



**00665/11/PL
WP 182**

Opinia 11/2011 w sprawie stopnia ochrony danych osobowych w Nowej Zelandii

przyjęta dnia 4 kwietnia 2011 r.

Grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest to niezależny europejski organ doradczy działający w dziedzinie ochrony danych i prywatności. Jej zadania określa art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE.

Funkcje sekretariatu pełni Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Komisji Europejskiej, Dyrekcja Generalna ds. Sprawiedliwości, B-1049 Brussels, Belgia, Office No MO-59 02/013.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych

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, a w szczególności art. 29 i art. 30 ust. 1 lit. b) dyrektywy,

uwzględniając regulamin wewnętrzny grupy roboczej, w szczególności jego art. 12 i 14,

przyjmuje niniejszą opinię.

1. Wprowadzenie i kontekst

W 2009 r. grupa robocza otrzymała wniosek dotyczący rozpatrzenia, czy prawodawstwo Nowej Zelandii w zakresie ochrony danych zapewnia prawidłowy stopień ochrony danych, a właściwa podgrupa uzyskała mandat w tym zakresie na posiedzeniu plenarnym w grudniu 2009 r.

Komisja Europejska przedstawiła zlecone przez siebie sprawozdanie dotyczące tego, czy Nowa Zelandia zapewnia prawidłowy stopień ochrony danych, które zostało sporządzone przez profesora Rotha z Wydziału Prawa Uniwersytetu Otawo, Dunedin, Nowa Zelandia. Sprawozdanie to zostało napisane pod nadzorem Centre de Recherches Informatique et Droit (zwanego dalej „CRID”) z Uniwersytetu w Namur. W sprawozdaniu tym przeanalizowano stopień, w jakim system prawny Nowej Zelandii spełnia wymogi w zakresie prawodawstwa w tej dziedzinie i mechanizmów stosowania przepisów służących ochronie danych osobowych określone w dokumencie roboczym „Przekazywanie danych osobowych do krajów trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych”, zatwierdzonym przez grupę roboczą art. 29 dyrektywy dnia 24 lipca 1998 r. (dokument WP12). W sprawozdaniu uwzględnia się również zasady pozaprawne, praktykę oraz ogólną kulturę administracyjną i korporacyjną istniejące w odniesieniu do ochrony prywatności.

Podgrupa przeanalizowała wspomniane sprawozdanie i uwagi dotyczące sprawozdania otrzymane od NZ DPA, Ministerstwa Sprawiedliwości Nowej Zelandii, oraz pismo Ministerstwa Sprawiedliwości dotyczące ustawy zmieniającej w sprawie ochrony prywatności (transgranicznego przekazywania informacji) z 2010 r. Podgrupa poprosiła również nowozelandzkiego Komisarza ds. Ochrony Prywatności (krajowy organ nadzorczy) o przedstawienie dalszych informacji i wyjaśnień na temat niektórych aspektów, które przedstawiono poniżej. Następnie podgrupa przeanalizowała otrzymane informacje zawierające wskazówki Komisarza ds. Ochrony Prywatności dotyczące zastosowania ustawy zmieniającej w sprawie ochrony prywatności (transgranicznego przekazywania informacji) po jej wejściu w życie dnia 7 września 2010 r.

Niniejsza opinia w znacznej mierze opiera się na sprawozdaniu profesora Rotha, które zostało napisane przejrzystie i usystematyzowane w pomocny sposób, tak aby można było przeanalizować prawodawstwo Nowej Zelandii pod kątem każdego z wymogów określonych w dokumencie WP 12.

2. Prawodawstwo w zakresie ochrony danych w Nowej Zelandii

Nowa Zelandia nie ma spisanej konstytucji i jest demokracją parlamentarną. Istnieje szereg ustaw o znaczeniu konstytucyjnym, które uznaje się za „prawo wyższe”. Obejmują one ustawę „Karta praw Nowej Zelandii” z 1990 r. oraz ustawę o prawach człowieka z 1993 r. Istnieje też szereg przepisów i zasad prawa zwyczajowego dotyczących ochrony danych, w tym uznawania deliktów prawa zwyczajowego w zakresie ochrony prywatności oraz naruszenia poufności.

Głównym aktem prawnym w zakresie ochrony danych w Nowej Zelandii jest ustawa o ochronie prywatności z 1993 r. (ustawa), która w znacznym stopniu opiera się na wytycznych OECD z 1980 r. w sprawie ochrony prywatności i transgranicznego przepływu danych osobowych. Istnieją trzy całościowe kodeksy praktyk w zakresie ochrony prywatności sporządzone na mocy sekcji 46 ustawy, które mają zastosowanie w szczególności, oraz przy zastosowaniu bardziej rygorystycznych norm, do danych dotyczących zdrowia, danych telekomunikacyjnych oraz danych w zakresie sprawozdawczości kredytowej. Istnieją również akty prawne związane z takimi obszarami, jak wolność informacji; spam; sankcje karne za niektóre naruszenia prywatności; wyroki za przestępstwa kryminalne; nadzór / inwigilacja; zatrzymanie informacji o zdrowiu; rejestry publiczne; oraz prawo w zakresie dyskryminacji. Również w innych aktach prawnych istnieją przepisy odnoszące się do ochrony prywatności, na przykład przepisy o tajności w ustawie wyborczej z 1993 r. chroniące prywatność wyborcy.

Na mocy ustawy o ochronie prywatności ustanawia się urząd Komisarza ds. Ochrony Prywatności, będący niezależnym podmiotem. Komisarz ds. Ochrony Prywatności wydał szereg wytycznych, broszur informacyjnych oraz innych informacji opisujących prawa i obowiązki organizacji i osób fizycznych, jak również anonimowe akta spraw związanych z konkretnymi skargami. Dokumenty te stanowią wytyczne w zakresie praktycznego zastosowania zasad ochrony prywatności. Ponadto orzecznictwo w zakresie praw człowieka daje wskazówki oraz wykładnię w odniesieniu do aspektów ustawy o ochronie prywatności.

Nowa Zelandia ma również dwie ustawy związane z wolnością informacji, które zawierają przepisy o ochronie prywatności. Ustawa o informacjach urzędowych dotyczy rządu centralnego oraz agencji sektora publicznego; ustawa o urzędowych informacjach i posiedzeniach organów samorządu terytorialnego z 1987 r. dotyczy władz lokalnych. Istnieją przepisy o ochronie prywatności regulujące przypadki, w których proponuje się ujawnianie danych rządowych, oraz prawo do uzyskania uzasadnienia decyzji rządowych dotyczących osób fizycznych.

Nowa Zelandia ma niezależne sądownictwo, a sprawy związane z ustawą o ochronie prywatności mogą być kierowane do Trybunału Rewizyjnego Praw Człowieka (Human Rights Review Tribunal). Sąd Rejonowy (District Court) rozpatruje sprawy z zakresu prawa zwyczajowego i prawa karnego. Odwołania od obu tych sądów rozpatruje Wysoki Sąd (High Court). Wyższą instancją wobec tego sądu jest Sąd Apelacyjny (Court of Appeal), a następnie Sąd Najwyższy (Supreme Court).

Istnieją środki prawa cywilnego dotyczące ochrony prywatności, w tym zniesławienia, zakłócania porządku, nękania, oszczerstwa, naruszenia własności, umyślnego wyrządzenia szkody, zaniechania oraz bezprawnego używania nazwy. Ponadto prawo karne obejmuje szereg przestępstw związanych z naruszeniem prywatności osoby fizycznej, takich jak bezprawne wykorzystanie lub ujawnienie danych osobowych.

Wreszcie istotne jest, że Nowa Zelandia to mały kraj, zamieszkały przez ok. 4,3 miliona osób, i zgodnie z ekspertyzą uczciwe obchodzenie się z informacjami jest postrzegane jako dobra praktyka. Organizacje nie mogą sobie pozwolić na zniechęcenie do siebie takiego małego rynku, a wieści o wiejskich praktykach rozchodzą się szybko. Ma to znaczący wpływ na praktykę biznesową.

