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

01446/12//PL
WP 198

Opinia 07/2012 w sprawie poziomu ochrony danych osobowych w Księstwie Monako

przyjęta dnia 19 lipca 2012 r.

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 związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych, a w szczególności jej art. 29 i art. 30 ust. 1 lit. b),

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

WYDAJE NASTĘPUJĄCĄ OPINIĘ:

1. WPROWADZENIE I KONTEKST

W dniu 11 listopada 2009 r. Księstwo Monako zwróciło się do Komisji o objęcie procedurą mającą na celu stwierdzenie, że Monako jest państwem zapewniającym odpowiedni poziom ochrony w rozumieniu art. 25 ust. 6 dyrektywy 95/46/WE w sprawie ochrony danych osobowych.

Aby zbadać poziom ochrony w Monako, Komisja zwróciła się do grupy roboczej o sporządzenie opinii, w której zostanie przeanalizowany zakres, w jakim system prawny Monako spełnia wymogi z zakresu stosowania unormowań dotyczących ochrony danych osobowych określone w dokumencie roboczym „Transfers of Personal Data to Third Countries : Applying Articles 25 and 26 of the EU data protection directive", przyjętym przez grupę roboczą ustanowioną na mocy art. 29 dyrektywy, w dniu 24 lipca 1998 r. (dokument WP 12).

Grupa Robocza Art. 29, w trakcie sesji plenarnej w dniach 4 i 5 kwietnia 2011 r. wyznaczyła francuską komisję ds. technologii informacyjnej i wolności (*Commission Nationale de l'Informatique et des Libertés* – CNIL), ze względu na jej historyczne więzi z Monako, jako sprawozdawcę w sprawie analizy dotyczącej odpowiedniego poziomu ochrony.

Francuska komisja ds. technologii informacyjnej i wolności odbyła kilka spotkań z organem ds. ochrony danych z Monako, mianowicie „komisją ds. kontroli danych osobowych" (*Commission de Contrôle des Informations Nominatives*) (zwaną dalej CCIN), aby zbadać ustawodawstwo Monako z zakresu ochrony danych i jego praktyczne wdrażanie. W odniesieniu do niektórych zastrzeżeń dotyczących rzeczywistej niezależności CCIN, przewodniczący CNIL wezwał do odbycia posiedzenia mediacyjnego między CCIN a rządem Monako w dniu 28 maja 2012 r. Posiedzenie doprowadziło do zawarcia umowy wyjaśniającej kwestię kompetencji i stosunków między obiema stronami w kontekście zasobów ludzkich i zarządzania budżetem.

Zgodnie z decyzją podjętą na posiedzeniu w dniu 6 czerwca 2012 grupa robocza przekazała projekt opinii do „podgrupy ds. odpowiedniego poziomu ochrony" w celu dokonania jej weryfikacji. Podjęła również decyzję, że niniejsza opinia zostanie przyjęta w drodze procedury pisemnej.

Po telekonferencji projekt opinii został wysłany w dniu 4 lipca 2012 r. do „podgrupy ds. odpowiedniego poziomu ochrony" w celu dokonania jej weryfikacji. Propozycja została zatwierdzona przez grupę roboczą w procedurze pisemnej.

2. USTAWODAWSTWO DOTYCZĄCE OCHRONY DANYCH W KSIĘSTWIE MONAKO

Monako jest drugim najmniejszym państwem świata, jak również drugim najgęściej zaludnionym krajem na świecie. Monako jest księstwem, w którym panuje dziedziczna monarchia konstytucyjna zgodnie z konstytucją z dnia 17 grudnia 1962 r., zmienioną w dniu 2 kwietnia 2002 r. Jest suwerennym państwem miastem, które graniczy z Francją z trzech stron, z jednej strony położone jest natomiast nad Morzem Śródziemnym. Populacja Monako liczy około 32 800 mieszkańców. Jego działalność gospodarcza obejmuje głównie transakcje handlowe i w szczególności turystykę. Monako i Francję łączy silna unia polityczna, celna i monetarna. Największą grupę ludności stanowią obywatele francuscy (28,4 %), następną zaś grupą są Monegaskowie (21,6%).

Ze względu na historyczne związki między Francją i Monako, monakijskie ustawodawstwo dotyczące ochrony danych osobowych jest zbliżone do francuskiego prawa z zakresu ochrony danych.

Artykuł 20 konstytucji Monako potwierdza, że prawo do prywatności jest chronione i stanowi, że „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego oraz zachowania tajemnicy korespondencji".

Ochrona danych osobowych jest uregulowana ustawą nr 1.165 z dnia 23 grudnia 1993 r. o ochronie danych osobowych (*la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives*) oraz rozporządzeniem nr 2.230 z dnia 29 czerwca 2009 r. określającym warunki wdrażania ustawy nr 1.165 (*l'Ordonnance Souveraine n° 2.230 du 29 juin 2009 fixant les modalités d'application de la loi n° 1.165*). Ustawa została zmieniona ustawą nr 1.353 z dnia 4 grudnia 2008 r. i ustawą nr 1.353 z dnia 1 kwietnia 2009 r. (zwana dalej „ustawą" lub „ustawą nr 1.165").

Ustawa ustanawia CCIN jako niezależny organ. W trakcie kilku lat funkcjonowania na podstawie nowych przepisów i statutu (od 2009 r.), CCIN wydał różne wytyczne, protokoły z obrad, dwa sprawozdania roczne i inne dokumenty na temat wielu zagadnień (na przykład danych biometrycznych, chipów GPS, nadzoru wideo itp.), by określić prawa i obowiązki jednostek, podmiotów gospodarczych i państwa oraz udzielić wskazówek dotyczących praktycznego zastosowania zasad ochrony prywatności.

Na forum międzynarodowym Monako podpisało i ratyfikowało europejską konwencję praw człowieka w 2005 r., Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Konwencja 108) i jej protokół dodatkowy (obowiązujący od 1 kwietnia 2009 r.), jak również Międzynarodowy pakt praw obywatelskich i politycznych w dniu 28 sierpnia 1997 r.

3. OCENA PRAWA DOTYCZĄCEGO OCHRONY DANYCH KSIĘSTWA MONAKO W ZAKRESIE ZAPEWNIENIA ODPOWIEDNIEGO POZIOMU OCHRONY DANYCH OSOBOWYCH

Grupa robocza podkreśla, że jej ocena odpowiedniego poziomu ochrony w obowiązującym w Monako ustawodawstwie dotyczącym ochrony danych odnosi się głównie do ustawy nr 1.165 o ochronie danych osobowych z dnia 23 grudnia 1993 r. z późn. zmianami z 2008 r. i 2009 r.

Przepisy tej ustawy zostały porównane z głównymi przepisami dyrektywy, z uwzględnieniem opinii grupy roboczej – WP 12. W niniejszej opinii przedstawiono listę zasad stanowiących „podstawę materialnych zasad ochrony danych i wymogów proceduralnych/dotyczących wykonania, zgodność z którymi mogłaby być rozumiana jako minimalny wymóg do uznania ochrony za odpowiednią".

3.1. Definicje

Ustawa wprowadza definicje „danych osobowych", „przetwarzania", "administratora danych", „odbiorcy" i „osoby, której dane dotyczą" (art. 1).

Niektóre definicje nie zostały jednak wprowadzone („zbiór danych", „przetwarzający", „osoba trzecia" i „zgoda osoby, której dane dotyczą") i wszystkie te pojęcia są używane i interpretowane na podstawie kilku artykułów tej ustawy[1].

Aby jednak uniknąć wykładni, która może być niekorzystna dla ochrony danych, byłoby lepiej, gdyby monakijski ustawodawca zdefiniował wyżej wymienione terminy. Jest to szczególnie istotne w przypadku definicji „zgody" i „przetwarzającego". W tym kontekście grupa robocza odsyła do przedstawionego w jej opiniach wyjaśnienia pojęć „administratora danych", „przetwarzającego" i „zgody" (w szczególności jej „wyraźności" i „świadomości"), jak również samego pojęcia „danych osobowych".

