Międzynarodowe Standardy Ochrony Danych Osobowych i Prywatności

Rezolucja Madrycka

Prezentacja

Z przyjemnością przedstawiam Państwu Wspólną Propozycję Projektu Międzynarodowych Standardów Ochrony Prywatności w odniesieniu do przetwarzania danych osobowych, którą z zadowoleniem przyjęto podczas Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, w dniu 5 listopada 2009 r. w Madrycie.

Wspólne wysiłki organów gwarantujących ochronę prywatności z 50 krajów, koordynowane przez Hiszpańską Agencję Ochrony Danych, doprowadziły do powstania tekstu, który stara się odzwierciedlić wiele podejść, na jakie pozwala ochrona tego prawa, łącząc ustawodawstwa pięciu kontynentów. Ten będący skutkiem konsensusu dokument dodaje nowe wartości, podkreślając uniwersalny charakter zasad i gwarancji leżących u podstaw tego prawa, oraz przyczyniając się do lepszej ochrony praw i wolności osób w zglobalizowanym świecie, charakteryzującym się transgranicznymi przepływami informacji.

Od tej chwili, my organy nadzorcze i monitorujące podejmujemy wyzwanie rozpowszechniania i propagowania informacji w tym zakresie, począwszy od silnego zobowiązania do zapewniania naszym obywatelom lepszej ochrony ich prywatności i danych osobowych.

ARTEMI RALLO LOMBARTE
DYREKTOR HISZPAŃSKIEJ AGENCJI OCHRONY DANYCH

Wspólna Propozycja Projektu Międzynarodowych Standardów Ochrony Prywatności w odniesieniu do przetwarzania danych osobowych

W celu uzyskania szczegółowych informacji na temat procedury przygotowywania tego dokumentu proszę odwiedzić stronę internetową Hiszpańskiej Agencji Ochrony Danych, **www.agpd.es**, gdzie dostępne jest Memorandum wyjaśniające oraz inne przydatne dokumenty.

Część I: Postanowienia ogólne

1. Cel

Celem niniejszego dokumentu jest:

a. określenie systemu zasad i praw gwarantujących skuteczną i jednolitą dla wszystkich krajów ochronę prywatności w odniesieniu do przetwarzania danych osobowych; oraz

b. usprawnienie transgranicznych przepływów danych osobowych niezbędnych w zglobalizowanym świecie.

2. Definicje

W kontekście niniejszego dokumentu:

a) "Dane osobowe" oznaczają informacje dotyczące zidentyfikowanej osoby fizycznej lub osoby, której identyfikacja jest możliwa za pomocą środków, które można racjonalnie zastosować.

b) "Przetwarzanie" oznacza operację lub zestaw operacji, zautomatyzowanych lub nie, dokonywanych na danych osobowych, takich jak gromadzenie, przechowywanie, wykorzystywanie, udostępnianie lub usunięcie.

c) "Osoba, której dane dotyczą" to osoba fizyczna, której dane osobowe są przedmiotem przetwarzania.

d) "Osoba odpowiedzialna" to osoba fizyczna lub organizacja, publiczna lub prywatna, która, sama lub wraz z innymi, podejmuje decyzję o przetwarzaniu.

e) "Dostawca usługi przetwarzania" to osoba fizyczna lub organizacja, inna niż osoba odpowiedzialna, która prowadzi przetwarzanie danych osobowych w imieniu tej osoby odpowiedzialnej.

3. Zakres zastosowania

1. Niniejszy dokument ma mieć zastosowanie wobec wszystkich rodzajów przetwarzania danych osobowych, prowadzonych w całości lub części za pomocą środków zautomatyzowanych, lub w inny zorganizowany sposób, w sektorze publicznym lub prywatnym.

2. Właściwe ustawodawstwo krajowe może stanowić, że postanowienia niniejszego dokumentu nie mają zastosowania wobec przetwarzania danych osobowych przez osobę fizyczną w czasie działań odnoszących się wyłącznie do jej życia prywatnego lub rodzinnego.

4. Środki dodatkowe

1. Państwa mogą uzupełnić poziom ochrony danych przewidziany w tym dokumencie o dodatkowe środki gwarantujące lepszą ochronę prywatności w odniesieniu do przetwarzania danych osobowych.

2. W każdym przypadku postanowienia niniejszego dokumentu stanowią odpowiednią podstawę do wyrażenia zgody na transgraniczne przekazywanie danych osobowych, gdy tego typu przekazywanie jest prowadzone zgodnie z artykułem 15 niniejszego dokumentu.

5. Ograniczenia

Państwa mogą ograniczyć zakres postanowień określonych w artykułach 7-10 oraz 16-18 niniejszego dokumentu, gdy jest to niezbędne w demokratycznym społeczeństwie, w interesie bezpieczeństwa narodowego, bezpieczeństwa publicznego, w celu ochrony zdrowia publicznego, lub w celu ochrony praw i wolności innych osób. Takie ograniczenia muszą być wyraźnie przewidziane w krajowym ustawodawstwie, określającym należyte gwarancje i ograniczenia, mające zapewnić ochronę praw osób, których dane dotyczą.

Część II: Podstawowe zasady

6. Zasada zgodności z prawem (legalności) i rzetelności

1. Dane osobowe powinny być przetwarzane rzetelnie, z poszanowaniem właściwego prawa krajowego oraz praw i wolności osób, zgodnie z postanowieniami niniejszego dokumentu oraz celami i zasadami Powszechnej Deklaracji Praw Człowieka i Międzynarodowego Paktu Praw Obywatelskich i Politycznych.

