

## Rezolucja Konferencji Europejskich Organów Ochrony Danych 18-20 maja 2015 r. – Manchester, Zjednoczone Królestwo

### Spełnienie oczekiwań w zakresie ochrony danych w cyfrowej przyszłości

#### **Wnioskodawca:**

Urząd Rzecznika Informacji, Zjednoczone Królestwo

#### **Współwnioskodawcy:**

Garante per la Protezione dei Dati Personali, Włochy  
Comissão Nacional de Protecção de Dados, Portugalia

#### **Preambuła**

Świat ogromnie się zmienił od czasu przyjęcia Konwencji 108 Rady Europy oraz obecnej Europejskiej Dyrektywy o Ochronie Danych 95/46. Osoby fizyczne słusznie oczekują od organów ochrony danych odpowiedzi na te zmiany. Nowe technologie i usługi cyfrowe stale ewoluują.

Zbiera się, udostępnia i analizuje coraz więcej danych osobowych w bardziej skomplikowane i potencjalnie inwazyjne sposoby. Osoby fizyczne coraz bardziej polegają na Internecie w celu dokonywania transakcji z podmiotami publicznymi i prywatnymi, uzyskania dostępu do informacji oraz interakcji z innymi.

To w kontekście tego zawsze zmieniającego się świata cyfrowego, jego wyzwań globalnych, modernizacji Konwencji 108 oraz pojawienia się pakietu reformy ochrony danych UE europejskie organy ochrony danych napotykają wiele nowych wyzwań, z implikacjami dla sposobu, w jaki wypełniają swoje funkcje w zakresie propagowania i ochrony praw do ochrony danych.

Miejsce ochrony danych i prywatności w agendzie publicznej jest złożoną kwestią. Niektórzy obywatele mogli zaakceptować fakt, że udostępnianie ich danych osobowych stało się po prostu częścią nowoczesnego życia, ale nie

oznacza to, że poddali się w kwestii ochrony prywatności. Istnieją przekonujące dowody wskazujące, że w praktyce wielu obywateli coraz częściej obawia się utracenia kontroli nad ich danymi osobowymi, ponieważ systemy stają się bardziej złożone, a wykorzystywanie tych systemów staje się nieuniknione w dzisiejszym społeczeństwie.

Mimo wysokiego poziomu obaw obywateli co do ich prywatności i ochrony danych osobowych, szczególnie w kontekście cyfrowym, istnieje względnie niski poziom świadomości publicznej zarówno na temat istnienia organów ochrony danych, jak i ich kluczowej roli w ochronie prawa osób do ochrony danych. Oznacza to, że istnieje potrzeba nie tylko podniesienia świadomości obywateli na temat ich praw dotyczących ochrony danych, ale również podniesienia świadomości publicznej na temat ważnej roli organów ochrony danych w ochronie danych osobowych.

Jednak organy ochrony danych coraz częściej napotykają ograniczenia finansowe i inne ograniczenia w zakresie zasobów, podczas gdy jednocześnie rosną stawiane im oczekiwania. Nie tylko prawo musi dotrzymać kroku bezustannie zmieniającemu się światu cyfrowemu, ale również możliwości organów ochrony danych w zakresie skutecznego nadzoru na poziomie krajowym, UE i szerszym poziomie europejskim. Jeżeli osoby fizyczne mają mieć zaufanie i ufność niezbędne dla pełnej sukcesów przyszłości, uprawnienia i zasoby dostępne dla organów ochrony danych muszą być wystarczające do umożliwienia im odpowiedniej ochrony praw podstawowych i wolności osób w erze cyfrowej.

Nie jest to jedynie kwestia zasobów. Niezbędne jest również, aby organy ochrony danych przyjęły zrównoważone podejście na poziomie krajowym, UE i szerszym europejskim poziomie w celu wykonywania swoich funkcji, adresowania swoich działań tam, gdzie potrzeba ochrony prywatności jest największa oraz posiadania dokładnego zrozumienia wpływów nowych i istniejących technologii na prywatność.

\*\*\*

## **Europejska Konferencja Organów Ochrony Danych**

- *Odnotowując* że Protokół dodatkowy do Konwencji nr 108 Rady Europy uznaje, że organy nadzorcze są niezbędnym elementem skutecznej ochrony osób fizycznych w odniesieniu do przetwarzania ich danych osobowych oraz że aby być skutecznymi, takie organy winny działać całkowicie niezależnie oraz muszą posiadać niezbędne uprawnienia i zasoby do wypełniania swoich obowiązków.
- *Zauważając również*, że artykuł 8 Karty Praw Podstawowych Unii Europejskiej przewiduje prawo do ochrony danych osobowych oraz że to prawo obejmuje kontrolę zgodności z zasadami ochrony danych przez niezależny organ nadzorczy.
- *Dalej odnotowując*, że ostatnio zrewidowane Wytyczne OECD regulujące ochronę prywatności i transgraniczne przepływy danych osobowych zawierają

przepis stanowiący, że państwa członkowskie powinny ustanowić i utrzymać organy ds. egzekwowania prawa z uprawnieniami zarządczymi, zasobami i specjalistyczną wiedzą techniczną niezbędnymi do skutecznej realizacji ich uprawnień.