3.2. Zakres stosowania ustawodawstwa

Zakres stosowania ustawy jest głównie określony w rozdziale V monakijskiej ustawy i jest bardzo zbliżony do art. 3, 4 i 13 dyrektywy.

W odniesieniu do zakresu przedmiotowego, ustawa obejmuje wszystkie formy przetwarzania danych osobowych (zautomatyzowanego lub niezautomatyzowanego, art. 24-1) w każdej postaci lub formie (art. 1 akapit pierwszy), chroni osoby fizyczne, jak również prawne (wywiedzione z art. 3, art. 13 itp.) i dotyczy przetwarzania przeprowadzanego przez cały sektor publiczny i prywatny.

Mogą zaistnieć pewne wątpliwości dotyczące wprowadzenia w art. 13 ustawy nr 1.165 przepisów zezwalających osobom prawnym na wniesienie sprzeciwu wobec przetwarzania ich danych osobowych. Grupa robocza uznaje, że zakres stosowania ustawy powinien zostać wyjaśniony, by uniknąć niespójności tekstu z pierwotnym zakresem stosowania określonym w art. 1 dotyczącym jedynie ochrony osób fizycznych.

[1] Zbiór jest wymieniony w art. 23-1, 24-1, 24-2, 25, przetwarzający w art. 1 (definicja odbiorcy), art. 17 (dotyczącym wymogów bezpieczeństwa), osoba trzecia w art. 8 ust. 6, 12, 14, 20-1, zgoda osoby, której dane dotyczą w art. 10-2, 12.

Jak przewidziano w dyrektywie, ustawa monakijska nie ma zastosowania do przetwarzania danych osobowych przeprowadzanego przez osobę fizyczną wyłącznie jako część jej działań w celach osobistych lub domowych. Ponadto ustawa nie ma zastosowania do przetwarzania danych zgodnie z art. 15 konstytucji (dotyczącym ułaskawienia, amnestii i naturalizacji) lub przeprowadzanego przez organy sądowe do celów postępowań przed sądami i międzynarodowych postępowań z zakresu pomocy prawnej (art. 24-2 ustawy).

Ponadto art. 25 ustawy przewiduje wyjątki dotyczące przetwarzania dla potrzeb literackich lub artystycznych, tak jak art. 9 dyrektywy.

W odniesieniu do zakresu terytorialnego art. 24 przewiduje w sposób zbliżony do dyrektywy, że ustawę stosuje się do przetwarzania zautomatyzowanego:

- przeprowadzanego przez administratora danych mającego siedzibę w Monako;
- przeprowadzanego w Monako, nawet jeżeli takie przetwarzanie jest przeznaczone wyłącznie do użytku za granicą;
- w przypadku gdy administrator danych ma siedzibę za granicą, ale korzysta z infrastruktury przetwarzania danych zlokalizowanej w Monako; w takim przypadku administrator danych musi wskazać pełnomocnika mającego miejsce zamieszkania w Monako, który będzie składać oświadczenia, wnioski o opinię lub wniosek o zatwierdzenie i na którym ciążą zobowiązania określone przez prawo, bez uszczerbku dla powództwa, które może być wytoczone przeciwko samemu administratorowi danych.

Grupa robocza uznaje zatem zakres stosowania monakijskiej ustawy za zbieżny z zakresem przewidzianym przez dyrektywę, chociaż zmiana niektórych obecnych sformułowań wydaje się jednak wskazana, by wyjaśnić, w jaki sposób przepisy mają zastosowanie do osób prawnych.

3.3. Zasady materialne

a) Podstawowe zasady

1) Zasada ograniczenia celu: Dane powinny być przetwarzane w konkretnym celu i następnie użyte lub przekazane dalej jedynie w takim zakresie, w jakim nie jest to sprzeczne z celem przekazania. Jedynymi wyjątkami od tej zasady są te sytuacje, które mogą być konieczne w demokratycznym społeczeństwie na podstawie jednej z przesłanek wymienionych w art. 13 dyrektywy.

Grupa robocza uznaje, że monakijskie ustawodawstwo realizuję tę zasadę poprzez art. 10-1, który przewiduje, że „dane osobowe muszą być: zebrane i przetworzone rzetelnie i zgodnie z prawem; zebrane w konkretnych, wyraźnych i zasadnych celach i nie mogą być dalej przetworzone w sposób niezgodny z tymi celami;(...)”

Ponadto art. 22 ustawy przewiduje, że „Następujące czyny są zagrożone karą pozbawienia wolności od trzech miesięcy do roku i karą grzywny określoną w art. 26 § 4 kodeksu karnego albo wyłącznie jedną z tych dwóch kar: (...) ust. 9 w przypadku gdy dana osoba świadomie używa lub przyczynia się do użycia danych osobowych do celów innych niż te opisane w oświadczeniu, wniosku o opinię lub wniosku o zatwierdzenie.”.

Grupa robocza uznaje zatem, że monakijskie ustawodawstwo jest zgodne z zasadą ograniczenia celu.

Ponadto należy odnotować, że art. 10-2 ustawy również przewiduje warunki przetwarzania zgodnego z prawem w następujący sposób: „Przetwarzanie danych osobowych jest uzasadnione:

- w przypadku gdy osoba, której dane dotyczą, udzieliła zgody, lub;
- w przypadku wypełnienia zobowiązania prawnego, któremu podlega administrator danych lub jego pełnomocnik, lub;
- w przypadku gdy leży to w interesie publicznym, lub;
- w drodze realizacji umowy lub środka przed zawarciem umowy z osobą, której dane dotyczą, lub;
- w drodze wypełnienia zgodnej z prawem czynności po stronie administratora danych lub jego pełnomocnika lub odbiorcy, pod warunkiem, że interesy lub prawa podstawowe lub wolności osoby, której dane dotyczą, nie zostaną naruszone.”.

2) Jakość danych i zasada proporcjonalności: Dane powinny być dokładne oraz, w stosownych przypadkach, aktualne. Dane powinny być prawidłowe, stosowne oraz nie nadmierne ilościowo w stosunku do celów, dla których są przekazywane lub dalej przetwarzane.

Grupa robocza uznaje, że zasada jakości jest wyraźnie zawarta w art. 10-1 ustawy nr 1165.

Zgodnie z art. 10-1 „Dane osobowe muszą być: - zebrane i przetworzone rzetelnie i zgodnie z prawem; (…) - dane muszą być odpowiednie do potrzeb i istotne dla danej sprawy oraz nie mogą wykraczać poza cel, w jakim są gromadzone lub dalej przetwarzane; (…)”. Ponadto ostatnie zdanie tego artykułu ma następujące brzmienie: „Administrator danych lub jego pełnomocnik musi zapewnić zgodność z tymi przepisami”.

Podobnie zgodnie z art. 9 ustawy okres zatrzymywania danych nie może przekraczać okresu określonego we wniosku o opinię, oświadczeniu lub wniosku o zatwierdzenie, z wyjątkiem gdy dane mają być przetwarzane do celów historycznych, statystycznych lub naukowych lub gdy CCIN go zatwierdził.

Zgodnie z art. 21 ust. 4 ustawy, osoby, które zatrzymują dane osobowe dłużej niż przez okres wskazany w oświadczeniu, wniosku o opinię lub wniosku o zatwierdzenie lub dłużej niż przez okres określony przez komisję ds. kontroli danych osobowych (tj. CCIN) są zagrożone karą pozbawienia wolności od jednego miesiąca do sześciu miesięcy oraz karą grzywny określoną w art. 26 § 3 kodeksu karnego.

Grupa robocza uznaje zatem, że monakijskie ustawodawstwo jest zgodne z zasadą jakości danych i proporcjonalności.

3) Zasada przejrzystości: Osoby fizyczne powinny otrzymywać informacje na temat celu przetwarzania danych oraz tożsamości administratora danych w państwie trzecim, oraz inne informacje w zakresie, w jakim jest to konieczne dla zapewnienia rzetelnego traktowania. Jedyne dopuszczone wyjątki powinny być zgodne z art. 11 ust. 2 i 13 dyrektywy.