2. W szczególności wszelkie przetwarzanie danych osobowych, które prowadzi do niezgodnej z prawem lub niesłusznej dyskryminacji osób, których dane dotyczą, uznaje się za nierzetelne.

7. Zasada określenia celu

1. Przetwarzanie danych osobowych powinno ograniczać się do spełnienia określonych, wyraźnych i zgodnych z prawem celów osoby odpowiedzialnej.

2. Osoba odpowiedzialna nie może prowadzić przetwarzania niezgodnego z celami, dla których zebrano dane osobowe, chyba że posiada jednoznaczną zgodę osoby, której dane dotyczą.

8. Zasada proporcjonalności

1. Przetwarzanie danych osobowych powinno być ograniczone do przetwarzania, które jest odpowiednie, istotne oraz nienadmierne w odniesieniu do celów określonych w poprzednim artykule.

2. W szczególności osoba odpowiedzialna powinna podjąć racjonalne wysiłki na rzecz ograniczenia ilości przetwarzanych danych osobowych do niezbędnego minimum.

9. Zasada jakości danych

1. Osoba odpowiedzialna musi cały czas zapewniać, aby dane osobowe były prawidłowe, wystarczające i aktualne w taki sposób, aby spełniać cele, dla których są przetwarzane.

2. Osoba odpowiedzialna powinna ograniczyć okres przechowywania przetwarzanych danych osobowych do niezbędnego minimum. Zatem, gdy dane osobowe stają się już niepotrzebne do wypełnienia celów uzasadniających ich przetwarzanie, muszą zostać usunięte lub zanonimizowane.

10. Zasada jawności

1. Osoba odpowiedzialna powinna posiadać przejrzystą politykę w zakresie przetwarzania danych osobowych.

2. Osoba odpowiedzialna powinna przekazać osobom, których dane dotyczą, co najmniej informacje na temat tożsamości osoby odpowiedzialnej, planowanego celu przetwarzania, odbiorców, którym ich dane osobowe zostaną ujawnione, oraz sposobu, w jaki mogą realizować swoje prawa przewidziane w tym dokumencie, jak również dalsze informacje niezbędne do zagwarantowania rzetelnego przetwarzania takich danych osobowych.

3. Gdy dane osobowe zebrano bezpośrednio od osoby, której dane dotyczą, informacje należy przekazać w momencie gromadzenia danych, chyba że zostały podane wcześniej.

4. Gdy danych osobowych nie zebrano bezpośrednio od osoby, której dane dotyczą, osoba odpowiedzialna musi także poinformować osobę, której dane dotyczą, o pochodzeniu danych osobowych. Informacje te należy zapewnić w rozsądnym terminie, ale można zamiast tego zastosować środki alternatywne, jeżeli zapewnienie zgodności jest niemożliwe lub wymagałoby nieproporcjonalnych wysiłków ze strony osoby odpowiedzialnej.

5. Wszelkie informacje, które mają być dostarczone osobie, której dane dotyczą, muszą być zapewniane w sposób zrozumiały, przy wykorzystaniu jasnego i prostego języka, w szczególności gdy przetwarzanie dotyczy niepełnoletnich.

6. W sytuacji, gdy dane osobowe są zbierane online poprzez sieci komunikacji elektronicznej, zobowiązania określone w pierwszym i drugim ustępie tego artykułu mogą być wypełnione poprzez umieszczenie polityk prywatności, które będą łatwo dostępne i łatwe do znalezienia, w tym wszystkich informacji wskazanych powyżej.

Część III: Legalność przetwarzania

11. Zasada odpowiedzialności

Osoba odpowiedzialna powinna:

a. podjąć niezbędne kroki w celu przestrzegania zasad i zobowiązań określonych w tym dokumencie oraz we właściwym ustawodawstwie krajowym, oraz

b. posiadać niezbędne mechanizmy wewnętrzne w celu zademonstrowania przestrzegania tych zasad i zobowiązań zarówno osobom, których dane dotyczą, jak i organom nadzorczym realizującym swoje uprawnienia, jak określono w artykule 23.

12. Ogólna zasada legalności

1. Co do zasady, dane osobowe mogą być przetwarzane tylko w następujących sytuacjach:

a. Po uzyskaniu dobrowolnej, jednoznacznej i świadomej zgody osoby, której dane dotyczą;

b. Gdy prawnie uzasadniony interes osoby odpowiedzialnej uzasadnia przetwarzanie, w sytuacji gdy pierwszeństwa nie mają prawnie uzasadnione interesy, prawa i wolności osób, których danych dotyczą;

c. Gdy przetwarzanie jest niezbędne do utrzymania lub wykonania stosunku prawnego między osobą odpowiedzialną a osobą, której dane dotyczą; lub

d. Gdy przetwarzanie jest niezbędne do wypełnienia zobowiązania nałożonego na osobę odpowiedzialną przez właściwe ustawodawstwo krajowe, lub jest prowadzone przez organ publiczny w ramach realizacji jego uprawnień; lub

e. Gdy zachodzą sytuacje wyjątkowe, które zagrażają życiu, zdrowiu lub bezpieczeństwu osoby, której dane dotyczą lub innej osoby.

2. Osoba odpowiedzialna musi zapewnić proste, szybkie i skuteczne procedury, które pozwalają osobom, których dane dotyczą, na wycofanie zgody w każdej chwili i które nie powodują nadmiernej zwłoki ani kosztów, ani nie przynoszą korzyści dla odpowiedzialnej osoby lub podmiotu.