3. Ocena, czy prawodawstwo w Nowej Zelandii zapewnia prawidłowy stopień ochrony danych osobowych

Grupa robocza podkreśla, że jej ocena, czy nowozelandzkie prawo w zakresie ochrony danych zapewnia prawidłowy stopień ochrony, skupia się na ustawie o ochronie prywatności z 1993 r.

Zawarte w ustawie przepisy, jak również orzecznictwo sądów w odniesieniu do ochrony danych osobowych porównano z głównymi przepisami dyrektywy, uwzględniając opinię WP 12 grupy roboczej. W opinii tej wymienia się kilka zasad, które stanowią „trzon” zasad związanych z treścią w zakresie ochrony danych i wymogów ‘proceduralnych / wykonawczych’, których spełnienie może być postrzegane jako wymóg minimalny dla uznania, że stopień ochrony jest prawidłowy”.

3.1. Zakres zastosowania prawodawstwa

Ustawa dotyczy wszelkich danych osobowych niezależnie od kształtu czy formy. Obejmuje w całości sektor publiczny i sektor prywatny, z uwzględnieniem kilku szczegółowych wyjątków związanych z interesem publicznym, jak to ma zazwyczaj miejsce w społeczeństwie demokratycznym. W ustawie definiuje się dane osobowe jako „informacje o osobie możliwej do zidentyfikowania”, przy czym osoba ta jest żyjącą osobą fizyczną, natomiast informacje takie obejmują również dane dotyczące zgonu w urzędowym rejestrze zgonów.

W odniesieniu do możliwości zidentyfikowania, nie tylko same informacje mogą służyć identyfikacji danej osoby. W sprawie *Komisarz ds. Postępowania przeciwko Komisarzowi Policji* [2000] NZAR 277, Trybunał uznał, że jeśli tylko na podstawie informacji „[osoba] mogła być zidentyfikowana przez część społeczeństwa”, były to dane osobowe w myśl ustawy o ochronie prywatności.

Ustawa obejmuje wszystkie nowozelandzkie agencje, chyba że zastosowanie ma szczegółowy wyjątek. Agencję definiuje się jako „każdą osobę lub grupę osób, zrzeszonych lub niezrzeszonych, w sektorze publicznym lub sektorze prywatnym; oraz, dla uniknięcia wątpliwości, do kategorii tej należy Departament”.

Mimo że definicja ta uwzględnia osoby fizyczne jako agencje, nie obejmuje jednak danych osobowych związanych ze sprawami domowymi („sprawami osobistymi, rodzinnymi lub domowymi danej osoby fizycznej”).

Każda osoba fizyczna może skierować skargę do Komisarza ds. Ochrony Prywatności oraz, zgodnie z ustawą zmieniającą w sprawie ochrony prywatności (transgranicznego przekazywania informacji), każda osoba fizyczna może złożyć do nowozelandzkiej agencji wniosek o dostęp do danych, które jej dotyczą.

Przewiduje się szczegółowe, określone na mocy prawa wyjątki. Główne wyjątki od zakresu ustawy mają podłoże polityczne, konstytucyjne i sądownicze. Informacyjne środki przekazu są objęte wyłączeniem w zakresie swojej działalności informacyjnej (podobnie jak w przypadku art. 9 dyrektywy UE).

Grupa robocza uważa zatem, że zakres zastosowania ustawy o ochronie prywatności jest podobny do zakresu zastosowania dyrektywy.

3.2. Zasady związane z treścią

Ustawa zawiera dwanaście zasad ochrony prywatności danych. Zasady te nie podlegają bezpośredniej egzekucji na drodze sądowej poza prawem dostępu do danych będących w posiadaniu agencji sektora publicznego. W przypadku zaistnienia „ingerencji w prywatność” można złożyć skargę do Komisarza ds. Ochrony Prywatności. „Ingerencja w prywatność” ma miejsce, gdy naruszeniu zasad towarzyszy szkoda lub strata poniesiona przez osobę fizyczną. W odniesieniu do podejścia opartego na szkodzie Komisarz ds. Ochrony Prywatności potwierdził, że jest ono określone, w szerokim zakresie, prawem i obejmuje „stratę, uszczerbek, szkodę lub krzywdę”, jak też „niekorzystny wpływ na prawa, korzyści, przywileje, obowiązki”. Co najważniejsze, do

obszarów, które są wyraźnie przewidziane w ustawie, należy szkoda emocjonalna lub psychiczna w postaci „poważnego poniżenia, znaczącej utraty godności, znaczącej krzywdy dla uczuć”. Aby zaistniała „ingerencja w prywatność”, nie jest konieczne wykazywanie szkody ani straty w odniesieniu do zasady dostępu do swoich danych i zasady korygowania.

Zasady podstawowe

1) Zasada ograniczenia celu: dane powinny być przetwarzane w konkretnym celu, a następnie wykorzystywane lub dalej przekazywane tylko, o ile nie jest to niezgodne z celem ich przekazania. Jedyne wyjątki dotyczące tej zasady to te, które są konieczne w demokratycznym społeczeństwie z ważnych względów wymienionych w art. 13 dyrektywy.

Grupa robocza uważa, że Nowa Zelandia realizuje tę zasadę poprzez swoje zasady ochrony prywatności danych 1 (Cel gromadzenia danych osobowych), 10 (Ograniczenia w zakresie wykorzystania danych osobowych) oraz 11 (Ograniczenia w zakresie ujawniania danych osobowych).

Zgodnie z zasadą 1, w przypadku gdy agencja gromadzi dane osobowe, cel tego gromadzenia musi być zgodny z prawem; dane muszą się wiązać z funkcją lub działalnością agencji; oraz muszą być niezbędne dla realizacji tego celu. Zgodnie z zasadami 10 i 11 wymaga się, aby wykorzystanie lub ujawnienie danych osobowych było zgodne z celem, w związku z którym zostały pozyskane, lub celem bezpośrednio związanym.

Zgodnie z zasadą 10 możliwe są wyjątki w przypadku celów drugorzędnych. W zasadzie 10 lit. e) określono, że agencja może wykorzystywać dane w innym celu, gdy uważa, mając ku temu uzasadnione podstawy, „że cel, dla którego dane są wykorzystywane wiąże się bezpośrednio z celem, w związku z którym dane te zostały pozyskane”. Zasada 11 lit. a) stanowi również, że agencja może ujawnić dane osobie, organowi bądź agencji, gdy uważa, mając ku temu uzasadnione podstawy, „że ujawnienie danych stanowi jeden z celów, w związku z którymi dane te zostały pozyskane lub wiąże się bezpośrednio z celami, w związku z którymi dane te zostały pozyskane”.

Drugorzędna podstawa „celu bezpośrednio związanego” w odniesieniu do wykorzystywania lub ujawniania danych osobowych odpowiada wymogowi określonemu w dokumencie WP 12 zakładającemu, że dane osobowe muszą być „następnie wykorzystywane lub dalej przekazywane tylko, o ile nie jest to niezgodne z celem ich przekazania”.

Większość z pozostałych wyjątków w ramach zasady 10 odpowiada wyjątkom przewidzianym w art. 13 dyrektywy. Tym, które nie odzwierciedlają przepisów art. 7 dyrektywy związanych z celami przetwarzania zgodnymi z prawem. Ponadto jeden wyjątek przewiduje możliwość wydawania przez Komisarza ds. Ochrony Prywatności zezwoleń na przetwarzanie danych. Ma to na celu uwzględnienie nieprzewidzianych okoliczności lub okoliczności, których nie obejmuje ustawa o ochronie prywatności. Szczegółowe informacje dotyczące tych zezwoleń zawarte są w sprawozdaniu rocznym Komisarza ds. Ochrony Prywatności.

Grupa robocza uważa zatem, że prawodawstwo Nowej Zelandia jest zgodne z tą zasadą.

2) Zasada jakości danych i proporcjonalności: dane powinny być dokładne i w razie konieczności uaktualniane. Dane powinny być prawidłowe, istotne dla danej sprawy oraz nie mogą wykraczać poza cel, w jakim są przekazywane lub dalej przetwarzane.