Ustawa przewiduje wymogi dotyczące przejrzystości w jej art.14, 14-2 i 10.

Artykuł 14 ustawy nakłada wymóg, w podobnych słowach jak art. 10 dyrektywy, żeby osoba, której dane dotyczą, była informowana przez administratora danych o:

- tożsamości administratora danych i, w stosownych przypadkach, tożsamości jego pełnomocnika w Monako;
- celu przetwarzania danych;
- obowiązkowym lub fakultatywnym charakterze odpowiedzi;
- konsekwencjach w przypadku braku odpowiedzi;
- odbiorcy lub kategoriach odbiorców danych;
- prawie do sprzeciwu, dostępu do danych i do ich poprawienia;
- swoim prawie do sprzeciwu wobec wykorzystania w imieniu osoby trzeciej swoich danych osobowych lub ich ujawnienia osobie trzeciej do celów marketingu, zwłaszcza o charakterze komercyjnym.

Artykuł przewiduje również, że: „W przypadku gdy dane osobowe nie są uzyskane bezpośrednio od osoby, której dane dotyczą, administrator danych lub jego pełnomocnik musi przedstawić osobie, której dane dotyczą, informacje, które zostały wymienione w poprzednim akapicie, z wyjątkiem gdy osoba, której dane dotyczą, została już poinformowana, nie może zostać poinformowana lub wymaga to nieproporcjonalnych środków w odniesieniu do przydatności działania lub jeżeli gromadzenie lub ujawnienie danych zostało wyraźnie przewidziane w przepisach ustawowych i wykonawczych.”.

Ponadto art. 14-2 dotyczący wykorzystania sieci łączności elektronicznej przewiduje, że abonent lub użytkownik musi otrzymać jasne i zrozumiałe informacje dotyczące celów przetwarzania oraz dostępnych środków, by nie zgodzić się na takie przetwarzanie.

Wyjątki od tego artykułu są opisane powyżej (zob. sekcja 3.2. „Zakres stosowania”) i są zgodne z wyjątkami przewidzianymi w dyrektywie.

Sankcje karne za naruszenie wymienionych wyżej przepisów są przewidziane w art. 21 ust. 6 i ust. 7 tej ustawy.

Ponadto art. 10 przewiduje prowadzenie rejestru operacji przetwarzania danych, do którego wgląd może mieć każda osoba prawna lub fizyczna i który zawiera dane szczegółowe dotyczące oświadczeń, wniosków o opinię i wniosków o zatwierdzenie odnoszących się do przetwarzania danych.

W rezultacie grupa robocza uznaje, że w monakijskim ustawodawstwie dotyczącym ochrony danych przestrzega się zasady przejrzystości.

> **4) Zasada bezpieczeństwa:** Administrator danych powinien stosować techniczne i organizacyjne środki bezpieczeństwa, które są odpowiednio dostosowane do rodzajów ryzyka związanego z przetwarzaniem. Żadnej osobie działającej z upoważnienia administratora danych, w tym przetwarzającym, nie wolno przetwarzać danych bez poleceń pochodzących od administratora danych.

Grupa robocza uznaje, że monakijskie ustawodawstwo jest zgodne z tą zasadą.

Sekcja III ustawy nr 1.165 wyraźnie dotyczy „Bezpiecznego i poufnego przetwarzania", w art. 17 zawarto wszystkie wymogi dotyczące środków bezpieczeństwa, które powinien stosować administrator danych i usługodawca i stanowi wyraźnie, iż:

„Administrator danych lub jego pełnomocnik zapewnia wprowadzenie odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą, zmianą, bezprawnym ujawnieniem lub dostępem, szczególnie wówczas gdy przetwarzanie danych obejmuje transmisję danych w sieci, jak również przed wszelkimi innymi bezprawnymi formami przetwarzania.

Wdrożone środki muszą zapewnić odpowiedni poziom bezpieczeństwa w odniesieniu do ryzyka związanego z przetwarzaniem i charakterem, danych, które mają być chronione.

W przypadkach gdy administrator danych lub jego pełnomocnik korzysta z usług jednego lub więcej usługodawców, musi dopilnować, by usługodawcy byli w stanie wypełnić zobowiązania określone w dwóch powyższych akapitach.

Przetwarzanie przeprowadzane przez usługodawcę musi być uregulowane w drodze pisemnej umowy między usługodawcą i administratorem lub jego pełnomocnikiem, w której zawarto zwłaszcza postanowienie, że usługodawca i członkowie jego personelu będą działać wyłącznie na polecenie administratora danych lub jego pełnomocnika i że zobowiązania opisane w dwóch powyższych akapitach ciążą także na danym usługodawcy.

Jeżeli usługodawca chciałby skorzystać z usług jednego lub więcej podwykonawców, by świadczyć wszystkie usługi określone w umowie, o której mowa powyżej, lub niektóre z nich, przepisy zawarte w powyższym akapicie stosuje się również do nich.".

Jak zalecono w sekcji 3.1, na potrzeby wyjaśnienia i aby uniknąć rozbieżnych wykładni, grupa robocza uznaje, że byłoby więcej niż zadowalające, gdyby w monakijskim ustawodawstwie wyraźnie zdefiniowano pojęcie „usługodawcy".

Ponadto art. 17-1 ustawy przewiduje konkretne środki bezpieczeństwa w przypadku przetwarzania dokonywanego przez organy administracji lub o szczególnym charakterze (np. dane biometryczne).

Artykuł 21 ust. 3 ustawy przewiduje karę pozbawienia wolności od jednego do sześciu miesięcy i karę grzywny określoną w art. 26 § 3 kodeksu karnego w przypadku naruszenia powyższych przepisów.

Grupa robocza uznaje zatem, że monakijskie ustawodawstwo jest zgodne z zasadą bezpieczeństwa.

5) Prawa dostępu do danych, ich poprawiania i wnoszenia sprzeciwu: Osoba, której dane dotyczą, powinna mieć prawo uzyskania kopii wszystkich przetwarzanych danych odnoszących się do niej oraz do ich poprawienia w przypadku, gdy okazały się niedokładne. W niektórych sytuacjach wspomniana osoba musi mieć również możliwość wniesienia sprzeciwu wobec przetwarzania danych, które jej dotyczą.

Jedyne wyjątki od tych praw powinny być dostosowane do przepisów art. 13 dyrektywy.

Różne artykuły odnoszą się do tych praw, a sekcja II ustawy została wyraźnie poświęcona wykonywaniu prawa dostępu do danych, sprzeciwu i poprawiania danych, jak również obowiązkom administratorów danych w odniesieniu do tych praw.

W szczególności zgodnie z art. 13 ustawy osoby fizyczne, jak i prawne, mają prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych i do dostępu do swoich danych w warunkach określonych w sekcji II ustawy, jak również do zmiany takich danych w stosownych przypadkach (art.15–16).

Artykuł 15 ustawy przewiduje prawo dostępu w sposób bardzo zbliżony do art. 12 dyrektywy. Faktycznie, „Wszystkie osoby, które mogą potwierdzić swoją tożsamość, mogą uzyskać od administratora danych i ich pełnomocnika*:*

1. informacje przynajmniej o celu przetwarzania, kategoriach odnośnych danych i odbiorców lub kategoriach odbiorców, którym dane są ujawnione;

2. potwierdzenie, czy dane odnoszące się do nich są przetwarzane;

3. takie dane przedstawione w formie pisemnej, niezakodowanej, odpowiadające przechowywanym danym;
informacje o charakterze medycznym przedstawia się osobie, której dane dotyczą, lub lekarzowi, który został do tego celu wyznaczony (...);

4. informacje odnoszące się do zautomatyzowanego procesu decyzyjnego prowadzącego do wydania decyzji określonej w art. 14-1.”.