13. Dane szczególnie chronione

1. Następujące dane uważa się za dane szczególnie chronione:

a. dane, które mają wpływ na najbardziej intymna sferę osoby, której dane dotyczą; lub

b. dane, które mogą przyczynić się, w przypadku niewłaściwego ich wykorzystania, do:

i. niezgodnej z prawem lub niesłusznej dyskryminacji; lub

ii. poważnego zagrożenia dla osoby, której dane dotyczą.

2. W szczególności dane osobowe, które mogą ujawnić aspekty takie, jak pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania polityczne, religijne lub filozoficzne, oraz dane dotyczące zdrowia lub życia seksualnego, uznaje się za dane o charakterze szczególnie chronionym.

3. Należy ustanowić należyte gwarancje w celu zapewnienia praw osób, których dane dotyczą, we właściwym prawie krajowym, które powinny określać dodatkowe warunki przetwarzania danych osobowych szczególnie chronionych.

14. Świadczenie usług przetwarzania

Osoba odpowiedzialna może prowadzić przetwarzanie danych osobowych za pośrednictwem jednego lub większej liczby dostawców usług, bez uznawania go za udostępnianie danych stronie trzeciej, pod warunkiem że:

a) Osoba odpowiedzialna zapewni, że dostawca usługi przetwarzania zagwarantuje co najmniej poziom ochrony wskazany w niniejszym dokumencie i we właściwym ustawodawstwie krajowym; oraz

b) Zostanie nawiązany stosunek prawny za pomocą umowy lub instrumentu prawnego, który potwierdza jego istnienie, zakres i treść, oraz określa zobowiązania dostawcy usługi przetwarzania do przestrzegania tych gwarancji oraz do zapewnienia, że dane osobowe będą przetwarzane zgodnie ze wskazówkami osoby odpowiedzialnej.

15. Transgraniczne przekazywanie danych

1. Co do zasady, transgraniczne przekazywanie danych osobowych może być prowadzone, gdy państwo, do którego takie dane są przekazywane, zapewni co najmniej poziom ochrony przewidziany w niniejszym dokumencie.

2. Możliwe będzie dokonywanie transgranicznego przekazywania danych osobowych do państw, które nie zapewniają poziomu ochrony przewidzianego w tym dokumencie, w sytuacji gdy zamierzający przekazać takie dane zagwarantują, że odbiorca zapewni taki poziom ochrony; taka gwarancja może na przykład wynikać z właściwych klauzul umownych. W szczególności, gdy przekazywanie jest dokonywane w ramach korporacji lub grup międzynarodowych, gwarancje takie mogą być określone w wewnętrznych zasadach ochrony prywatności, zgodność z którymi jest obowiązkowa.

2. Podmiot zamierzający dokonać transgranicznego przekazania danych osobowych musi z należytą starannością rozważyć, czy poziom ochrony danych zapewniony przez odbiorcę jest podobny do tego przewidzianego w niniejszym dokumencie.

3. Ponadto ustawodawstwo krajowe mające zastosowanie do podmiotów, które zamierzają przekazać dane, może zezwalać na transgraniczne przekazywanie danych osobowych do państw, które nie zapewniają poziomu ochrony przewidzianego w tym dokumencie, gdy jest to konieczne i jest to w interesie osoby, której dane dotyczą, w ramach umowy, w celu ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby, lub gdy jest to wymagane prawem na podstawie istotnego interesu publicznego.

3. Właściwe prawo krajowe może dać organom nadzorczym, o których mowa w artykule 23, uprawnienia do wyrażania zgody na niektóre lub wszystkie przypadki transgranicznego przekazywania danych podlegające ich jurysdykcji, przed ich dokonaniem. W każdym razie podmioty zamierzające prowadzić transgraniczne przekazywanie danych osobowych powinny być w stanie wykazać, że przekazanie jest zgodne z gwarancjami przewidzianymi w tym dokumencie oraz w szczególności, gdy jest to wymagane przez organy nadzorcze zgodnie z uprawnieniami określonymi w art. 23.2.

Część IV: Prawa osoby, której dane dotyczą

16. Prawo dostępu

1. Osoba, której dane dotyczą, ma prawo do uzyskania od osoby odpowiedzialnej, na wniosek, informacji na temat określonych danych osobowych będących przedmiotem przetwarzania, jak również pochodzenia takich danych, celów przetwarzania oraz odbiorców lub kategorii odbiorców, którym takie dane są lub będą udostępniane.

2. Wszelkie informacje, które mają być dostarczone osobie, której dane dotyczą, muszą być zapewniane w sposób zrozumiały, przy wykorzystaniu jasnego i prostego języka.

3. Właściwe ustawodawstwo krajowe może ograniczyć realizację tego prawa, która wymagałaby od osoby odpowiedzialnej odpowiadania na liczne wnioski w krótkim okresie, chyba że osoba, której dane dotyczą, wskaże prawnie uzasadniony powód przy realizacji tego prawa.

17. Prawo do poprawienia oraz prawo do usunięcia danych

1. Osoba, której dane dotyczą, ma prawo zwrócić się do osoby odpowiedzialnej z wnioskiem o usunięcie lub poprawienie danych osobowych, które są nieprawidłowe, niepotrzebne lub nadmierne.