Grupa robocza uważa, że zasada dotycząca jakości danych jest realizowana poprzez zasady ochrony prywatności danych 7 (Korygowanie danych osobowych), 8 (Dokładność itp. danych osobowych, którą należy sprawdzać przed ich wykorzystaniem) oraz 9 (Agencja nie może przechowywać danych osobowych dłużej niż jest to konieczne). Zasada proporcjonalności jest realizowana poprzez zasadę ochrony prywatności danych 1 (Cel gromadzenia danych osobowych).

Zgodnie z zasadą 8 „agencja posiadająca dane osobowe nie wykorzystuje tych danych bez podjęcia takich kroków (o ile zostaną podjęte jakiegokolwiek kroki), które są w danych okolicznościach uzasadnione dla zagwarantowania, przy uwzględnieniu celu, w jakim proponuje się wykorzystać te dane, że dane są dokładne, aktualne, kompletne, stosowne i nie wprowadzają w błąd”.

Agencje mają obowiązek, na mocy zasady 7 ust. 2, korygować informacje albo z własnej inicjatywy albo na wniosek osoby fizycznej w celu zagwarantowania, że dane są dokładne, aktualne, kompletne i nie wprowadzają w błąd. Jeżeli dana osoba zwróci się z wnioskiem o dokonanie korekty, której agencja nie będzie chciała wykonać, osoba ta może zwrócić się z wnioskiem o dołączenie do istniejących informacji oświadczenia korygującego.

Zatrzymanie jest uregulowane w ramach zasady 9, zgodnie z którą „agencja posiadająca dane osobowe nie przechowuje tych danych dłużej niż jest to konieczne dla celów, dla których dane te mogą być wykorzystywane zgodnie z prawem”. Sprawdzenie tego, czy dane te mogą być wykorzystywane zgodnie z prawem uwzględnia zasada 10, która ogranicza wykorzystywanie danych osobowych.

Proporcjonalność jest uwzględniona w ramach zasady ochrony prywatności danych 1 lit. a), która stanowi, że gromadzone dane muszą „wiązać się z funkcją lub działalnością agencji”. Zasada 1 lit. b) stanowi, że gromadzenie danych musi być „konieczne” dla celu, dla którego są gromadzone. Istnieją akta spraw Komisarzy ds. Ochrony Prywatności oraz spraw Trybunału Rewizyjnego Praw Człowieka, w których zbadano wykładnię pojęcia „niewykraczania poza cel” i norm konieczności.

Grupa robocza uważa zatem, że prawodawstwo Nowej Zelandii jest zgodne z tą zasadą.

3) Zasada przejrzystości: osoby, których dane dotyczą, powinny być informowane o celu przetwarzania ich danych i o tożsamości osoby przetwarzającej dane w państwie trzecim oraz o wszelkich innych aspektach koniecznych do zapewnienia zgodności z zasadą sprawiedliwego traktowania. Jedyne dopuszczalne wyjątki muszą być ujęte w art. 11 ust. 2 oraz art. 13 dyrektywy.

Grupa robocza uważa, że wymogi w zakresie przejrzystości są ujęte w zasadach ochrony prywatności danych 2 (Źródło danych osobowych), 3 (Gromadzenie danych od osoby, której dane dotyczą) oraz 4 (Sposób gromadzenia danych osobowych).

Zgodnie z zasadą 2 ust. 1 „w przypadku gdy agencja gromadzi dane osobowe, agencja pozyskuje dane bezpośrednio od osoby zainteresowanej”. Zasada 3 ust. 1 stanowi, że „w przypadku gdy agencja gromadzi dane bezpośrednio od osoby, której dane dotyczą, agencja musi podjąć kroki uzasadnione w danych okolicznościach w celu zagwarantowania, aby osoba, której dane dotyczą, jest poinformowana o...”, a następnie przytacza wykaz danych, które należy przekazać tej osobie. Wykaz ten obejmuje oraz wykracza poza elementy określone w art. 10 dyrektywy.

W ustawie o ochronie prywatności nie przewiduje się powiadamiania osoby fizycznej, gdy dane są pozyskiwane ze źródła innego niż ta osoba, gdyż choć istnieją pewne wyjątki, zasadą prawa jest, że dane nie powinny być pozyskiwane od jakiegokolwiek innych osób niż osoba, której dane dotyczą.

W każdym razie osoba fizyczna jest chroniona w ramach wszystkich pozostałych zasad ochrony prywatności danych.

W ramach zasady 4 uwzględnia się kwestię uczciwości, stanowiąc, że agencja nie może gromadzić danych osobowych:

- (a) *metodami niezgodnymi z prawem; ani*
- (b) *metodami, które w okolicznościach danej sprawy, --*
 - (i) *są nieuczciwe; lub*
 - (ii) *ingerują w nieuzasadnionym zakresie w sprawy osobiste zainteresowanej osoby fizycznej.*

Niektóre wyjątki od zasady przejrzystości odpowiadają wyjątkom określonym w art. 11 ust. 2 i art. 13 dyrektywy. Jednak niektóre z wyjątków nie mają żadnego odpowiednika w dyrektywie. Wyjątki te omówiono poniżej.

(v) Agencja uważa, mając ku temu uzasadnione podstawy, że istnieje zezwolenie osoby, której dane dotyczą

W ustawie użyto pojęcia „zezwoenie”, a nie pojęcia „świadoma zgoda”. Jednakże Komisarz ds. Ochrony Prywatności i Trybunał zinterpretowali „zezwoenie” jako czynne i przemyślane wyrażenie zgody. W aktach sprawy Komisarz ds. Ochrony Prywatności stwierdza, że „zezwoenie wymaga decyzji potwierdzającej” oraz że brak sprzeciwu nie oznacza zezwolenia.

(vi) Agencja uważa, mając ku temu uzasadnione podstawy, że niezgodność z prawem nie stanowiłaby uszczerbku dla interesów osoby, której dane dotyczą

Wyjątek ten bierze się z podejścia opartego na szkodzie przyjętego w Nowej Zelandii. Odzwierciedla on test bilansujący wymagany na mocy art. 7f dyrektywy, chociaż w Nowej Zelandii test ten odnosi się do szkody lub straty, którą mogą spowodować działania organizacji. W celu zachowania ostrożności, organizacje mogą również powiadomić osobę i uzyskać zezwolenie na tę czynność. Pasuje to w wymiarze logicznym do podejścia przyjętego w Nowej Zelandii, gdzie ustawa obejmuje wszystkie dane osobowe, w tym rozmowy, plotki oraz informacje, którymi dana osoba dysponuje. W tych ramach konieczna jest pewna elastyczność, aby ustawa była wykonalna w praktyce, a podejście oparte na szkodzie jest jednym ze sposobów na osiągnięcie tego celu. Różni się ono od podejścia europejskiego, jednak jest mało prawdopodobne, aby doprowadziło do jakiegokolwiek uszczerbku dla praw i wolności osób. Dane osobowe w ramach tego wyjątku nadal podlegają pod pozostałe zasady ochrony prywatności danych.

(viii) Agencja uważa, mając ku temu uzasadnione podstawy, że zgodność z prawem może stanowić uszczerbek dla celów gromadzenia danych

Choć w dyrektywie nie ma dokładnego odpowiednika, wyjątek ten odzwierciedla wyjątki przewidziane w art. 13 lit. a)-f) i może być potencjalnie używany w związku z działaniami w zakresie monitorowania i nadzoru, w szczególności w obszarach zatrudnienia i egzekwowania prawa.

(xi) Specjalne zezwolenie udzielone przez Komisarza ds. Ochrony Prywatności

Wyjątek ten służy uwzględnieniu nieprzewidzianych okoliczności nieuwjętych w ustawie, w przypadku gdy przetwarzanie danych osobowych jest pożądane lub niezbędne. Komisarz wydaje zezwolenie jedynie wówczas, gdy ma pewność, że interes publiczny „przeważa w znacznym stopniu” nad jakąkolwiek potencjalną szkodą osoby fizycznej wynikającą z udzielenia zezwolenia lub że zezwolenie niesie za sobą „oczywistą korzyść dla zainteresowanej osoby, która przeważa nad” jakąkolwiek potencjalną szkodą, która może wyniknąć. Komisarz ds. Ochrony Prywatności nie może udzielić zezwolenia, jeżeli zainteresowana osoba fizyczna odmówiła udzielenia zezwolenia na gromadzenie, wykorzystywanie lub ujawnianie danych osobowych. Oznacza to, że

agencja musi najpierw spróbować uzyskać zgodę danej osoby fizycznej. Jeżeli osoba ta odmówi wyrażenia zgody, Komisja nie może udzielić zezwolenia.