Ponadto art. 15-1 ustawy przewiduje pośrednie prawo dostępu w przypadku przetwarzania przeprowadzanego przez organy sądowe lub administracyjne, wyłącznie w zakresie obowiązków prawnie na nie nałożonych.

Podobnie administrator danych lub jego pełnomocnik mają na podstawie art. 15-2 ustawy obowiązek podjęcia odpowiednich środków w celu zmiany niezupełnych lub błędnych danych osobowych, usunięcia danych, które mogły zostać pozyskane w sposób bezprawny, usunięcia danych pozwalających na identyfikację osoby z chwilą upływu okresu przechowywania określonego przez CCIN.

Jednocześnie w art. 16 ustawy uznaje się, w ten sam sposób jak w dyrektywie (art.12 lit. b), prawo osób, których dane dotyczą, do ich poprawienia, uzupełnienia, wyjaśnienia, zaktualizowania lub usunięcia, gdy takie dane okażą się niedokładne, niekompletne, niejednoznaczne, przestarzałe lub ich gromadzenie jest bezprawne; podobnie zgodnie z art. 16 zabronione jest ich zapisywanie, ujawnianie i przechowywanie.

Mają zastosowanie wyjątki zbliżone do art. 13 dyrektywy (zob. sekcja 3.2. „Zakres stosowania”). Ponadto w ostatnim akapicie w art. 15 ustawy przewiduje się wyjątek od obowiązku udzielenia odpowiedzi na wnioski, które ze względu na swoją liczbę lub powtarzalny i systematyczny charakter noszą znamiona nadużycia.

Artykuł 21 ust. 2 ustawy przewiduje karę pozbawienia wolności od jednego miesiąca do sześciu miesięcy i karę grzywny określoną w art. 26 § 3 kodeksu karnego w przypadku umyślnego sprzeciwu co do przekazania danych osobowych osobie, której dane dotyczą, lub zmiany lub usunięcia jakiejkolwiek z tych informacji, która okazała się niedokładna, niekompletna, niejednoznaczna, lub zgromadzona w sposób stanowiący naruszenie prawa.

Artykuł 22 ust. 5 ustawy przewiduje bardziej restrykcyjne sankcje w przypadku naruszenia prawa do wniesienia sprzeciwu wobec przetwarzania danych odnoszących się do osoby, której dane dotyczą.

Uznajemy zatem, że Monako gwarantuje prawa dostępu do danych, ich poprawienia i wnoszenia sprzeciwu, pod warunkiem że wyjątki nie są interpretowane rozszerzająco.

> **6) Ograniczenia dotyczące dalszego przekazywania:** Dalsze przekazywanie danych osobowych przez odbiorcę pierwotnego przekazania danych powinno być dopuszczalne jedynie, gdy drugi odbiorca (tj. odbiorca dalszego przekazania) również podlega przepisom zapewniającym odpowiedni poziom ochrony. Jedyne dopuszczone wyjątki powinny być zgodne z art. 26 ust. 1 dyrektywy.

Trzeci rozdział ustawy dotyczy unormowań z zakresu przekazywania danych. W szczególności art. 20 przewiduje, że do przekazania danych osobowych może dojść jedynie, gdy państwo-odbiorca zapewnia odpowiedni poziom ochrony. Odpowiedni poziom ochrony zapewniony przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazywania danych lub zestawu takich operacji; CCIN udostępnia wykaz państw zapewniających zadowalający poziom ochrony na swojej stronie internetowej.

Artykuł 20-1 ustawy ustanawia wyjątki od powyższego przepisu w niektórych okolicznościach:
- gdy osoba, której dane dotyczą, wyraziła zgodę;
- gdy przekazanie jest konieczne w związku z umową lub roszczeniem prawnym;
- gdy wymaga tego ochrona ważnego interesu publicznego;
- gdy przekazane dane pochodzą z rejestru ustanowionego ustawowo i przeznaczonego do wglądu powszechnego lub przez osoby wykazujące słuszny interes;
- gdy przekazanie jest niezbędne w celu wykonania umowy między osobą, której dane dotyczą, i administratorem danych, sporządzonej na wniosek osoby, której dane dotyczą, itp.

Ponadto, tak jak przewiduje dyrektywa (art. 26), przekazywanie danych osobowych do państwa lub organizacji, które nie zapewniają odpowiedniego poziomu ochrony, jest dopuszczalne za zezwoleniem CCIN, jeżeli administrator danych lub jego pełnomocnicy zapewnią zadowalające gwarancje, na przykład odpowiednie klauzule umowne.

Ponadto art. 21 ust. 5 ustawy przewiduje karę pozbawienia wolności od jednego do sześciu miesięcy i karę grzywny za naruszenie ograniczeń dalszego przekazywania danych.

Grupa robocza uznaje, że przepisy, które zostały przyjęte, są zgodne z zasadą ograniczenia dalszego przekazywania danych do państw trzecich.

Dodatkowo grupa robocza chciałaby zalecić, by w każdej ocenie dokonywanej przez CCIN uwzględniano wykładnię pojęcia „odpowiedniego poziomu" opracowaną w dokumencie WP 12 oraz przez odpowiednią grupę roboczą, jak również wykładnię standardowych klauzul umownych.

Grupa robocza uznaje, że monakijskie ustawodawstwo jest zgodne z zasadą dalszego przekazywania danych.

b) Dodatkowe zasady

Dokument WP 12 dotyczy niektórych zasad, które powinno się stosować w przypadku konkretnych typów przetwarzania, przy szczególnym uwzględnieniu poniższych kwestii.

1) **Dane szczególnie chronione** W przypadku gdy chodzi o kategorię danych „szczególnie chronionych" (tych, które zostały wyliczone w art. 8 dyrektywy) powinno się wprowadzić dodatkowe zabezpieczenia, takie jak wyraźna zgoda osoby, której dotyczą dane, na przetwarzanie.

Grupa robocza uznaje, że zasada ta jest uwzględniona w monakijskim ustawodawstwie dotyczącym ochrony danych, szczególnie zaś w art. 12 ustawy, który zawiera wykaz takich danych, jak również warunki przetwarzania zgodnego z prawem, które są zbieżne z przesłankami wymienionymi w art. 8 dyrektywy.

Artykuł 12 ustawy przewiduje wyraźny zakaz przetwarzania danych osobowych ujawniających

- przynależność polityczną lub opinie polityczne,
- pochodzenie rasowe lub etniczne,
- przekonania religijne lub filozoficzne,
- przynależność do związków zawodowych,
- dane dotyczące zdrowia i życia seksualnego,
- styl życia i świadczenia socjalne.

Grupa robocza zauważa, że wykaz „szczególnych kategorii danych" obejmuje również dane genetyczne, co jest zgodne z zaleceniami przyjętymi przez grupę roboczą w związku z trwającym przeglądem ram prawnych ochrony danych w UE, jak również z obecnym tekstem wniosku dotyczącego rozporządzenia w zakresie ochrony danych przedstawionego przez Komisję Europejską; obejmuje również dane odnoszące się do „stylu życia" („moeurs") i „świadczeń socjalnych", co znacząco rozszerza zakres stosowania omawianego zakazu.

Przetwarzanie tych danych może być zgodne z prawem jedynie w razie spełnienia enumeratywnie wymienionych przesłanek, które są bardzo zbliżone do przesłanek przewidzianych w dyrektywie, takich jak pisemna i wyraźna zgoda, interes publiczny, przetwarzanie przez organizację kościelną lub podmiot prowadzący działalność w celach politycznych, religijnych, filozoficznych, humanitarnych lub związkowych, przetwarzanie niezbędne do celów medycyny prewencyjnej, przetwarzanie danych odnoszące się do informacji, które zostały podane wyraźnie do wiadomości publicznej przez osobę, której dane

dotyczą, przetwarzanie wymagane do celów rejestracji, wykonywania lub obrony praw przed sądami lub by wypełnić zobowiązanie prawne.