2. Gdy to uzasadnione, osoba odpowiedzialna powinna dokonać wnioskowanego poprawienia lub usunięcia danych. Osoba odpowiedzialna musi zgłosić ten fakt stronom trzecim, którym dane osobowe ujawniono, gdy są one znane.

3. Usunięcie danych osobowych nie jest uzasadnione, gdy dane osobowe muszą być zatrzymane w celu realizacji zobowiązania nałożonego na osobę odpowiedzialną przez właściwe ustawodawstwo krajowe, lub ewentualnie przez umowy między osobą odpowiedzialną a osobą, której dane dotyczą.

18. Prawo do wyrażenia sprzeciwu

1. Każda osoba, której dane dotyczą, może wyrazić sprzeciw wobec przetwarzania jej danych osobowych, jeżeli istnieje ku temu prawnie uzasadniona przyczyna związana z jej osobistą sytuacją.

2. Realizacja tego prawa do wyrażenia sprzeciwu nie jest uzasadniona, gdy przetwarzanie jest niezbędne do realizacji obowiązku nałożonego na osobę odpowiedzialną przez właściwe ustawodawstwo krajowe

2. Każda osoba, której dane dotyczą, może także sprzeciwić się tym decyzjom, które wywołują skutki prawne jedynie na podstawie automatycznego przetwarzania danych osobowych, z wyjątkiem sytuacji, gdy o wydanie decyzji zwróciła się osoba, której dane dotyczą, lub gdy jest to konieczne do ustanowienia, utrzymania lub wykonania stosunku prawnego między osobą odpowiedzialną a osobą, której dane dotyczą. W tym ostatnim przypadku osoba, której dane dotyczą, musi mieć możliwość przedstawienia swojego punktu widzenia w celu ochrony jej prawa lub interesu.

19. Realizacja tych praw

1. Prawa przewidziane w artykułach 16-18 niniejszego dokumentu mogą być realizowane:

a. bezpośrednio przez osobę, której dane dotyczą, która powinna odpowiednio potwierdzić swoją tożsamość osobie odpowiedzialnej;

b. za pośrednictwem przedstawiciela, który odpowiednio potwierdzi jej/jego status osobie odpowiedzialnej.

2. Osoba odpowiedzialna musi wdrożyć procedury mające na celu umożliwienie osobom, których dane dotyczą, realizację praw przewidzianych artykułach 16-18 niniejszego dokumentu w prosty, szybki i skuteczny sposób, nie przyczyniając się do nadmiernej zwłoki ani kosztów, czy też zysków dla osoby odpowiedzialnej.

3. W przypadku, gdy osoba odpowiedzialna dojdzie do wniosku, że, zgodnie z właściwym ustawodawstwem krajowym, realizacja praw przewidzianych w tej Części nie jest uzasadniona, powinna poinformować osobę, której dane dotyczą, o powodach wyciągnięcia takiego wniosku.

Część V: Bezpieczeństwo

20. Środki bezpieczeństwa

1. Zarówno osoba odpowiedzialna, jak i każdy dostawca usługi przetwarzania, muszą chronić dane osobowe będące przedmiotem przetwarzania za pomocą odpowiednich środków technicznych i organizacyjnych w celu zapewnienia, za każdym razem, integralności, poufności i dostępności. Środki te zależą od istniejącego ryzyka, możliwych konsekwencji dla osób, których dane dotyczą, wrażliwego charakteru danych osobowych, stanu rzeczy, kontekstu, w jakim prowadzone jest przetwarzanie, oraz, gdy to właściwe, od zobowiązań przewidzianych we właściwym ustawodawstwie krajowym.

2. Podmioty zaangażowane w jakikolwiek etap przetwarzania muszą informować osoby, których dane dotyczą, o każdym naruszeniu bezpieczeństwa, które może znacząco wpłynąć na prawa majątkowe i niemajątkowe osób, których dane dotyczą. Informacje te należy dostarczyć we właściwym czasie, aby umożliwić osobom, których dane dotyczą, domaganie się ochrony ich praw.

21. Obowiązek zachowania poufności

Osoba odpowiedzialna oraz podmioty zaangażowane w którykolwiek etap przetwarzania danych osobowych są zobowiązani do zachowania poufności danych osobowych. Obowiązek ten obowiązuje nawet po zakończeniu relacji z osobą, której dane dotyczą, lub, gdy to właściwe, z osobą odpowiedzialną.

Część VI: Zgodność i nadzór

22. Środki proaktywne

Państwa powinny, poprzez swoje prawo krajowe, zachęcać podmioty zaangażowane w którykolwiek etap przetwarzania, do wdrażania środków w celu propagowania większej zgodności z mającymi zastosowanie przepisami w zakresie ochrony prywatności w odniesieniu do przetwarzania danych osobowych. Środki takie mogłyby obejmować między innymi:

a) Wdrożenie procedur w zakresie zapobiegania i wykrywania naruszeń, które mogą być oparte na ujednoliconych modelach zarządzania i/lub kontroli nad bezpieczeństwem informacji.

b) Powołanie jednego lub kilku urzędników ds. ochrony danych lub prywatności, posiadających odpowiednie kwalifikacje, środki i uprawnienia do właściwej realizacji przysługujących im funkcji nadzorczych.

c) Okresowe wdrażanie programów szkoleniowych, edukacyjnych i informacyjnych wśród członków organizacji, mających na celu lepsze zrozumienie obowiązujących przepisów dotyczących ochrony prywatności w odniesieniu do przetwarzania danych, osobowych, jak również procedur ustanowionych przez organizację w tym celu.