Mimo że podejście w Nowej Zelandii odnośnie do przejrzystości różni się w niektórych aspektach od podejścia europejskiego, grupa robocza jest przekonana, że ustawa jest zgodna z omawianą zasadą, biorąc pod uwagę fakt, że podstawową regułą na mocy ustawy jest to, iż dane osobowe muszą być zawsze gromadzone bezpośrednio od zainteresowanych osób fizycznych, a w momencie gromadzenia danych osoba jest powiadamiana o celu i pozostałych zagadnieniach z tym związanych. Pozyskiwanie danych z innych źródeł lub też brak wymaganego powiadomienia w czasie gromadzenia danych traktuje się jako wyjątek od tej podstawowej reguły.

4) Zasada bezpieczeństwa: Administrator musi zapewnić odpowiednie środki techniczne i organizacyjne zapobiegające zagrożeniom związanym z przetwarzaniem danych. Osoby działające z upoważnienia administratora, w tym osoba odpowiedzialna za przetwarzanie danych, nie mogą przetwarzać danych inaczej niż na podstawie instrukcji administratora.

Grupa robocza uważa, że zasada 5 (Przechowywanie i bezpieczeństwo danych osobowych) obejmuje aspekty wymagane w przypadku zasady bezpieczeństwa. Zasada ta opiera się na zasadzie OECD dotyczącej gwarancji bezpieczeństwa, a sformułowania są podobne do sformułowań zawartych w art. 17 ust. 1 i 2 dyrektywy w tym, że środki bezpieczeństwa muszą zabezpieczać przed utratą, dostępem, wykorzystaniem, zmianą, ujawnieniem i nadużyciem danych. Agencje muszą uczynić możliwie wszystko, co w ich mocy, aby zapobiec nieupoważnionemu dostępowi i ujawnianiu danych, w przypadku gdy dane są przekazywane osobie przetwarzającej dane. Osoby przetwarzające dane wykorzystujące dane w zakresie wykraczającym poza instrukcje administratora danych naruszałby szereg zasad przewidzianych w ustawie. Akta spraw Komisarza ds. Ochrony Prywatności pokazują, że dane szczególnie chronione lub dane poufne (na przykład dane bankowe) muszą być chronione w ramach rygorystycznych gwarancji bezpieczeństwa. Zasada ta dotyczy zarówno administratorów danych, jak i osób przetwarzających dane.

Grupa robocza uważa, zatem, że prawo Nowej Zelandii jest zgodne z zasadą bezpieczeństwa.

5) Prawo do dostępu, sprostowania i sprzeciwu: osoba fizyczna musi mieć prawo do otrzymania kopii wszystkich danych, które jej dotyczą, oraz prawo do sprostowania danych, które są nieprawidłowe. W niektórych sytuacjach osoba fizyczna musi mieć również możliwość wniesienia sprzeciwu wobec przetwarzania danych, które jej dotyczą. Jedyne wyjątki dotyczące tych praw powinny być zgodne z art. 13 dyrektywy.

Grupa robocza uważa, że w ustawie przewiduje się prawa do dostępu i korygowania w ramach zasad 6 (Dostęp do danych osobowych) oraz 7 (Korygowanie danych osobowych). Wcześniej prawa do dostępu i korygowania ograniczały się do osób, które były obywatelami lub mieszkańcami bądź fizycznie przebywały w Nowej Zelandii. Jednak ustawa zmieniająca w sprawie ochrony prywatności (transgranicznego przekazywania informacji) z 2010 r. znowelizowała ustawę o ochronie prywatności w taki sposób, aby każdy miał prawo do składania „wniosków dotyczących ochrony prywatności danych”. Dotyczy to: wniosków o uzyskanie potwierdzenia tego, czy agencja posiada dane osobowe; wniosków o dostęp; oraz wniosków o skorygowanie. W odniesieniu do agencji sektora publicznego, prawo dostępu jest bezpośrednim prawem ustawowym, a w celu jego egzekucji dana osoba fizyczna może zwrócić się bezpośrednio do sądu zamiast korzystać z pośrednictwa Komisarza ds. Ochrony Prywatności.

Większość wyjątków od prawa do dostępu jest zgodna z przepisami art. 13 dyrektywy. Wyjątek, który dotyczy bezpieczeństwa narodowego i obronności dotyczy również stosunków międzynarodowych z innymi państwami i organizacjami międzynarodowymi, co nie jest

szczegółowo przewidziane w dyrektywie. Grupa robocza nie uważa jednak, aby miało to wpływ na prawidłowy poziom ochrony.

Istnieje szereg wyjątków, które odpowiadają art. 13 lit. g), jednak, ta sekcja ustawy obejmuje również wyjątki związane z administracją, które nie są przewidziane w dyrektywie. Przeanalizowano je poniżej.

Dostępu można odmówić, w przypadkach gdy „wniosek jest niepoważny lub przykry, lub dane, których dotyczy wniosek, są błahe”. Ma to zapobiec nadużywaniu prawa do dostępu i odzwierciedla przepisy europejskiego prawodawstwa w zakresie wolności informacji.

Istnieją trzy praktyczne wyjątki administracyjne, w przypadku gdy dane „nie są bezpośrednio dostępne”; w przypadku gdy „nie istnieją bądź nie można ich znaleźć”; oraz w przypadku gdy nie znajdują się w posiadaniu zainteresowanej agencji i nie ma żadnych podstaw do twierdzenia, że znajdują się w posiadaniu innej agencji lub że wiążą się ściślej z funkcjami czy działalnością innej agencji. W tym ostatnim przypadku agencja jest zobowiązana przekazać właściwej innej agencji wniosek o dostęp.

W odniesieniu do praw do sprzeciwu, nie istnieje bezpośrednie prawo w ramach prawodawstwa Nowej Zelandii. Jednak na mocy zasady 3 (Gromadzenie danych od osoby, której dane dotyczą) osoby fizyczne mogą wnieść sprzeciw wobec przetwarzania danych w chwili ich powiadomienia o tym fakcie. Na mocy zasady 3 ust. 1 lit. e) i f) osoby fizyczne należy powiadomić o następujących kwestiach.

(e) Czy na gromadzenie danych wydano zezwolenie lub czy jest ono wymagane prawem lub na mocy prawa,—

(i) Konkretnie prawo, na mocy którego wydano takie zezwolenie na gromadzenie danych bądź na mocy którego jest ono wymagane; oraz

(ii) Czy przekazanie danych przez daną osobę fizyczną jest dobrowolne czy obowiązkowe; oraz

(f) Konsekwencje (o ile takowe istnieją) dla tej osoby fizycznej, jeżeli całość lub jakakolwiek część danych, których dotyczy wniosek, nie zostanie przekazana.

Odnotowano dwa zgłoszone przypadki, w których Komisarz ds. Ochrony Prywatności rozpatrzył skargi, w przypadku których osobom odmówiono możliwości wniesienia sprzeciwu. W jednym przypadku związanym z przepisami dotyczącymi połowów agencja zmieniła swoją politykę, tak aby osoby fizyczne odpowiadały jedynie na pytania mające znaczenie dla odnośnych zagadnień. W drugim przypadku, związanym z warunkami członkostwa w klubie, w statucie klubu określono wyraźnie, jakie dane są gromadzone, w jakim celu oraz jacy są odbiorcy, a zatem nie wystąpiło żadne naruszenie zasady.

W dokumencie WP 12 stwierdza się, że jedynie w pewnych sytuacjach osoby fizyczne powinny mieć prawo do sprzeciwu oraz że to prawo obowiązuje w odniesieniu do danych unijnych w UE przed przekazaniem ich do Nowej Zelandii. Grupa robocza uważa, zatem, że prawodawstwo Nowej Zelandii jest zgodne z zasadą dotyczącą prawa do dostępu, sprostowania i sprzeciwu.