Ponadto, zgodnie z art. 7-1 ustawy, nie przetwarza się danych osobowych do celów badań medycznych, chyba że CCIN wydał uzasadnioną opinię.

Grupa robocza odnotowuje również, że niezbędne jest uzyskanie „uprzedniego upoważnienia" CCIN zgodnie z art. 11-1 zezwalającego administratorom danych innym niż organy sądowe i administracyjne na przetwarzanie pewnych kategorii danych jak informacje dotyczące „podejrzeń prowadzenia niezgodnej z prawem działalności" lub „danych biometrycznych niezbędnych do potwierdzania tożsamości jednostek" lub „do celów prowadzenia obserwacji".

Grupa robocza uwzględnia fakt, że w praktyce artykuł ten jest stosowany przez CCIN w celu zapewnienia wyższego poziomu ochrony w drodze objęcia procedurą uzyskiwania uprzedniego upoważnienia szczególnego rodzaju przetwarzania w zakresie monitorowania i obserwacji (takiego jak nadzór wideo, geolokalizacja lub kontrola dostępu).

Ponadto art. 21 ustawy przewiduje bardziej restrykcyjne kary za nielegalne przetwarzanie danych szczególnie chronionych.

Grupa robocza uznaje zatem, że ustawa jest zgodna z wymogami ochrony danych szczególnie chronionych.

2) **Bezpośredni marketing:** w przypadku gdy dane są przekazywane do celów bezpośredniego marketingu, osoba, której dane dotyczą, powinna móc skorzystać z wariantu *opt-out*, tak by jej dane nie były wykorzystywane do takich celów na żadnym etapie.

Od 2008 r. ustawa przewiduje prawo do sprzeciwu wobec przetwarzania danych osobowych lub ich ujawniania osobom trzecim lub wykorzystywania do celów marketingu komercyjnego prowadzonego przez przetwarzającego.

Artykuł 13 ustawy przyznaje prawo sprzeciwu, z uzasadnionych powodów, osobom, których dane osobowe są przedmiotem przetwarzania.

Ponadto artykuł 14 stanowi następująco:
„Osoby, od których uzyskano dane osobowe, muszą być informowane o: [...]
- swoim prawie do sprzeciwu, dostępu do danych i do ich poprawienia;
- o swoim prawie do sprzeciwienia się wykorzystaniu ich danych osobowych w imieniu osoby trzeciej lub ujawnieniu osobie trzeciej tych danych do celów marketingu, zwłaszcza o charakterze komercyjnym. [...]".

Artykuł 21 ust. 6 i 7 przewidują kary w przypadku naruszenia przepisów powyższych artykułów.

Chociaż bardziej jednoznaczne byłoby włączenie sformułowania podobnego do art. 14 lit. b) dyrektywy UE, tj. zagwarantowania „prawa sprzeciwu, na wniosek i bez opłaty, wobec przetwarzania dotyczącego … danych osobowych, dla potrzeb bezpośredniego obrotu (…)",

grupa robocza uznaje, że w świetle wymogów dokumentu WP 12, przepisy art. 14 ustawy nr 1.165 dotyczące prawa abonenta lub użytkownika do bycia poinformowanym, w związku z art. 13, zapewniają zadowalające zabezpieczenia, w tym konkretne prawo sprzeciwu w przypadku przetwarzania do celów związanych z marketingiem bezpośrednim.

3) **Zautomatyzowane decyzje indywidualne:** W przypadku gdy celem przekazania jest podjęcie zautomatyzowanej decyzji indywidualnej w rozumieniu art. 15 dyrektywy, jednostka powinna mieć prawo do poznania przesłanek podjętej decyzji, i należy stworzyć inne sposoby zabezpieczenia uzasadnionych interesów jednostki.

Zgodnie z art. 14-1, ustawa przyznaje prawo osobie, której dane dotyczą, do niepodlegania decyzji stwarzającej skutki prawne dotyczące jej lub mające na nią znaczący wpływ, która jest oparta wyłącznie na zautomatyzowanym przetwarzaniu danych mającym na celu dokonanie oceny niektórych dotyczących jej aspektów o charakterze osobistym.

Stanowi również, iż:

„Osoba może jednak podlegać decyzji opisanej w poprzednim ustępie, jeżeli taka decyzja:

- zostanie podjęta w trakcie zawierania lub realizacji umowy, pod warunkiem że wniosek w sprawie zawarcia lub realizacji umowy, wniesiony przez osobę, której dane dotyczą, zostanie przyjęty, lub że istnieją odpowiednie sposoby zabezpieczenia jej uzasadnionych interesów, takie jak uregulowania umożliwiające jej przedstawienie swojego punktu widzenia i ponowne zbadanie wniosku;
- lub jest dopuszczona na podstawie przepisów ustawowych lub wykonawczych, które określają sposoby zabezpieczenia uzasadnionych interesów osoby."

Grupa robocza uznaje zatem, że ustawa jest zgodna z zasadą „zautomatyzowanych decyzji indywidualnych".

W końcu warto odnotować, że zgodnie z art. 7 ustawy, o przetwarzaniu przez administratorów danych, osoby prawne regulowane prawem publicznym, organy publiczne, jednostki regulowane prawem prywatnym, którym powierzono świadczenie usług w interesie publicznym, lub podmioty, które podpisały umowy na świadczenie usług użyteczności publicznej, decydują organy po wydaniu uzasadnionej opinii przez CCIN.

Mechanizmy proceduralne/wykonywania prawa

W opinii grupy roboczej WP 12 „Transfers of Personal Data to Third Countries : Applying Articles 25 and 26 of the EU data protection directive" wskazano, że by ocenić poziom ochrony w systemie prawnym danego państwa, niezbędne jest określenie celów leżących u podstaw systemu proceduralnej ochrony danych i na tej podstawie dokonanie weryfikacji szeregu różnych proceduralnych mechanizmów sądowych i pozasądowych stosowanych w państwach trzecich.

Pod tym względem cele systemu ochrony danych osobowych są głównie trojakiego rodzaju:

– zapewniają zadowalający poziom przestrzegania przepisów,

– zapewniają pojedynczym osobom, których dane dotyczą, pomoc w wykonywaniu ich praw oraz wsparcie,
– zapewniają stosowne odszkodowanie stronie, która poniosła szkodę, w razie gdy przepisy nie były przestrzegane.

a) **Zapewnienie zadowalającego poziomu przestrzegania przepisów:** dobrze funkcjonujący system charakteryzuje się wysokim stopniem świadomości administratorów danych na temat ich obowiązków i dużą wiedzą osób, których dane dotyczą, na temat ich praw oraz sposobów ich wykonywania. Istnienie skutecznych i zniechęcających sankcji może odegrać ważną rolę w zapewnieniu poszanowania przepisów, podobnie jak sprawić to mogą systemy bezpośredniej weryfikacji przez organy, audytorów lub niezależnych inspektorów ochrony danych.

1. **Wiedza administratorów danych i jednostek**

Grupa robocza uznaje, że poziom wiedzy zapewniony przez monakijskie ustawodawstwo z zakresu ochrony danych jest zadowalający w świetle ostatnich zmian (2009 r.) uprawnień i składu monakijskiego organu ds. ochrony danych, jak również niewielkich rozmiarów tego państwa.

Artykuł 6 ustawy przewiduje obowiązek uprzedniego zgłoszenia zautomatyzowanego przetwarzania danych osobowych, prowadzonego przez administratorów danych i osoby fizyczne i prawne regulowane prawem prywatnym, które obejmuje podjęcie się zobowiązania, że przetwarzanie jest zgodne z wymogami prawa.