- *Zważywszy odpowiednio* na istotną rolę, jakiej odgrywania oczekuje się od silnych, niezależnych organów ochrony danych przy ochronie praw i wolności osób w erze cyfrowej.
- *Zważywszy że* bez niezbędnych uprawnień i wystarczających zasobów organy ochrony danych nie będą w stanie pełnić swojej istotnej roli, która obejmuje lepsze zrozumienie obaw i oczekiwań osób w celu zapewnienia im skutecznej ochrony prywatności.
- *Uznając że* nieuchronnie pozostawi to osoby bez skutecznych zabezpieczeń i tym samym zagrozi zaufaniu publicznemu i ufności w przyszłość cyfrową.
- *Przypominając że* znaczeniem finansowania i niezależności organów ochrony danych zajął się wcześniej Trybunał Sprawiedliwości Unii Europejskiej<sup>1</sup>.
- *Świadomi że* prawa i obowiązki na papierze zawsze muszą być możliwe do wyegzekwowania i zapewnienia, a inaczej będą one w najlepszym przypadku złudzeniem, a w najgorszym przypadku oszukiwaniem obywateli.

**1. Wzywa Komisję Europejską i rządy krajów europejskich** do zapewnienia, że finansowanie organów ochrony danych będzie wystarczające do sprostania nieustannie rosnącym nakładom na nie wymaganiom oraz do zapewnienia, że wymogi określone przez ustawodawców będą należycie przestrzegane w praktyce. Musi to uwzględnić potrzebę wzajemnej współpracy oraz być osiągnięte w sposób szanujący i utrzymujący ich niezbędną niezależność.

**2. Wzywa ustawodawców w całej Europie** do zapewnienia, że, o ile to możliwe, następna generacja przepisów w zakresie ochrony danych będzie opracowana w jasny i prosty sposób oraz że przepisy te będą zrozumiałe i stosowane przez organizacje, osoby fizyczne i organy ochrony danych, tak aby były tak skuteczne jak to możliwe w zapewnianiu w praktyce wysokiego standardu ochrony danych, do którego osiągnięcia dążą.

---

<sup>1</sup> Komisja Europejska przeciwko Republice Federalnej Niemiec (C-518/07 z 9 marca 2010 r.); Komisja Europejska przeciwko Republice Austrii (C-614/10 z 16 października 2012 r.); Komisja Europejska przeciwko Węgrom (C-288/12 z 8 kwietnia 2014 r.).

### 3. Przypomina europejskim organom ochrony danych o potrzebie:

- **wznowienia swoich wysiłków** na rzecz podniesienia świadomości publicznej na temat praw do ochrony danych oraz widoczności prac organów ochrony danych, uznając przy tym wyzwania, jakie przyniosą rosnące wymagania;
- **przyjęcia** odpowiednich metodologii, aby jak najlepiej ukierunkować swoje wyczerpywalne zasoby w celu osiągnięcia wyników rzeczywiście służących ochronie prywatności osób oraz w szczególności propagować rozwój przyszłości cyfrowej przyjaznej dla prywatności poprzez zabezpieczenia prywatności wbudowane w technologię;
- **współpracy** ze stronami trzecimi, w tym partnerstw między europejskimi organami ochrony danych, współpracy z Międzynarodową Konferencją oraz z innymi stronami trzecimi – takimi jak inne organy regulacyjne, w celu zapewnienia, że informacje o ochronie danych, na tyle na ile to możliwe, będą propagowane i zwiększane poprzez współpracę z innymi;
- **zachęcania** do rozwoju mechanizmów wspierających ochronę danych i prywatności, takich jak certyfikaty prywatności i kodeksy postępowania, w celu propagowania zgodności i dobrych praktyk – ułatwiających „wyścig na sam szczyt” i zapewniających bodźce do przestrzegania zasad ochrony danych;
- **rozwijania** systematycznego i proaktywnego podejścia to radzenia sobie z nie zapewnianiem zgodności przez administratorów danych, których działania stanowią największe zagrożenie dla praw obywateli do ochrony danych;
- **aby jeszcze bardziej odpowiadać** na nowe technologie i ich skutki dla ochrony danych. Dotyczy to kontynuowania rozwijania i dzielenia się wewnętrzną specjalistyczną wiedzą techniczną;
- **bycia asertywnym** przy przekonywaniu do zasobów, jakie organy ochrony danych potrzebują do zapewnienia wysokiego poziomu ochrony osób w skuteczny sposób. Dotyczy to dalszego wpływania na dyskusje na temat pakietu reformy ochrony danych UE, jak również dyskusje nad modernizacją Konwencji 108 Rady Europy na podstawie, że ustawodawcy nie powinni powierzać nowych zadań organom ochrony danych przy ochronie podstawowych praw do prywatności i ochrony danych, bez jednoczesnego umożliwienia im pełnej realizacji tych zadań poprzez zapewnienie niezbędnych uprawnień i zasobów; oraz

- **dalszego rozwijania** inicjatyw, takich jak podgrupa Grupy Roboczej Artykułu 29 ds. współpracy oraz Grupa Robocza Wiosennej Konferencji ds. współpracy europejskiej, które umożliwią wymianę informacji, wiedzy i badań dotyczących praktycznych podejść, aby pomóc organom ochrony danych sprostać wielu wyzwaniom, które napotykają.