6) Ograniczenia w zakresie dalszego przekazywania danych do innych państw: dalsze przekazywanie danych osobowych z państwa przeznaczenia będącego stroną trzecią do innego państwa może być dozwolone jedynie, w przypadku gdy to kolejne państwo również zapewnia prawidłowy stopień ochrony. Jedynymi dopuszczalnymi wyjątkami od tej zasady są wyjątki przewidziane w art. 26 ust. 1 dyrektywy.

Ponieważ prawo Nowej Zelandii opiera się na wytycznych OECD, nie ma szczegółowego przepisu w zakresie środków ochrony i gwarancji, gdy dane osobowe są przekazywane do państwa trzeciego. Sekcja 10 ustawy ma zastosowanie w przypadkach, gdy agencje z Nowej Zelandii posiadają dane w państwie trzecim, dzięki czemu agencje nie mogą omijać zasad określonych w ustawie ze względu na fakt, że znajdują się poza Nową Zelandią. Przepis ten obejmuje również dane posiadane w państwie trzecim przez osobę przetwarzającą dane, działającą na rzecz agencji nowozelandzkiej. W ramach zasady 11 wprowadza się ograniczenia w zakresie ujawniania danych, również agencjom w państwach trzecich. Wyjątki od tego przepisu są w dużej mierze zgodne z odstępstwami określonymi w art. 26 dyrektywy. Nawet w przypadku gdy dane znajdują się w państwie trzecim, agencje nowozelandzkie wciąż ponoszą odpowiedzialność za jakąkolwiek szkodę lub stratę wynikającą z wykorzystania bądź ujawnienia danych w tym państwie trzecim, dlatego w ich interesie jest zminimalizowanie ryzyka i zapewnienie odpowiednich środków ochronnych.

Ustawa zmieniająca w sprawie ochrony prywatności (transgranicznego przekazywania informacji) z 2010 r. wprowadziła przepisy umożliwiające kierowanie skarg transgranicznych do właściwego organu oraz nadające Komisarzowi ds. Ochrony Prywatności uprawnienia, aby w wyjątkowych przypadkach zakazywał dalszego przekazywania danych osobowych uzyskanych z zagranicy. Komisarz ds. Ochrony Prywatności sporządził wskazówki wyjaśniające, jak działa ten przepis i jak urząd zamierza realizować nowe uprawnienia. Komisarz może wydać zakaz przekazywania danych, a naruszenie tego zakazu może skutkować oskarżeniem o popełnienie przestępstwa zagrożonego karą grzywny w wysokości 10 000 NZD.

Aby wydać zakaz, Komisarz musi mieć pewność, że:

- dane osobowe uzyskano z innego państwa i zostaną one przekazane do państwa trzeciego, w którym nie będą podlegały prawu zapewniającemu środki ochronne porównywalne z ustawą o ochronie prywatności; oraz
- przekazanie danych może stanowić naruszenie podstawowych zasad stosowania prawa w tym zakresie na szczeblu krajowym określonych w wytycznych OECD.

Przed podjęciem decyzji o wydaniu zakazu przekazywania danych Komisarz musi rozpatrzyć:

- kwestie określone w sekcji 114 (odnoszące się do praw człowieka oraz innych interesów społecznych, które kłócą się z ochroną prywatności; międzynarodowych zobowiązań Nowej Zelandii; zasad dotyczących poufności danych; zasad dotyczących poufności rejestrów publicznych);
- czy proponowany transfer danych osobowych ma wpływ lub może mieć potencjalnie wpływ na jakiegokolwiek osoby fizyczne;
- celowość ułatwiania swobodnego przepływu danych pomiędzy Nową Zelandią i innymi państwami; oraz
- wszelkie istniejące lub opracowywane wytyczne międzynarodowe w zakresie transgranicznego przepływu danych osobowych (w tym wytyczne OECD oraz dyrektywę UE).

Jeżeli chodzi o skuteczne egzekwowanie przepisów transgranicznych, przepisy oraz wytyczne Komisarza oznaczają, że w przypadku gdy europejskie organy ochrony danych zaalarmują Komisarza ds. Ochrony Prywatności odnośnie do transferu danych, Komisarz potraktuje taki przypadek priorytetowo i będzie mógł w razie potrzeby wydać zakaz przekazywania danych. Komisarz ma również uprawnienia dochodzeniowe, aby czynnie ujawniać potencjalne ustalenia dotyczące przekazania danych, które mogą gwarantować realizację uprawnień w zakresie zakazu do przekazywania danych.

Grupa robocza ma pewne obawy dotyczące skuteczności przepisów w praktyce, gdyż nie jest jasne, jak Komisarz dowie się o transferach danych poza Nową Zelandią w inny sposób niż za

pośrednictwem organów ds. ochrony danych osobowych. Mimo to zmiany w prawie oraz wytyczne Komisarza ds. Ochrony Prywatności wyczuły przedsiębiorstwa na potrzebę zapewnienia „prawidłowego stopnia ochrony” w odniesieniu do wszelkich przypadków dalszego przekazywania danych pod rygorem zakazu przekazywania danych. W rzeczywistości, biorąc pod uwagę odizolowanie geograficzne Nowej Zelandii od Europy, jej wielkość i charakter gospodarki, jest mało prawdopodobne, aby agencje nowozelandzkie miały jakikolwiek interes gospodarczy w wysyłaniu znacznych ilości danych pochodzących z UE do państw trzecich.

Choć grupa robocza nie uważa, że prawo nowozelandzkie jest w pełni zgodne z zasadą dotyczącą dalszego przekazywania danych, nie sądzi też, aby istniało znaczące uchybienie, ani aby miało ono wpływ na ustalenie dotyczące prawidłowego stopnia ochrony danych.

Zasady dodatkowe

Dokument WP12 odnosi się do niektórych zasad, które powinny być stosowane do konkretnych rodzajów przetwarzania, które obejmują w szczególności poniższe kwestie.

1) Dane szczególnie chronione – w przypadku gdy w grę wchodzi kategorie danych „szczególnie chronionych” (wymienione w art. 8 dyrektywy), zastosować należy dodatkowe środki zabezpieczające, na przykład wymóg, aby osoby fizyczne wyraziły wyraźną zgodę na przetwarzanie danych.

Ustawa, w odróżnieniu od dyrektywy, nie przewiduje rozróżnienia między danymi szczególnie chronionymi, a danymi nieobjętymi szczególną ochroną. W ustawie wszystkie dane traktuje się jako potencjalnie szczególnie chronione i dlatego wszystkie dane podlegają takim samym normom ochrony. Kategorie danych określone w art. 8 dyrektywy są ujęte w ustawie o prawach człowieka z 1993 r. Jako że prawodawstwo w zakresie ochrony danych w Nowej Zelandii poprzedza dyrektywę UE, jest ono zgodne z podejściem określonym w wytycznych OECD. W szczególności oznacza to podejście oparte na celu, ponieważ cel gromadzenia danych będzie determinował warunki ich wykorzystania i ujawniania w ramach zasad 10 i 11. Ponadto w części 11 i załączniku 5 ustawy o ochronie prywatności ściśle uregulowano dostęp agencji sektora publicznego do informacji dotyczących egzekwowania prawa.

Nowa Zelandia zachowała również zgodność z wytycznymi OECD poprzez oznaczanie niektórych kategorii danych jako wymagających szczególnej uwagi. Polega to na zastosowaniu szczegółowych kodeksów praktyk. Informacje dotyczące zdrowia są przedmiotem Kodeksu ochrony prywatności danych dotyczących zdrowia z 1994 r., który zawiera bardziej rygorystyczne przepisy niż ustawa. Do innych kodeksów należą Kodeks ochrony prywatności danych telekomunikacyjnych z 2003 r. oraz Kodeks ochrony prywatności danych w zakresie sprawozdawczości kredytowej z 2004 r. W kodeksie ochrony prywatności danych w zakresie sprawozdawczości kredytowej przewiduje się wymóg, że podmioty zajmujące się sprawozdawczością kredytową „nie mogą gromadzić danych osobowych do celów sprawozdawczości kredytowych, o ile nie są to informacje kredytowe”.