Oświadczenia te muszą zawierać pewne elementy określone w art. 8 ustawy (np. określać dane podmiotu podpisującego oświadczenie i administratora danych, metody, cele i uzasadnienie, tożsamość osób odpowiedzialnych za używanie danych i środków umożliwiających wykonywanie prawa dostępu, kategorie osób mających dostęp do danych, kategorie danych, i dane, które są przetwarzane, ich pochodzenie, czas zatrzymywania, kategorie osób, których dotyczy przetwarzanie, i kategorie upoważnionych odbiorców, którym takie dane mogą zostać ujawnione, powiązania między danymi lub inne środki połączenia danych, jak również wszystkie operacje przekazania danych osobom trzecim, środki podjęte w celu zapewnienia bezpieczeństwa przetwarzania danych oraz dochowania tajemnic chronionych przez prawo, wskazanie w stosownych przypadkach, że przetwarzane dane mają zostać przekazane za granicę, nawet gdy uprzednie operacje przetwarzania danych miały miejsce poza Monako).

W drodze rozporządzenia ministra mogą być jednak wprowadzone w życie standardy, w następstwie wniosku lub opinii wydanej przez CCIN, określające kryteria, które muszą spełnić pewne kategorie przetwarzania, które wyraźnie nie naruszają praw podstawowych i wolności. Takie przetwarzanie może być przedmiotem uproszczonego oświadczenia zgodności lub zostać wyłączone z obowiązku składania oświadczenia, na podstawie przesłanek określonych przez wspomniane wyżej rozporządzenie ministra (art. 6).

Ponadto strona internetowa CCIN jest praktyczna i łatwa w obsłudze i zawiera pożyteczne informacje wyjaśniające przepisy ustawowe dotyczące praw i obowiązków osób fizycznych i prawnych i sposób wdrażania nowego prawa. Na stronie umieszczono również wyniki obrad CCIN, jak również sprawozdania roczne, wyjaśniające działalność tego organu.

Zgodnie z ostatnimi statystykami CCIN otrzymał w 2009 r. bardzo niewiele wniosków, co jest zrozumiałe, ponieważ był to pierwszy rok pełnienia nowych zadań przez ten organ. Rok 2010 wydaje się jednak bardzo aktywnym drugim rokiem działania: 28 opinii, 13 decyzji dotyczących wniosków o upoważnienie, 2 debaty na temat dochodzeń, 3 zalecenia, 2 wnioski w sprawie uproszczenia formalności, 1 debata w ramach konsultacji aktu prawnego, 1 debata w sprawie wewnętrznej organizacji CCIN.

CCIN uczestniczył również w 86 posiedzeniach z administratorami danych z sektora prywatnego oraz 27 z administratorami danych z sektora publicznego i udzielił odpowiedzi na 159 zapytań telefonicznych.

Ponadto art. 10 ustawy przewiduje funkcjonowanie rejestru wszystkich zbiorów danych osobowych prowadzonych w Księstwie Monako. Każda osoba fizyczna lub prawna, która chciałaby uzyskać informacje na temat administratorów danych i szczegółów związanych z przetwarzaniem, może uzyskać do niego wgląd.

Jedyną kwestią, którą można wskazać jako kontrowersyjną w nowelizacji ustawy o ochronie danych w Monako, jest brak przepisu o niezależnym inspektorze ochrony danych w sektorze prywatnym lub publicznym, któremu można byłoby powierzyć zadanie zapewnienia, w sposób niezależny, zgodności z obowiązkami przewidzianymi w tej ustawie (inspektor ochrony danych zaproponowany w art. 18 ust. 2 dyrektywy). Nie stanowi to wyraźnego wymogu w dokumencie WP 12, a jedynie zalecenie grupy roboczej dla monakijskiego ustawodawcy.

2. „Komisja ds. kontroli danych osobowych” (CCIN)

Sekcja II (od art. 2 do art. 5–6 ustawy) ustanawia komisję ds. kontroli danych osobowych jako organ nadzorczy mający za zadanie monitorowanie przepisów ustawowych i wykonawczych dotyczących ochrony danych osobowych i kontrolę zgodności z tymi przepisami, cieszący się zupełną niezależnością, na podstawie przesłanek określonych w ustawie.

Jej główne zadanie obejmuje monitorowanie przetwarzania danych osobowych przeprowadzanego w Księstwie Monako przez podmioty publiczne i prawne, jak również przez jednostki**.** Artykuł 2 ustawy określa uprawnienia komisji ds. kontroli danych osobowych, na które składają się: rejestracja, prowadzenie kontroli, udzielanie upoważnień, wydawanie opinii, sporządzanie zaleceń, prowadzenie dochodzeń, wydawanie ostrzeżeń i oficjalnych upomnień skierowanych do administratorów danych itp**.**

W odniesieniu do niezależności organizacyjnej, ustawa przewiduje w art. 2, że CCIN wykonuje swoje uprawnienia w sposób w pełni niezależny, na podstawie warunków określonych tą ustawą, w zakresie rejestrowania, upoważniania, kontroli i innych zadań, które są wymagane przez dyrektywę. Ponadto, zgodnie z art. 5 (zdanie drugie) ustawy członkowie komisji w trakcie wykonywania swoich obowiązków nie przyjmują instrukcji od żadnych organów.

Sekretarz Generalny i wszyscy członkowie oraz urzędnicy tych służb podlegają ogólnym zasadom stosowanym wobec urzędników cywilnych i funkcjonariuszy państwowych, z

wyjątkiem gdy obowiązują szczególne przepisy prawne lub wykonawcze. Jednak hierarchicznie i dyscyplinarnie podlegają wyłącznie przewodniczącemu CCIN (art.5-3).

Ponadto przewodniczący CCIN jest wybierany większością absolutną spośród jej przedstawicieli, jego mandat, jak również mandat pozostałych pięciu członków, jest ważny przez 5 lat i może być odnowiony jeden raz (art. 5).

W skład komisji ds. kontroli danych osobowych wchodzi sześciu członków zaproponowanych, ze względu na ich szczególną wiedzę ekspercką, przez konkretne i wymienione enumeratywnie organy (art. 4). Propozycje składa się niezależnie od zainteresowanych organów, rad, instytucji (art. 4), następnie są one przedstawione księciu (art. 1 rozporządzenia).

W odniesieniu do niemożności łączenia urzędów, art. 5 rozporządzenia nr 2.230 przewiduje, że nie może sprawować funkcji członka CCIN osoba sprawująca funkcję w pięciu innych organach wymienionych w tym artykule (mianowicie członek parlamentu monakijskiego lub członek jednostki samorządu terytorialnego, członek rady stanu, sędzia w służbie czynnej z wyjątkiem członka zaproponowanego przez ministra sprawiedliwości, urzędnik służby cywilnej lub urzędnik państwowy, urzędnik jednostki samorządu terytorialnego lub urzędnik instytucji państwowej, w służbie czynnej, oraz podmioty pełniące funkcje lub mające udziały w monakijskich lub zagranicznych spółkach przyczyniających się do wytwarzania sprzętu wykorzystywanego w komputerach, urządzeniach telekomunikacyjnych lub przy świadczeniu usług telekomunikacyjnych).

Ponadto urzędnicy i członkowie CCIN są zobowiązani na podstawie ustawy do zachowania tajemnicy zawodowej oraz poufności (art.5-1).

Zgodnie z art. 5-5 ustawy przewodniczący komisji zawiera wszystkie umowy i porozumienia, które są konieczne, by jego departamenty odpowiednio funkcjonowały.

Zgodnie z monakijskimi przepisami administracyjnymi i praktyką wybór przewodniczącego CCIN podlega jednak zwyczajowo radzie ministrów (a potem księciu). Umowy dotyczące zatrudnienia pracowników kontraktowych są podpisywane przez dyrekcję ds. służby cywilnej, a nie przez przewodniczącego CCIN. Na ostatnim etapie każdy awans zaproponowany przez przewodniczącego musi zostać przedłożony w dyrekcji ds. służby cywilnej, następnie przekazany do akceptacji radzie ministrów i księciu, by podjął on ostateczną decyzję.

W odniesieniu do niezależności finansowej art. 5-4 ustawy przewiduje, że niezbędne środki finansowe na funkcjonowanie wykazuje się w określonym rozdziale budżetu państwa.