d) Okresowe przeprowadzanie przejrzystych audytów przez wykwalifikowane i najlepiej niezależne strony służących zweryfikowaniu zgodności prowadzonych działań z obowiązującymi przepisami w zakresie ochrony prywatności w odniesieniu do przetwarzania danych osobowych oraz z procedurami ustanowionymi przez organizację w tym celu.

e) Dostosowanie systemów informatycznych i/lub technologii wykorzystywanych do przetwarzania danych osobowych do obowiązujących przepisów w zakresie ochrony prywatności w odniesieniu do przetwarzania danych osobowych, w szczególności w momencie podejmowania decyzji dotyczących ich parametrów technicznych oraz ich rozwoju i wdrażania.

f) Przeprowadzanie oceny wpływu na prywatność, przed wprowadzeniem nowych systemów informatycznych i/lub technologii służących do przetwarzania danych osobowych, jak również przed zastosowaniem każdej nowy metody przetwarzania danych osobowych, lub przed wprowadzeniem istotnych zmian w już prowadzonym przetwarzaniu.

g) Przyjęcie kodeksów postępowania, których przestrzeganie jest wiążące i które obejmują elementy, które umożliwiają badanie skuteczności pod względem zgodności i poziomu ochrony danych osobowych, oraz które określają skutecznie środki w przypadku braku zgodności.

h) Wdrożenie planu reagowania, który ustanawia wytyczne w zakresie działań podejmowanych w przypadku weryfikacji naruszeń obowiązujących przepisów w zakresie ochrony prywatności w odniesieniu do przetwarzania danych osobowych, w tym co najmniej obowiązek ustalenia przyczyny i zakresu naruszenia, w celu opisania jego szkodliwych skutków oraz podjęcia odpowiednich środków, aby uniknąć naruszeń w przyszłości.

23. Monitoring

1. W każdym państwie musi istnieć jeden lub więcej organów nadzorczych, zgodnie z prawem krajowym, które będą odpowiedzialne za nadzór nad przestrzeganiem zasad określonych w niniejszym dokumencie.

2. Organy nadzorcze muszą być bezstronne i niezależne oraz posiadać kwalifikacje techniczne. Muszą także posiadać wystarczające uprawnienia i odpowiednie środki do rozpatrywania skarg składanych przez osoby, których dane dotyczą, oraz do prowadzenia dochodzeń i interwencji, gdy jest to konieczne do zapewnienia zgodności z obowiązującymi przepisami w zakresie ochrony prywatności w odniesieniu do przetwarzania danych osobowych.

3. W każdym przypadku, bez szkody dla jakichkolwiek administracyjnych środków odwoławczych przed organami nadzorczymi wskazanymi w poprzednich ustępach, osoba, której dane dotyczą, może zwrócić się do sądu w celu egzekwowania swoich praw wynikających z przepisów określonych we właściwym ustawodawstwie krajowym.

24. Współpraca i koordynacja

1. Organy wymienione w poprzednim artykule postarają się współpracować ze sobą w celu osiągnięcia bardziej jednolitej ochrony prywatności w odniesieniu do przetwarzania danych osobowych, zarówno na poziomie krajowym, jak i międzynarodowym.

2. Organy te dodatkowo dołożą należytych starań na rzecz:

a) Wymiany raportów, technik dochodzeniowych, komunikacji i strategii regulacyjnych oraz wszelkich innych przydatnych informacji w celu bardziej skutecznej realizacji swoich funkcji, w szczególności współpracy z innym organem nadzorczym, na jego wniosek, w zakresie prowadzenia dochodzeń lub interwencji;

b) Prowadzenia skoordynowanych dochodzeń lub interwencji, zarówno na poziomie krajowym, jak i międzynarodowym, w sprawach będących przedmiotem zainteresowania jednego lub większej liczby organów;

c) Uczestnictwa w stowarzyszeniach, grupach roboczych i wspólnych forach, jak również seminariach, warsztatach lub kursach, które przyczyniają się do przyjmowania wspólnych stanowisk lub do poprawiania technicznych umiejętności pracowników takich organów nadzorczych;

d) Utrzymywania odpowiedniego poziomu poufności informacji wymienianych podczas współpracy.

3. Państwa będą zachęcać do negocjowania umów o współpracy między organami nadzorczymi, regionalnymi, krajowymi i międzynarodowymi, które przyczynią się do skuteczniejszego przestrzegania tego artykułu.

25. Odpowiedzialność

1. Osoba odpowiedzialna ponosi odpowiedzialność za wszelkie szkody wynikłe dla osób, których dane dotyczą, z przetwarzania danych osobowych, które naruszyło właściwe przepisy w zakresie ochrony prywatności w odniesieniu do przetwarzania danych osobowych, z wyjątkiem sytuacji, gdy osoba odpowiedzialna może wykazać, że nie można jej przypisać wyrządzenia szkody. Odpowiedzialność ta jest bez uszczerbku dla jakiegokolwiek działania osoby odpowiedzialnej przeciwko dostawcy usług przetwarzania zaangażowanemu w jakikolwiek etap przetwarzania.

2. Państwa są zobowiązane do propagowania odpowiednich środków ułatwiających osobom, których dane dotyczą, dostęp do właściwych procedur sądowych lub administracyjnych, które umożliwią im uzyskanie wyrównania szkody, o której mowa w poprzednim ustępie.