Środki prawne dla osób fizycznych są dostępne na mocy ustawy, jeżeli osoby fizyczne doznają „poważnego poniżenia, znaczącej utraty godności lub znaczącej krzywdy dla uczuć”. Wyrządzona szkoda emocjonalna jest osądzana pod kątem tego, jak dana osoba została w rzeczywistości pokrzywdzona w skutek naruszenia przepisów, a nie pod kątem tego, w jaki sposób dotknęłaby ona ewentualną przeciętną osobę.

Przepisy przeciwdziałające dyskryminacji zawarte w ustawie o prawach człowieka oraz inne przepisy prawa przewidują ochronę pewnych kategorii danych. Na przykład ustawa o przestępstwach z 1961 r. dotyczy przestępstw w zakresie ochrony prywatności osobistej i zawiera zakaz przejmowania danych. Ustawa w sprawie prywatnych detektywów i służb ochrony z 1974 r.

stanowi, że prywatni detektywi nie mogą robić zdjęć ani nagrywać obrazów danej osoby bez jej wcześniejszej pisemnej zgody oraz że takie fotografie lub nagrania nie mogą być wykorzystywane w postępowaniu cywilnym. Podobnie jak w przypadku niektórych państw europejskich prawodawstwo w zakresie wolności informacji zawiera przepisy przeciwdziałające ujawnianiu informacji, w przypadku gdy „wiązałoby się to z nieuzasadnionym ujawnieniem informacji o innej osobie” i nie występuje nadrzędny interes publiczny. Ponadto w szeregu przypadków, w których na mocy ustawy o ochronie prywatności uznano, że wskutek nieupoważnionego gromadzenia, wykorzystywania lub ujawniania danych doznano poważnego poniżenia, znaczącej utraty godności lub znaczącej krzywdy dla uczuć; kategorie danych wykraczają poza zakres art. 8 dyrektywy.

Grupa robocza uważa zatem, że prawo Nowej Zelandii jest zgodne z zasadą dotyczącą danych szczególnie chronionych.

2) Marketing bezpośredni – w przypadku gdy dane są przekazywane na potrzeby marketingu bezpośredniego, osoba fizyczna powinna mieć możliwość niewyrażenia zgody na wykorzystanie jej danych do takich celów w dowolnym momencie.

Analizując tę zasadę, grupa robocza przyjmuje, że Nowa Zelandia jest małym państwem, a działalność w zakresie marketingu bezpośredniego nie jest tu tak rozwinięta, jak w innych państwach. W ustawie nie ujęto żadnego szczegółowego przepisu odnoszącego się do marketingu bezpośredniego, jednak zasady ochrony prywatności danych mają identyczne zastosowanie w tej dziedzinie. Dotyczy to również ogólnej zasady, że dane osobowe, w tym dane wykorzystywane na potrzeby marketingu bezpośredniego, należy pozyskiwać bezpośrednio od osób fizycznych. Dlatego okoliczności, w których dane osobowe są przekazywane z UE do Nowej Zelandii i wykorzystywane w Nowej Zelandii na potrzeby marketingu bezpośredniego, mogą wystąpić jedynie rzadko, jeżeli w ogóle. Ponadto Kodeks ochrony prywatności danych telekomunikacyjnych z 2003 r. wprowadza ograniczenia w zakresie rodzaju informacji, które mogą być gromadzone, oraz w zakresie ich wykorzystania. Kodeks ma zastosowanie do operatorów sieci; podmiotów świadczących usługi telekomunikacyjne; wydawców katalogów adresowych i agencji informacyjnych, podmiotów świadczących usługi internetowe, centrów informacji telefonicznych (*call centre*) świadczących usługi informacyjne na zlecenie innej agencji oraz detalicznych podmiotów świadczących usługi telefonii komórkowej. Kodeks dopuszcza jedynie wykorzystywanie danych telekomunikacyjnych na potrzeby marketingu bezpośredniego za zgodą danej osoby.

Ustawa w sprawie niezamawianych reklam rozsyłanych pocztą elektroniczną z 2007 r. odnosi się do spamu i obejmuje pocztę email, komunikatory internetowe, wiadomości SMS i MMS o charakterze komercyjnym. Funkcjonuje podobnie do dyrektywy 2002/58/WE: wiadomości mogą być rozsyłane jedynie do osób, które wyraziły na to zgodę, i muszą zawierać mechanizm rezygnacji z subskrypcji.

Komisarz pomyślnie rozpatrzył wiele skarg dotyczących marketingu bezpośredniego.

Jeżeli chodzi o samoregulację, Nowozelandzkie Stowarzyszenie Marketingu i Urząd ds. Standardów Sektora Reklamy wykazały proaktywne podejście, szkoląc swoich członków w zakresie ochrony prywatności osób fizycznych. Wydały kodeks praktyk i oczekuje się, że wszyscy sprzedawcy będą stosować się do określonych w nim zasad. Osoby fizyczne mogą korzystać z bezpłatnego serwisu rozpatrywania skarg.

Nowozelandzkie Stowarzyszenie Marketingu prowadzi również bezpłatne serwisy „Nie wysyłaj” („Do Not Mail”) i „Nie dzwoń” („Do Not Call”), które dotyczą niezamawianych reklam

przekazywanych drogą telefoniczną i mailową, choć uaktualnione kopie list są rozsyłane jedynie do członków stowarzyszenia.

Pomimo że uregulowania dotyczące marketingu bezpośredniego w Nowej Zelandii różnią się od zasad stosowanych w Europie, to w praktyce osoba fizyczna ma kilka możliwości rezygnacji (*opt out*). Nawet bez formalnego prawa do rezygnacji, osoby fizyczne mogą składać skargi do Komisarza ds. Ochrony Prywatności, który uznał, że prawo musi zostać wzmocnione w tym obszarze. W rzeczywistości jest bardzo mało prawdopodobne, aby osoby fizyczne w UE otrzymywały wiadomości w ramach marketingu bezpośredniego z Nowej Zelandii, i dlatego grupa robocza uważa, że choć prawo Nowej Zelandii nie jest w pełni zgodne z zasadą dotyczącą marketingu bezpośredniego, nie występuje znaczące uchybienie ani nie powinno to mieć wpływu na ustalenie dotyczące prawidłowego stopnia ochrony danych.

3) Automatyczna decyzja indywidualna: w przypadku gdy celem przekazania danych jest podjęcie automatycznej decyzji w rozumieniu art. 15 dyrektywy, zainteresowana strona musi mieć prawo do poznania uzasadnienia takiej decyzji i należy podjąć inne środki w celu ochrony uzasadnionych interesów tej osoby.

W ekspertyzie wyraźnie określono, że podejmowanie decyzji automatycznych nie jest powszechne w Nowej Zelandii i że istnieją różne przepisy służące przeciwdziałaniu tej praktyce. Niektóre rządowe programy zestawiania informacji dopuszczają podejmowanie pewnych automatycznych decyzji, a uregulowania dotyczące tej kwestii są zawarte w części 10 (Zestawianie informacji) i załączniku 4 (Zasady zestawiania informacji) ustawy o ochronie prywatności. Komisarz pełni rolę nadzorczą w przypadku takich programów. W ramach przepisów przewiduje się wymóg stosowania środków ochronnych w odniesieniu do osób fizycznych, do których należą sprawdzenie poprawności wyników zautomatyzowanego wyszukiwania oraz przekazywanie osobom fizycznym informacji dotyczących jakichkolwiek rozbieżności i działań w celu ich usunięcia.

Zazwyczaj osobę fizyczną trzeba poinformować o celu, w jakim gromadzone są dane osobowe, w momencie gromadzenia danych (zasada 3); trzeba zapewnić dokładność danych osobowych przed ich wykorzystaniem (zasada 8); a dane osobowe zazwyczaj nie mogą być wykorzystywane do jakichkolwiek innych celów niż cel, w jakim zostały pozyskane (zasada 10). Agencje podejmujące decyzje automatyczne ponoszą również odpowiedzialność prawną, w przypadku gdy ich działania powodują szkodę lub stratę poniesioną przez osobę fizyczną.

