony konsumentów, Departament zapewni przestrzeganie przez linie lotnicze podjętych publicznie zobowiązań dotyczących ochrony prywatności oraz będzie rozpatrywał sprawy domniemanego ich nieprzestrzegania, które otrzymamy od instytucji samoregulacji i innych podmiotów, w tym Państw Członkowskich Unii Europejskiej.

Uprawnienie Departamentu do podejmowania działań zapewniających prawu skuteczność w tej dziedzinie wynika z 49 U. S. C 41712, który zakazuje przewoźnikowi przy sprzedaży lotniczych usług transportowych uprawiania „nieuczciwej lub wprowadzającej w błąd praktyki bądź nieuczciwej konkurencji", która jest albo może być przyczyną szkody dla konsumenta. Sekcja 41712 jest sformułowana na wzór sekcji 5 Ustawy o Federalnej Komisji Handlu (15 U. S. C. 45). Jednakże przewoźnicy lotniczy zostali wyłączeni z przepisów sekcji 5 przez Federalną Komisję Handlu na podstawie 15 U. S. C. 45 lit. a) pkt 2.

Moje biuro bada i kieruje do sądu sprawy na podstawie 49 U. S. C. 41712. Patrz: np. decyzje DOT 99–11–5, z dnia 9 listopada 1999 r.; 99–8–23, z dnia 26 sierpnia 1999 r.; 99–6–1, z dnia 1 czerwca 1999 r.; 98–6–24, z dnia 22 czerwca 1998 r.; 98–6–21, z dnia 19 czerwca 1998 r.; 98–5–31, z dnia 22 maja 1998 r.; i 97–12–23, z dnia 18 grudnia 1997 r.) Wszczynamy takie sprawy w oparciu o nasze własne dochodzenie, a także na podstawie formalnych i nieformalnych skarg, jakie otrzymujemy od osób fizycznych, biur podróży, linii lotniczych, a także amerykańskich oraz zagranicznych agencji rządowych.

Chciałbym zwrócić uwagę, że niedochowanie przez przewoźnika prywatności informacji uzyskanej od pasażerów nie będzie samo przez się naruszeniem przepisów sekcji 41712. Jednakże z chwilą, gdy przewoźnik oficjalnie i publicznie zobowiąże się do przestrzegania zasady „bezpiecznej przystani" o zapewnieniu ochrony prywatności zdobytych przez niego informacji o konsumentach, wówczas Departament będzie upoważniony do skorzystania z ustawowych uprawnień wynikających z sekcji 41712 w celu zapewnienia przestrzegania tych zasad. Zatem w momencie, gdy pasażer przekaże informacje przewoźnikowi, który zobowiązał się honorować zasady „bezpiecznej przystani", każdy przypadek niedotrzymania tego zobowiązania może spowodować szkodę dla konsumenta i będzie stanowić naruszenie przepisów sekcji 41712. Mój urząd przyzna pierwszeństwo dochodzeniom w sprawie każdej takiej domniemanej działalności i ściganiu każdego przypadku świadczącego o takiej działalności. Poinformujemy także Departament Handlu o wynikach każdej takiej sprawy.

Naruszenia przepisów sekcji 41712 mogą być powodem wydania nakazów zaprzestania i nałożenia kar cywilnych za naruszenie tych nakazów. Pomimo, że nie posiadamy uprawnień do przyznawania odszkodowań albo zadośćuczynienia pieniężnego skarżącym osobom fizycznym, posiadamy jednak uprawnienia do uznania ugody będącej skutkiem dochodzeń i spraw wszczętych przez Departament, która zapewnia konsumentom korzyści w postaci złagodzenia albo wyrównania kar pieniężnych, które w przeciwnym razie musiałyby być zapłacone. Tak postępowaliśmy w przeszłości i możemy i będziemy tak postępować w związku z zasadami „bezpiecznej przystani", kiedy okoliczności będą dawały ku temu podstawę. Powtarzające się przypadki naruszenia przepisów sekcji 41712 przez jakąkolwiek amerykańską linię lotniczą postawiłyby także pod znakiem zapytania zdolność linii lotniczej do przestrzegania przepisów, co w drastycznych przypadkach mogłoby doprowadzić do uznania, że utraciła ona zdolność prowadzenia swojej działalności i że w związku z tym traci uprawnienia do prowadzenia swojej działalności. (Patrz: przepisy DOT 93–6–34, z dnia 23 czerwca 1993 r. i 93–6–11, z dnia 9 czerwca 1993 r. Pomimo, że

postępowanie to nie miało związku z sekcją 41712, to jednak skutkiem jego było cofnięcie uprawnienia do prowadzenia działalności przewozowej z powodu całkowitego lekceważenia przepisów Federal Aviation Act (Federalnej Ustawy o Lotnictwie), „dwustronnego porozumienia" oraz zasad i przepisów Departamentu).

Mam nadzieję, że informacje te okażą się pomocne. Gdyby miał Pan jeszcze jakieś pytania albo potrzebował dalszych informacji, to jestem do Pańskiej dyspozycji.

Z poważaniem,

Samuel Podberesky

(Radca — asystent ds. postĘpowania prawnego
i przestrzegania prawa w lotnictwie)

*ZAŁĄCZNIK VII*

W odniesieniu do art. 1 ust. 2 lit. b), organami rządowymi w Stanach Zjednoczonych uprawnionymi do badania skarg i uwalniania od nieuczciwych lub wprowadzających w błąd praktyk, a także do uzyskiwania zadośćuczynienia dla osób fizycznych niezależnie od ich państwa stałego zamieszkania lub obywatelstwa w przypadku nieprzestrzegania zasad wdrożonych zgodnie z NZP są:

1. Federalna Komisja Handlu i

2. Departament Transportu USA.

Federalna Komisja Handlu działa w granicach swoich uprawnień wynikających z sekcji 5 Federal Trade Commission Act (Ustawy o Federalnej Komisji Handlu). Właściwość Federalnej Komisji Handlu na mocy Sekcji 5 jest wyłączona w stosunku do banków, instytucji oszczędnościowo-kredytowych oraz spółdzielni kredytowych; operatorów telekomunikacyjnych, międzystanowych przewoźników publicznych, przewoźników lotniczych, a także zakładów rzeźnych oraz punktów skupu bydła rzeźnego. Chociaż branża ubezpieczeniowa nie jest wyraźnie włączona do listy wyjątków sekcji 5, Ustawa McCarran — Fergusson ([1]) pozostawia regulację działalności ubezpieczeniowej poszczególnym stanom. Jednakże przepisy Ustawy o FKH stosuje się do branży ubezpieczeniowej w takim zakresie, w jakim taka działalność nie jest regulowana przez prawo stanowe. FKH zachowuje pozostałe uprawnienia w sprawach nieuczciwych lub wprowadzających w błąd praktyk stosowanych przez zakłady ubezpieczeniowe wtedy, gdy nie zajmują się działalnością ubezpieczeniową.

Departament Transportu USA działa na podstawie swoich uprawnień wynikających z tytułu 49 Kodeksu Stanów Zjednoczonych, sekcja 41712. Departament Transportu USA wszczyna postępowania w oparciu o swoje własne dochodzenia, a także na podstawie formalnej i nieformalnej skargi otrzymanej od osób fizycznych, biur podróży, linii lotniczych, a także amerykańskich oraz zagranicznych agencji rządowych.

([1]) 15 U. S. C. § 1011 i następny.