3. Wyżej wspomniana odpowiedzialność powinna istnieć bez uszczerbku dla przewidzianych sankcji karnych, cywilnych lub administracyjnych, gdy to właściwe, w przypadku naruszenia przepisów ustawodawstwa krajowego w zakresie ochrony prywatności w odniesieniu do przetwarzania danych osobowych.

4. Przy ustalaniu odpowiedzialności i sankcji przewidzianych w tym artykule należy rozważyć wdrożenie środków proaktywnych, takich jak te opisane w artykule 22 niniejszego dokumentu.

PROJEKT REZOLUCJI W SPRAWIE MIĘDZYNARODOWYCH STANDARDÓW OCHRONY PRYWATNOŚCI

Projektodawcy: Hiszpańska Agencja Ochrony Danych (Hiszpania)
Federalny Rzecznik Ochrony Danych i Prywatności (Szwajcaria)
Europejski Inspektor Ochrony Danych
Krajowa Komisja ds. Informatyki i Wolności (Francja)
Irlandzki Rzecznik Ochrony Danych
Rzecznik Ochrony Prywatności Kanady
Urząd Rzecznika Ochrony Danych (Republika Czeska)
Federalny Rzecznik Ochrony Danych i Wolności Informacji (Niemcy)
Garante per la Protezione dei Dati Personali (Włochy)
College Bescherming Persoonsgegevens (Holandia)
Rzecznik Ochrony Prywatności Nowej Zelandii
Urząd Rzecznika Ochrony Informacji (Zjednoczone Królestwo)

Współautorzy: Agencja Ochrony Danych Andory (Andora)
Katalońska Agencja Ochrony Danych (Hiszpania)
Agencja Ochrony Danych Regionu Madryt (Hiszpania)
Baskijska Agencja Ochrony Danych (Hiszpania)
Urząd Inspektora Ochrony Danych (Wyspa Man)
Estoński Inspektorat Ochrony Danych
Krajowy Inspektorat Ochrony Danych Republiki Litwy
Berliński Rzecznik Ochrony Danych i Wolności Informacji (Niemcy)
Rzecznik Ochrony Danych Landu Szlezwik-Holsztyn (Niemcy)
Krajowa Dyrekcja Ochrony Danych Osobowych (Argentyna)
Rzecznik Ochrony Danych (Malta)
Komisja ds. Komputerów i Wolności (Burkina-Faso)
Rzecznik Ochrony Danych Osobowych (Cypr)
Rzecznik Ochrony Danych (Finlandia)
Rzecznik Ochrony Informacji (Słowenia)
Grecki Organ Ochrony Danych (Grecja)

Zważywszy że:

30 Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności w Strasburgu jednogłośnie przyjęła Rezolucję dotyczącą naglącej potrzeby ochrony prywatności w świecie bez granic oraz w sprawie wypracowania Wspólnej Propozycji stworzenia Międzynarodowych Standardów Ochrony Prywatności i Danych Osobowych.

Rezolucja wyznaczyła zadanie ustanowienia Grupy Roboczej, która miała być koordynowana przez Hiszpańską Agencję Ochrony Danych jako gospodarza 31 Konferencji i w której jej skład miały wejść zainteresowane organy ochrony danych, w celu sporządzenia projektu Wspólnej propozycji ustanowienia międzynarodowych standardów ochrony prywatności i danych osobowych i przedłożenia tego projektu podczas 31 Konferencji.

Zgodnie z tym zadaniem, Hiszpańska Agencja Ochrony Danych utworzyła Grupę Roboczą oraz propagowała i koordynowała prace nad opracowaniem Wspólnej Propozycji Projektu Międzynarodowych Standardów.

Grupa Robocza przygotowała Wspólną Propozycję Projektu Międzynarodowych Standardów Ochrony Danych i Prywatności w odniesieniu do przetwarzania danych osobowych, w oparciu o zasady, które zawarte są w różnych instrumentach, wytycznych lub rekomendacjach o międzynarodowym zakresie i które uzyskały szeroki konsensus we właściwych obszarach geograficznych, ekonomicznych lub prawnych.

Wspólną Propozycję opracowano przy założeniu, że wszystkie te zasady i podejścia wnoszą elementy znaczące przy ochronie i poprawianiu ochrony prywatności i danych osobowych, w celu poszerzenia ich o rozwiązania i określone przepisy, które mogą mieć zastosowanie niezależnie od wszelkich różnic, które mogą istnieć między różnymi istniejącymi modelami ochrony danych i prywatności.

Konferencja przyjmuje Rezolucję w sprawie:

1. Przyjęcia z zadowoleniem Wspólnej Propozycji Projektu Międzynarodowych Standardów Ochrony Prywatności w odniesieniu do przetwarzania danych osobowych, stanowiącej Załącznik nr 1 do niniejszej rezolucji. Wspólna Propozycja wskazuje na wykonalność takich standardów, jako nowy krok w kierunku opracowania wiążącego międzynarodowego instrumentu w odpowiednim czasie.