W odniesieniu do sektora publicznego wszystkie osoby fizyczne mają ustawowe prawo dostępu do uzasadnienia decyzji dotyczących danej osoby na mocy ustawy o informacjach urzędowych oraz ustawy o urzędowych informacjach i posiedzeniach organów samorządu terytorialnego. Prawo to stosuje się jednak tylko do obywateli i rezydentów Nowej Zelandii lub osób fizycznie przebywających w Nowej Zelandii.

Grupa robocza uważa zatem, że prawo Nowej Zelandii jest w wystarczającym zakresie zgodne z zasadą dotyczącą automatycznych decyzji indywidualnych.

3.3. Mechanizmy proceduralne oraz mechanizmy egzekucji

W dokumencie WP 12 wskazuje się, że aby określić podstawę oceny prawidłowości realizowanej ochrony, konieczne jest zidentyfikowanie nadrzędnych celów proceduralnego systemu ochrony danych, i na tej podstawie dokonuje się oceny szeregu sądowych i pozasądowych mechanizmów proceduralnych stosowanych w państwach trzecich.

W tym względzie cele systemu ochrony danych są następujące.

- zapewnienie prawidłowego poziomu zgodności z przepisami.

- zapewnienie wsparcia i pomocy osobom fizycznym, których dane dotyczą, w wykonywaniu swoich praw.
- zapewnienie odpowiedniego zadośćuczynienia dla osób poszkodowanych w przypadku nieprzestrzegania przepisów.

a) Zapewnienie prawidłowego poziomu zgodności z przepisami: dobry system na ogół charakteryzuje się wysokim poziomem wiedzy wśród administratorów na temat ich obowiązków oraz wśród osób fizycznych na temat swoich praw i sposobów wykonywania tych praw.

Skuteczne sankcje i środki zniechęcające odgrywają ważną rolę w kontekście zagwarantowania przestrzegania przepisów, co dotyczy również systemów bezpośredniej kontroli sprawowanej przez władze, audytorów lub niezależnych urzędników zajmujących się ochroną danych.

Poziom wiedzy wśród administratorów danych i osób fizycznych

Ustawa o ochronie prywatności obowiązuje od 1993 r. i nakłada na każdą agencję publiczną i prywatną wymóg posiadania przynajmniej jednego pracownika ds. ochrony prywatności. Specjaliści tacy są odpowiedzialni za wspieranie swoich agencji w zapewnianiu zgodności z zasadami ochrony prywatności danych; rozpatrywanie wniosków o dostęp do danych; współdziałanie z Komisarzem ds. Ochrony Prywatności w przypadku dochodzeń; oraz wspieranie, w inny sposób, zgodności agencji z ustawą o ochronie prywatności. W całej Nowej Zelandii istnieje kilka sieci specjalistów ds. ochrony prywatności, w ramach których odbywają się spotkania. Urząd Komisarza ds. Ochrony Prywatności zamieszcza obszerne informacje na swojej stronie internetowej oraz publikuje kwartalnik i anonimowe akta spraw dotyczących wybranych dochodzeń. Na terenie całego kraju urząd prowadzi regularne szkolenia i warsztaty dla specjalistów ds. ochrony prywatności i innych osób oraz jest zaangażowany w organizowany corocznie tydzień wiedzy w zakresie ochrony prywatności w regionie Azji i Pacyfiku. Co kilka lat urząd przeprowadza badania służące ocenie poziomu wiedzy i oszacowaniu skuteczności działania Komisarza.

Urząd Komisarza ds. Ochrony Prywatności

Komisarz ds. Ochrony Prywatności jest organem publicznym, od którego wymaga się niezależnego działania w zakresie funkcji, obowiązków i uprawnień urzędu. Komisarz ds. Ochrony Prywatności jest mianowany przez Gubernatora Generalnego (będącego przedstawicielem głowy państwa w Nowej Zelandii) z rekomendacji właściwego ministra, którym jest Minister Sprawiedliwości. Mianowanie przez Gubernatora Generalnego jest specjalną procedurą wysokiego szczebla zarezerwowaną dla zaledwie kilku ważnych stanowisk ustawowych. Aby rekomendować daną osobę na stanowisko Komisarza, właściwy minister musi wiedzieć, że osoba ta posiada odpowiednią wiedzę, odpowiednie umiejętności i doświadczenia, aby wspierać ustawowy organ w realizacji jego celów i wypełnianiu jego funkcji. W sekcji 13(1A) ustawy o ochronie prywatności przewiduje się, że Komisarz musi działać niezależnie w ramach wypełniania swoich ustawowych funkcji i obowiązków oraz w ramach wykonywania swoich ustawowych uprawnień.

Do obowiązków Urzędu Komisarza ds. Ochrony Prywatności należy składanie corocznego sprawozdania Parlamentowi. Sprawozdania te zawierają szczegółowe informacje dotyczące wszystkich dopuszczonych programów zestawiania informacji prowadzonych w trakcie roku oraz ocenę ich zgodności z przepisami.

Komisarz ds. Ochrony Prywatności działa jak rzecznik praw obywatelskich, prowadząc dochodzenia i dążąc do rozstrzygania skarg oraz wszczynając i prowadząc dochodzenia z urzędu. Komisarz ma również zadania określone w ustawie, na przykład zadania związane z edukacją,

monitorowaniem zgodności z przepisami, doradzaniem w zakresie polityki, reagowaniem na zapytania, składaniem sprawozdań premierowi itd. W części 9 ustawy Komisarzowi ds. Ochrony Prywatności nadaje się uprawnienia do takich czynności, jak powoływanie i przesłuchiwanie świadków pod przysięgą oraz żądanie od nich przekazania informacji i dokumentów w terminie 20 dni roboczych.

Komisarz ds. Ochrony Prywatności ma również uprawnienia, funkcje i obowiązki wynikające z innych aktów prawnych niż ustawa o ochronie prywatności (na przykład z ustawy o ochronie zdrowia, ustawy w sprawie zabezpieczenia społecznego, ustawy o przeciwdziałaniu przemocy w rodzinie oraz ustawy o paszportach).

Ponadto Urząd Komisarza ds. Ochrony Prywatności został akredytowany przy Międzynarodowej Konferencji Komisarzy ds. Ochrony Danych i Prywatności; przyjęty do uczestnictwa w Umowie w ramach Współpracy Gospodarczej Azji i Pacyfiku (APEC) dotyczącej transgranicznego egzekwowania przepisów w zakresie ochrony prywatności; oraz uznany członkiem Globalnej sieci na rzecz egzekwowania przepisów w zakresie ochrony prywatności.

Środki egzekwowania i sankcje

W części 9 ustawy (Postępowania Komisarza) opisana jest procedura i uprawnienia dochodzeniowe Komisarza ds. Ochrony Prywatności. Zaniechanie współpracy w ramach dochodzeń Komisarza ds. Ochrony Prywatności lub utrudnianie ich jest naruszeniem prawa zagrożonym karę grzywny do 2 000 NZD.

Jeżeli skarga nie może być rozstrzygnięta przez Komisarza, można ją skierować do Trybunału Rewizyjnego Praw Człowieka, jeżeli osoba skarżąca lub Dyrektor ds. Postępowań w zakresie Praw Człowieka zdecyduje o kontynuowaniu sprawy. Osoba skarżąca może poprosić Dyrektora o skierowanie sprawy do Trybunału, nawet jeżeli Komisarz ds. Ochrony Prywatności odmówi tego. Trybunał dysponuje pełnym zakresem środków prawnych, w tym odszkodowaniami wyrównawczymi i zarządzeniami o charakterze zakazującym i obowiązkowym. Środki masowego przekazu zazwyczaj przekazują informacje o takich decyzjach, a fakt, że Nowa Zelandia jest krajem niewielkim, powoduje, że negatywny rozgłos ma efekt odstraszający. W przypadku gdy Dyrektor ds. Postępowań w zakresie Praw Człowieka podejmuje decyzję o niereprezentowaniu osoby skarżącej, Komisarz ds. Ochrony Prywatności jest zazwyczaj reprezentowany w czasie posiedzenia, gdy, co często ma miejsce, osoba skarżąca nie jest reprezentowana przez adwokata; na mocy ustawy o ochronie prywatności istnieje ważna zasada prawna w tej kwestii. W ramach prawa Komisarza ds. Ochrony Prywatności do stawania lub reprezentacji w takich sprawach Komisarz może stawać i zabierać głos we wszelkich postępowaniach, w których Dyrektor ds. Postępowań w zakresie Praw Człowieka jest uprawniony do stawania i zabierania głosu, ale odmawia tych czynności. Dyrektor ds. Postępowań w zakresie Praw Człowieka ma również prawo wnieść powództwo grupowe w imieniu grupy osób fizycznych, choć jak dotąd nie miało to miejsca.