Przewodniczący przygotowuje i przedkłada premierowi (*Ministre d'Etat*) propozycje obejmujące planowane dochody i wydatki. Wykaz wydatków przygotowywany jest przez sekretarza generalnego lub przewodniczącego. Rachunki komisji podlegają audytowi co roku na podstawie przesłanek określonych przez rozporządzenie (art. 5-4 ustawy).

Zgodnie z art. 28 rozporządzenia nr 2.230 przewodniczący CCIN przekazuje premierowi rachunki po ich zamknięciu, tak by mogły zostać poddane audytowi przez audytora generalnego (*Contrôleur Général des Dépenses*).

W praktyce CCIN jest objęty drobiazgową uprzednią kontrolą wydatków przez audytora generalnego. Kontrola wydaje się opierać na monakijskiej praktyce administracyjnej stosowanej w przypadku znacznej większości organów publicznych, ale nie można jej uznać za w pełni spełniającą wymóg niezależności przewidziany przez art. 28 dyrektywy.

W odniesieniu do tej kwestii istotne jest, by przywołać, że wielka izba Trybunału Sprawiedliwości Unii Europejskiej opowiedziała się za wykładnią rozszerzającą terminu „całkowita niezależność" zawartego w art. 28 dyrektywy (C-518/07 z dnia 9 marca 2010 r.):

Zatem zgodnie z orzeczeniem:

- „Z tego wynika, że przy wykonywaniu swoich obowiązków organy nadzorcze powinny działać w sposób obiektywny i bezstronny. W tym celu powinny pozostawać poza jakimkolwiek wpływem z zewnątrz, w tym bezpośrednim czy pośrednim wpływem państwa czy krajów związkowych, a nie tylko poza wpływem organów kontrolujących." (pkt 25).
- „Ta niezależność wyklucza nie tylko jakikolwiek wpływ ze strony instytucji kontrolowanych, lecz również jakiekolwiek nakazy i jakikolwiek inny wpływ z zewnątrz, bez względu na to, czy bezpośredni, czy pośredni, który mógłby podważyć wykonywanie przez te organy ich zadań polegających na ustaleniu słusznej równowagi pomiędzy ochroną prawa do poszanowania życia prywatnego a swobodą przepływu danych osobowych."(pkt 30).
- „Ponadto należy podkreślić, że samo tylko zagrożenie możliwości wpływu politycznego organów nadzoru na decyzje organów kontroli jest wystarczającą przeszkodą w niezależnym wykonywaniu przez nie zadań." (pkt 36).

CNIL, działający w charakterze sprawozdawcy, uznał, że powyższe elementy dotyczące wpływu monakijskiego rządu na rekrutację, awans personelu CCIN, jak również w odniesieniu do drobiazgowej uprzedniej kontroli wydatków CCIN, mogłyby potencjalnie podważyć niezależność CCIN, a w konsekwencji mogłyby mieć wpływ na to, czy przepisy monakijskie w zakresie ochrony danych odpowiadają wymogom europejskim.

Aby rozwiązać problemy uniemożliwiające uznanie przepisów za odpowiednie, przewodniczący CNIL wezwał do odbycia posiedzenia mediacyjnego między CCIN i monakijskim rządem w dniu 28 maja 2012 r.

Posiedzenie to doprowadziło do zawarcia porozumienia między rządem monakijskim i CCIN, mającym na celu wyjaśnienie praktyk administracyjnych i kompetencji obu stron w zakresie zasobów ludzkich i zarządzania budżetem, by wzmocnić zasadę niezależności.

Zgodnie z umową przewodniczący CCIN będzie miał uprawnienia do:
- określenia sposobu rekrutacji bez rządowej kontroli merytorycznej (*contrôle d'opportunité*) (np. sporządzenia formularza rekrutacji, określenia wymaganych umiejętność i warunków wyboru, decydowania o procesie rekrutacji i rozmowach kwalifikacyjnych);
- w przypadku gdy rekrutacja dotyczy urzędnika lub pracownika kontraktowego, CCIN powinien dopilnować, z pomocą rządu, aby warunki rekrutacji były dostosowane do obowiązujących przepisów dotyczących urzędników cywilnych i pracowników kontraktowych. Ponadto powołanie danej osoby będzie przedmiotem debaty na forum rady

ministrów. Przewodniczący CCIN jest organem uprawnionym do podpisywania umów o pracę z pracownikami kontraktowymi;
- decydowania o wewnętrznym awansie pracowników CCIN w ramach budżetu rządowego;
Ponadto porozumienie określa w sposób formalny, że nie jest dozwolone, by kontrola wydatków *a priori* przyjmowała formę kontroli merytorycznej; musi ona ograniczyć się wyłącznie do kontroli legalności.

3. Środki i mechanizmy wykonywania prawa

Rozdział III ustawy (art. 18 i 19) przewiduje środki wykonywania prawa i sankcje w odniesieniu do legalności zbiorów danych. Artykuły 13 do 15 rozporządzenia nr 2.230 przewidują również szczegółowe unormowania dotyczące dochodzenia i osób prowadzących dochodzenie.

- Zgodnie z art. 18 ustawy, członkowie powołani przez CCIN zgodnie z warunkami określonymi w ostatnim zdaniu art. 13 rozporządzenia nr 2.230, mają dostęp, od 6 rano do 9 wieczorem, do pomieszczeń, w których mają przeprowadzić kontrolę. Powinni okazać oficjalne pismo przewodniczącego CCIN i mogą zażądać wglądu do każdego dokumentu lub przesłuchania osoby, jeżeli według ich uznania jest to konieczne do celów dochodzenia.

- Artykuł 19 ustawy przewiduje kary administracyjne, które CCIN nakłada w przypadku niezgodności z ustawą (ostrzeżenie lub oficjalne upomnienie nakazujące usunięcie nieprawidłowości lub ich skutków).

W przypadku nieprawidłowości stanowiących przestępstwo CCIN powinien bezzwłocznie zwrócić się do prokuratora generalnego za pośrednictwem przewodniczącego komisji. Ponadto jeżeli administrator danych nie dostosował się do postanowień oficjalnego upomnienia, prezes sądu pierwszej instancji, do którego została przekazana sprawa przez przewodniczącego komisji, rozpoznający ją w postępowaniu przyspieszonym, orzeka o odpowiednich środkach, by usunąć nieprawidłowości lub ich skutki, bez uszczerbku dla nałożonych sankcji karnych lub roszczeń odszkodowawczych ze strony osób, których dane dotyczą i które poniosły szkodę. W orzeczeniu tym można orzec zapłatę grzywny.

- Artykuły 21 do 23 ustawy przewidują kary za naruszenie praw i przepisów ustawy. Wszystkie te kary powinny doprowadzić do ustania skutków oświadczenia lub upoważnienia i usunięcia z rejestru automatycznego przetwarzania danych osobowych.

W świetle powyższego grupa robocza uznaje, że cel, jakim jest zapewnienie dobrego poziomu zgodności, został osiągnięty tylko częściowo. W szczególności zachęca zatem monakijskie organy do przyjęcia przepisów mających na celu lepszą realizację postulatu organizacyjnej i finansowej niezależności CCIN i wzmocnienie uprawnień do wykonywania prawa, nadanych organowi w odniesieniu do zapewnienia zgodności w sektorze publicznym, i bardziej ogólnie środków nakładanych na administratorów danych, którzy nie dostosują się do przepisów ustawy, tak by wychodziły one poza zakres sankcji karnych nakładanych za pośrednictwem organów sądowych. Grupa robocza chciałaby się odnieść w tym kontekście do wykładni pojęcia „niezależności" organu ochrony danych określonego w wyroku C-518/07 Trybunału Sprawiedliwości Unii Europejskiej.

b) **Zapewnienie osobom, których dane dotyczą, pomocy w wykonywaniu ich praw oraz wsparcia:** jednostka musi mieć możliwość wykonywania swoich praw szybko i skutecznie bez ponoszenia nadmiernych kosztów. Aby mogła tak uczynić, musi istnieć rodzaj mechanizmu instytucjonalnego pozwalającego na niezależne badanie skarg.