2. Stwierdzenia, że Wspólna Propozycja przedstawia szereg zasad, praw, obowiązków i procedur, do których przestrzegania powinien dążyć każdy system prawny ochrony danych i

prywatności. Z tej perspektywy, przetwarzanie danych osobowych w sektorze publicznym i prywatnym prowadzone będzie, w bardziej ujednoliconym pod względem międzynarodowym podejściu:

a. rzetelnie, zgodnie z prawem i w sposób proporcjonalny w odniesieniu do określonych, wyraźnych i zgodnych z prawem celów;

b. w oparciu o przejrzyste polityki, przy odpowiednim poinformowaniu osób, których dane dotyczą, oraz bez niesłusznej dyskryminacji tych osób;

c. z zapewnieniem prawidłowości, poufności i bezpieczeństwa danych oraz legalności przetwarzania, a także praw osób, których dane dotyczą, do dostępu do danych, ich poprawiania, usuwania oraz do wyrażenia sprzeciwu wobec ich przetwarzania;

d. z wdrożeniem zasad rozliczalności i odpowiedzialności, nawet gdy operacje przetwarzania prowadzone są przez dostawców usług w imieniu administratora;

e. przy zapewnieniu bardziej odpowiednich gwarancji, gdy dane mają charakter szczególnie chroniony;

f. z zapewnieniem, że dane osobowe przekazywane za granicę będą miały zapewniony poziom ochrony przewidziany przez wyżej wskazany zestaw standardów;

g. podlegając nadzorowi niezależnych i bezstronnych organów nadzorczych, posiadających odpowiednie uprawnienia i środki także w związku z ich obowiązkiem współpracy między sobą;

h. w ramach nowej, nowoczesnej struktury środków proaktywnych, takich jak te ukierunkowane w szczególności na zapobieganie i wykrywanie naruszeń oraz oparte na powołaniu urzędników ds. ochrony prywatności, jak również na skutecznych kontrolach oraz ocenach wpływu na prywatność.

3. Zaproszenia organów ochrony danych i prywatności akredytowanych na Międzynarodową Konferencję do jak najszerszego rozpowszechnienia Wspólnej Propozycji Projektu Międzynarodowych Standardów Ochrony Prywatności w odniesieniu do przetwarzania danych osobowych.

4. Powierzenia organom organizującym 31 i 32 Międzynarodową Konferencję zadania koordynowania Grupy ds. Promocji, w której skład wejdą zainteresowane organy ochrony danych i która będzie odpowiedzialna za:

a. rozpowszechnianie i propagowanie Wspólnej Propozycji wśród właściwych podmiotów prywatnych, ekspertów oraz organów krajowych i międzynarodowych, jako podstawy do opracowania wiążącej międzynarodowej konwencji, a w szczególności wśród organów i organizacji wskazanych w Deklaracji z Montreux; oraz

b. badanie i informowanie o innych sposobach wykorzystania Wspólnej Propozycji jako podstawy do wypracowania międzynarodowego porozumienia i współpracy w zakresie ochrony danych i prywatności, w szczególności w kontekście umożliwienia, aby międzynarodowe przepływy danych osobowych miały miejsce w sposób, które zabezpiecza prawa i wolności osób.

5. Zwrócenia się do Grupy ds. Promocji z wnioskiem o:

a. koordynowanie jej pracy z Konferencyjnym Komitetem Sterującym ds. Reprezentacji na posiedzeniach organizacji międzynarodowych, oraz

b. przekazanie informacji na temat istotnych postępów podczas 32 Międzynarodowej Konferencji w celu zapewnienia, że niniejsza rezolucja nadal będzie przedmiotem uwagi.

Nota wyjaśniająca

30 Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności przyjęła Rezolucję dotyczącą naglącej potrzeby ochrony prywatności w świecie bez granic oraz w sprawie wypracowania Wspólnej Propozycji stworzenia Międzynarodowych Standardów Ochrony Prywatności i Danych Osobowych, przedłożonej wspólnie przez organy ochrony danych Szwajcarii i Hiszpanii oraz popartej przez dwadzieścia innych organów.

W rezolucji tej Konferencja przypomniała szereg deklaracji i rezolucji przyjętych w ciągu ostatnich dziesięciu lat, które miały na celu wzmocnienie uniwersalnego charakteru prawa do ochrony danych osobowych i prywatności i wezwanie do opracowania uniwersalnej konwencji o ochronie prywatności osób fizycznych w odniesieniu do przetwarzania danych osobowych.

Ponadto, w rezolucji stwierdzono, że prawo do ochrony danych i prywatności jest podstawowym prawem każdego człowieka, niezależnie od narodowości i miejsca zamieszkania, zauważając że ciągłe różnice jeśli chodzi o poziom ochrony danych osobowych i prywatności wynikające głównie z faktu, że wiele krajów nie wprowadziło jeszcze odpowiednich przepisów, źle wpływają na możliwość wymiany danych i możliwość wprowadzenia efektywnej ochrony na szczeblu globalnym.

W związku z tym w rezolucji wyrażono przekonanie Konferencji, że uznanie tych praw wymaga przyjęcia uniwersalnego, prawnie wiążącego instrumentu określającego, bazującego na i uzupełniającego powszechne zasady ochrony danych i prywatności określone w kilku istniejących instrumentach oraz wzmacniającego międzynarodową współpracę organów ochrony danych.

W tym zakresie, w rezolucji wyrażono poparcie Konferencji dla wysiłków Rady Europy na rzecz poprawy ochrony podstawowych praw do ochrony danych i prywatności. Zachęcono także państwa, będące jak i niebędące członkami tej organizacji, do ratyfikowania Konwencji o ochronie osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych oraz jej protokołu dodatkowego, potwierdzając jednocześnie wsparcie Konferencji dla działań prowadzonych przez APEC, OECD oraz inne regionalne i międzynarodowe fora w celu opracowania skutecznych środków służących propagowaniu lepszych międzynarodowych standardów ochrony prywatności i danych osobowych.