Jak wspomniano powyżej, na mocy ustawy zmieniającej w sprawie ochrony prywatności (transgranicznego przekazywania informacji) z 2010 r. Komisarz uzyskuje uprawnienia do wydawania zakazów przekazywania danych w odniesieniu do transferów danych z Nowej Zelandii do państw trzecich bez prawidłowego stopnia ochrony danych.

W świetle wszystkich powyższych ustaleń grupa robocza uważa, że prawodawstwo Nowej Zelandii wprowadziło niezbędne elementy zapewnienia prawidłowego poziomu zgodności z przepisami w zakresie ochrony danych.

b) Zapewnienie wsparcia i pomocy osobom fizycznym, których dane dotyczą, w wykonywaniu swoich praw. Osoba fizyczna musi mieć możliwość szybkiego i skutecznego dochodzenia swoich praw, bez nadmiernych kosztów. W tym celu musi istnieć pewnego rodzaju mechanizm instytucjonalny umożliwiający niezależne rozpatrywanie skarg.

Jak wspomniano powyżej, Komisarz ds. Ochrony Prywatności ma obowiązek niezależnego działania w zakresie funkcji, obowiązków i uprawnień urzędu. W ciągu ostatnich kilku lat urząd wprowadził mechanizmy bardziej efektywnego rozpatrywania skarg i zmniejszania zaległości. Komisarz ds. Ochrony Prywatności ma prawo do wzywania stron na obowiązkowe konferencje w ramach rozpatrywania skargi, mając na celu rozpoznanie istotnych kwestii i dążenie do osiągnięcia porozumienia między stronami w zakresie rozstrzygnięcia sprawy. Niekiedy Komisarz może zorganizować niezależne lub wewnętrzne mediacje służące rozwiązaniu sporów. Agencje mogą zawrzeć ugodę przewidującą środki prawne, które nie są szczegółowo przewidziane na mocy ustawy o ochronie prywatności.

Osoby fizyczne nie ponoszą żadnych opłat z tytułu wnoszenia skarg do Komisarza lub bycia reprezentowanymi w sądzie przez Dyrektora ds. Postępowań w zakresie Praw Człowieka. Osoby skarżące mogą samodzielnie wnosić sprawy do Trybunału Rewizyjnego Praw Człowieka i nie ponoszą żadnych kosztów z tytułu wniesienia pozwu ani nie istnieje żaden wymóg bycia reprezentowanym przez prawnika. Jednak w przypadku gdy strona skarżąca przegra sprawę, może być na nią nałożony obowiązek pokrycia rzeczywistych i uzasadnionych kosztów prawnych strony, która proces wygrała.

Grupa robocza uważa, że prawodawstwo Nowej Zelandii oferuje wystarczające mechanizmy zapewnienia pomocy i wsparcia osobom fizycznym.

c) Zapewnienie odpowiedniego zadośćuczynienia dla osób poszkodowanych w przypadku nieprzestrzegania przepisów. Jest to kluczowy element, który musi obejmować system wydawania decyzji sądowych i arbitrażowych, a w odpowiednich przypadkach udzielanie odszkodowań i nakładanie sankcji.

Większość skarg dotyczących ochrony prywatności jest rozstrzyganych przez Komisarza lub zostaje zamknięta po przeprowadzeniu dochodzenia. Liczba spraw kierowanych do Trybunału Rewizyjnego Praw Człowieka pozostaje niemal na stałym poziomie i wynosi około 20 rocznie.

Trybunał ma prawo do wydawania deklaracji i zarządzeń ograniczających oraz do ukrycia szczegółów sprawy lub utajnienia części lub całości rozprawy. Trybunał może również przyznawać odszkodowania wyrównawcze do kwoty maksymalnej 200 000 NZD; najwyższą jak dotąd kwotą na mocy ustawy o ochronie prywatności była kwota 40 000 NZD przyznana z tytułu „poniżenia, utraty godności, krzywdy dla uczuć poszkodowanej osoby fizycznej”. W przypadku gdy kwota roszczenia odszkodowawczego przekracza 200 000 NZD, Trybunał może skierować sprawę do Wysokiego Sądu, który może przyznać odszkodowanie.

Trybunał może wydawać zarządzenia określające działania, jakie musi podjąć agencja, na przykład ujawnienie informacji w przypadku gdy udzielono odmowy w odniesieniu do wniosku o dostęp do danych. Może również wydawać zarządzenia dotyczące „innych środków pomocy” obejmujących środki prawne nieprzewidziane w ustawie.

Od decyzji Trybunału przysługuje odwołanie do Wysokiego Sądu, jeżeli decyzje te dotyczą kwestii faktycznych, a od decyzji Wysokiego Sądu przysługuje odwołanie do Sądu Apelacyjnego w odniesieniu jedynie do kwestii prawnych. Jeżeli Wysoki Sąd nie udzieli zgody na odwołanie, Sąd

Apelacyjny może jej udzielić, jeżeli uzna, że kwestia prawna ma na tyle istotne znaczenie, że sąd może rozpatrzyć sprawę. Ta sama procedura ma zastosowanie do odwołania do Sądu Najwyższego.

Grupa robocza uważa zatem, że prawo Nowej Zelandii zapewnia odpowiednie środki odszkodowawcze.

4. Wyniki oceny

Prawo Nowej Zelandii w zakresie ochrony danych i prywatności znacznie poprzedza dyrektywę UE, wdrażając wytyczne OECD. Ostatnio wprowadzono jednak zmiany dotyczące w szczególności problemów związanych z „prawidłowym stopniem ochrony” transferów danych osobowych z UE. Grupa robocza podkreśla, że mimo iż wciąż istnieją pewne problemy, prawidłowość nie oznacza ekwiwalencji między ustawą a dyrektywą.

Grupa robocza uważa zatem, że **Nowa Zelandia zapewnia prawidłowy stopień ochrony danych** w rozumieniu art. 25 ust. 6 dyrektywy 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 takich danych.

Grupa robocza zachęca jednak władze Nowej Zelandii do podjęcia koniecznych kroków służących wyeliminowaniu słabych punktów w obecnym systemie prawnym. W szczególności grupa robocza zachęca Komisarza ds. Ochrony Prywatności do podtrzymywania wezwania do wzmocnienia prawa w odniesieniu do marketingu bezpośredniego; oraz do utrzymania skutecznego nadzoru nad transferami danych z Nowej Zelandii do państw trzecich, które nie podlegają ustaleniu w zakresie prawidłowego stopnia ochrony danych. Grupa robocza prosi również, aby przy podejmowaniu decyzji o zakazie przekazywania danych oprócz wytycznych OECD i dyrektywy UE Komisarz ds. Ochrony Prywatności uwzględniał również odpowiednie decyzje Komisji Europejskiej i wskazówki Grupy Roboczej Art. 29.

Grupa robocza podkreśla również fakt, że w ramach wszelkich decyzji podejmowanych przez Komisję, będzie ona ściśle obserwować zmiany w zakresie ochrony danych w Nowej Zelandii i sposób stosowania przez Urząd Komisarza ds. Ochrony Prywatności zasad ochrony danych, o których mowa w dokumencie WP12 i w niniejszym dokumencie.

Sporządzono w Brukseli dnia 4 kwietnia
2011 r.

W imieniu Grupy Roboczej
Przewodniczący
Jacob KOHNSTAMM