Oprócz powyższych zastrzeżeń dotyczących niezależności CCIN, grupa robocza zauważa, że monakijskie ustawodawstwo wprowadziło różne mechanizmy mające na celu dostosowanie się do tego celu.

W szczególności:

- na CCIN został nałożony obowiązek przyjmowania skarg (art. 3) związanych z naruszeniem praw lub innych przepisów prawa (naruszenie bezpieczeństwa, zgoda na przekazanie itp.). Skargi te mogą stanowić podstawę wszczęcia kontroli CCIN i mogą doprowadzić do otwarcia postępowania o nałożenie kary administracyjnej.
- organ ma również obowiązek poinformowania osób fizycznych o ich prawach, zawiadomienia prokuratora generalnego o zdarzeniach stanowiących przestępstwo, o których się dowiedział, wydać ostrzeżenie lub formalne upomnienie skierowane do administratorów danych do celów i na podstawie przesłanek określonych tą ustawą, działać w charakterze strony w postępowaniu sądowym do celów i na podstawie przesłanek określonych tą ustawą itp. (art. 2).
- zgodnie z art. 16 ustawy osoba, której dane dotyczą, ma prawo uzyskać kopię informacji zgromadzonych, poprawionych itp. na swój temat bez żadnych opłat.
- jak wynika z powyższego CCIN ma uprawnienie do kontroli stosowania ustawy, prowadzenia dochodzeń (art.18), występowania w charakterze strony do celów i na podstawie warunków określonych niniejszą ustawą, nakładania kar administracyjnych itp.
- jak zostało pokazane powyżej, CCIN został skonsultowany 159 razy w 2010 r., co jest raczej zadowalające w świetle wielkości kraju i dopiero drugiego roku funkcjonowania na podstawie nowych przepisów.

Grupa robocza uznaje zatem, że ustawodawstwo Księstwa Monako ma wystarczające mechanizmy zapewniające wsparcie i pomoc dla jednostek.

c) **Zapewnienie stosownych środków odwoławczych dla poszkodowanej strony w przypadku naruszenia przepisów:** jest to najważniejszy element, który wiąże się z systemem niezależnego orzekania i arbitrażu umożliwiającym wypłatę kompensaty i w stosownych przypadkach nałożenie sankcji zgodnie z obowiązującymi przepisami krajowymi.

Zgodnie z art. 3 ustawy każda osoba fizyczna i prawna, której prawa zostały naruszone, lub osoby mające podstawy, by przypuszczać, że ich prawa zostały naruszone, mogą skierować sprawę do przewodniczącego CCIN, by, w stosownych przypadkach, zostały wdrożone środki określone przez ustawę, jak na przykład ostrzeżenie lub oficjalne upomnienie.

Jeżeli środki te nie zostaną zrealizowane z chwilą upływu danego okresu, prezes sądu pierwszej instancji, do którego sprawę powinien skierować przewodniczący CCIN, rozpoznający sprawę w postępowaniu przyspieszonym, nakazuje przyjęcie odpowiednich środków, by usunąć takie nieprawidłowości lub wyeliminować ich skutki, bez uszczerbku dla

nałożonych sankcji lub roszczeń odszkodowawczych ze strony osób, których dane dotyczą i które poniosły szkodę. W orzeczeniu tym można orzec zapłatę grzywny (art.19).

Warto zauważyć, że CCIN nie ma uprawnienia do nakładania sankcji karnych, ale ma uprawnienie do przekazania bezzwłocznie prokuratorowi generalnemu sprawy dotyczącej nieprawidłowości stanowiących przestępstwo.

Ponadto sąd jest uprawniony do nakładania następujących kar przewidzianych przepisami art. 21 i 22 ustawy:

- kary pozbawienia wolności od jednego do sześciu miesięcy oraz kary grzywny od 9 000 do 18 000 euro (lub jednej z nich) za naruszenie zasad dotyczących statusu danych osobowych i warunków zgodnego z prawem przetwarzania, w przypadku umyślnego sprzeciwu wobec przekazania danych osobowych osobie, której dane dotyczą, lub zmiany lub usunięcia jakiejkolwiek z tych informacji, która okazała się niedokładna, niekompletna, niejednoznaczna, lub zgromadzona w sposób stanowiący naruszenie prawa, niezwracania uwagi na środki bezpieczeństwa, przechowywania po określonym terminie, bezprawnego przekazania itp.

- kary pozbawienia wolności od trzech do dwunastu miesięcy i kary grzywny od 18 000 do 90 000 euro (lub jednej z nich) za naruszenie przepisów dotyczących przetwarzania danych osobowych szczególnie chronionych, bezprawnego gromadzenia danych, celowego zapobiegania dochodzeniu lub jego utrudniania, przekazania niewłaściwych dokumentów osobom prowadzącym dochodzenie, itp.

Ponadto sąd jest uprawniony, zgodnie z art. 23 ustawy, do zarządzenia przepadku i zniszczenia, bez odszkodowania, nośników zawierających zaskarżone dane osobowe i zabronienia ponownej rejestracji na okres przekraczający trzy lata i nie krótszy niż sześć miesięcy. Może również orzec o przypisaniu osobie prawnej prawa prywatnego, solidarnie z jej prokurentem, odpowiedzialności za zapłatę grzywny orzeczonej w stosunku do prokurenta.

Grupa robocza uznaje zatem, że monakijskie ustawodawstwo w wystarczający sposób gwarantuje prawo osoby, której dane dotyczą, do odszkodowania za każdą szkodę na jej prawach lub własności w następstwie nielegalnego przetwarzania jej danych osobowych.

3. WYNIK OCENY

Podsumowując, na podstawie powyższego i zgodnie z porozumieniem, grupa robocza uznaje, że Księstwo Monako gwarantuje odpowiedni poziom ochrony 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 tych danych.

Jednocześnie grupa robocza zachęca monakijskie organy do uwzględnienia zaleceń zawartych w tej opinii, w szczególności dotyczących:

- definicji brakujących pojęć wprowadzonych dyrektywą 95/46 (np. „zbioru danych", „przetwarzającego", „osoby trzeciej" i „osoby, której dane dotyczą");

- potrzeby wyjaśnienia, w jaki sposób przepisy mają zastosowanie do osób prawnych w świetle pierwotnego zakresu stosowania ustawy ustanowionego w art. 1.
- potrzeby wyjaśnienia prawa osób, których dane dotyczą, do bycia informowanym w odpowiednim czasie (szczególnie, kiedy dane nie zostały uzyskane bezpośrednio od osoby, której dane dotyczą), i do wniesienia sprzeciwu bez uzasadnionej podstawy wobec przetwarzania do celów marketingu bezpośredniego; w obecnym brzmieniu art. 13 i 14 ustawy nie występuje sformułowanie „bez uzasadnionej podstawy".
- konieczności zwiększenia uprawnień do wykonywania prawa, nadanych organowi w odniesieniu do zapewniania zgodności w sektorze publicznym, i nakładania środków na administratorów danych, którzy nie dostosują się do przepisów ustawy, tak by wychodziły one poza zakres wydawania ostrzeżeń, formalnych upomnień i orzekania sankcji karnych za pośrednictwem organów sądowych;
- ustanowienia instytucji niezależnych inspektorów ds. ochrony danych, by zapewnić lepsze dostosowanie się administratorów do przepisów ustawy;
- bieżącego uwzględniania decyzji Komisji Europejskiej i dokumentów Grupy Roboczej Art. 29 w kontekście oceny odpowiedniego poziomu ochrony w państwach trzecich;

Grupa robocza gratuluje ponadto CCIN i monakijskiemu rządowi podpisania porozumienia zapewniającego niezależność organu ochrony danych (CCIN) i wzywa obie strony do restrykcyjnego przestrzegania zobowiązań wynikających z warunków porozumienia.

Sporządzono w Brukseli dnia 19 lipca 2012 r.

W imieniu Grupy Roboczej
Przewodniczący
Jacob KOHNSTAMM