Rezolucja powierzyła Hiszpańskiej Agencji Ochrony Danych, jako gospodarzowi 31 Międzynarodowej Konferencji, zadanie ustanowienia i koordynowania Grupy Roboczej, w której skład miały wejść zainteresowane organy ochrony danych, w celu sporządzenia projektu Wspólnej propozycji ustanowienia międzynarodowych standardów ochrony danych osobowych i prywatności i przedłożenia tego projektu podczas sesji zamkniętej Konferencji.

Rezolucja zawierała listę kryteriów regulujących proces przygotowywania projektu tej Wspólnej Propozycji, a w szczególności wskazała, że musi on być opracowywany przy zachęcaniu do szerokiego udziału organizacji i podmiotów publicznych i prywatnych, w celu uzyskania jak najszerszego konsensusu instytucjonalnego i społecznego.

Zgodnie z tym zadaniem, Hiszpańska Agencja Ochrony Danych utworzyła Grupę Roboczą, o której mowa w rezolucji, oraz propagowała i koordynowała prace nad opracowaniem Wspólnej Propozycji Projektu Międzynarodowych Standardów.

Hiszpańska Agencja Ochrony Danych wysłała zaproszenia do udziału w Grupie Roboczej wszystkim organom ochrony danych i prywatności akredytowanym na Międzynarodową Konferencję. Organy wymienione w Załączniku nr 2* wyraziły chęć uczestniczenia w Grupie Roboczej oraz w rezultacie przystąpiły do niej.

Grupa Robocza odbyła posiedzenia w styczniu i czerwcu 2009 r. Podczas pierwszego posiedzenia osiągnięto porozumienie co do metody przygotowywania projektu Wspólnej Propozycji oraz jego zakresu rzeczowego, zaś podczas drugiego posiedzenia omówiono i

dopracowano wersję projektu propozycji celem następnego przedłożenia podczas 31 Konferencji.

Zgodnie z kryteriami i metodologią przedstawionymi w Rezolucji ze Strasburga oraz ustalonymi przez Grupę Roboczą, Hiszpańska Agencja Ochrony Danych prowadziła intensywną działalność i wypracowała różnorodne dokumenty, zawierające wkłady od organów ochrony danych i prywatności oraz innych publicznych podmiotów związanych z ochroną danych, jak również od ekspertów z sektora, branży prawniczej, organizacji akademickich i międzynarodowych oraz organizacji pozarządowych.

W szczególności Grupa Robocza przygotowała Wspólną Propozycję Projektu Międzynarodowych Standardów Ochrony Prywatności w odniesieniu do przetwarzania danych osobowych, w oparciu o zasady, które zawarte są w różnych instrumentach, wytycznych lub rekomendacjach o międzynarodowym zakresie i które uzyskały szeroki konsensus we właściwych obszarach geograficznych, ekonomicznych lub prawnych.

Wspólną Propozycję opracowano przy założeniu, że wszystkie te zasady i powszechne podejścia wnoszą elementy znaczące przy ochronie i poprawianiu ochrony prywatności i danych osobowych, w celu poszerzenia ich o rozwiązania i określone przepisy, które mogą mieć zastosowanie niezależnie od wszelkich różnic, które mogą istnieć między różnymi istniejącymi modelami ochrony danych i prywatności.

* ORGANY NALEŻĄCE DO GRUPY ROBOCZEJ: KOMISJA OCHRONY DANYCH (Austria), KOMISJA OCHRONY PRYWATNOŚCI (Belgia), KOMISJA DS. KOMPUTERÓW I WOLNOŚCI (Burkina-Faso), URZĄD RZECZNIKA OCHRONY PRYWATNOŚCI KANADY, KOMISJA DOSTĘPU DO INFORMACJI QUEBEKU (Kanada), URZĄD OCHRONY DANYCH OSOBOWYCH (Republika Czeska), EUROPEJSKI INSPEKTOR OCHRONY DANYCH, KRAJOWA KOMISJA DS. INFORMATYKI I WOLNOŚCI (Francja), FEDERALNY RZECZNIK OCHRONY DANYCH (Niemcy), BERLIŃSKI RZECZNIK OCHRONY DANYCH I WOLNOŚCI INFORMACJI (Niemcy), RZECZNIK OCHRONY DANYCH LANDU SZLEZWIK-HOLSZTYN (Niemcy), RZECZNIK OCHRONY PRYWATNOŚCI I DANYCH OSOBOWYCH (Hong Kong), IRLANDZKI RZECZNIK OCHRONY DANYCH, WŁOSKI ORGAN OCHRONY DANYCH, KOMISJA OCHRONY DANYCH (Holandia), RZECZNIK OCHRONY PRYWATNOŚCI NOWEJ ZELANDII, KRAJOWA KOMISJA OCHRONY DANYCH (Portugalia), RZECZNIK OCHRONY INFORMACJI REPUBLIKI SŁOWENII, HISZPAŃSKA AGENCJA OCHRONY DANYCH (Hiszpania), KATALOŃSKI ORGAN OCHRONY DANYCH (Hiszpania), AGENCJA OCHRONY DANYCH REGIONU MADRYT (Hiszpania), BASKIJSKA AGENCJA OCHRONY DANYCH (Hiszpania), FEDERALNY RZECZNIK OCHRONY DANYCH (Szwajcaria), URZĄD RZECZNIKA OCHRONY INFORMACJI (Zjednoczone Królestwo).