Rada
Unii Europejskiej

Bruksela, 14 maja 2018 r.
(OR. en)

8792/18

**Międzyinstytucjonalny numer referencyjny:**
**2018/0051 (NLE)**

**SCH-EVAL 102**
**COMIX 244**

**WYNIK PRAC**

| | |
|---|---|
| Od: | Sekretariat Generalny Rady |
| Data: | 14 maja 2018 r. |
| Do: | Delegacje |
| Nr poprz. dok.: | 8285/18 |
| Dotyczy: | Decyzja wykonawcza Rady ustanawiająca zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2017 r. oceny dotyczącej stosowania przez **Portugalię** dorobku Schengen w dziedzinie **ochrony danych** |

Delegacje otrzymują w załączeniu decyzję wykonawczą Rady ustanawiającą zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2017 r. oceny dotyczącej stosowania przez Portugalię dorobku Schengen w dziedzinie ochrony danych. Decyzję tę przyjęła Rada na posiedzeniu w dniu 14 maja 2018 r.

Zgodnie z art. 15 ust. 3 rozporządzenia Rady (UE) nr 1053/2013 z dnia 7 października 2013 r. przedmiotowe zalecenie zostanie przekazane Parlamentowi Europejskiemu i parlamentom narodowym.

**ZAŁĄCZNIK**

Decyzja wykonawcza Rady ustanawiająca

**ZALECENIE**

**w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2017 r. oceny dotyczącej stosowania przez Portugalię dorobku Schengen w dziedzinie ochrony danych**

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Rady (UE) nr 1053/2013 z dnia 7 października 2013 r. w sprawie ustanowienia mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen oraz uchylenia decyzji komitetu wykonawczego z dnia 16 września 1998 r. dotyczącej utworzenia Stałego Komitetu ds. Oceny i Wprowadzania w Życie Dorobku Schengen[1], w szczególności jego art. 15,

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) Niniejsza decyzja ma na celu przedstawienie działań naprawczych, których wdrożenie zaleca się Portugalii w celu wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2017 r. oceny stosowania dorobku Schengen w dziedzinie ochrony danych. Po dokonaniu oceny sprawozdanie obejmujące ustalenia i opinie, zawierające optymalne rozwiązania oraz wymieniające niedociągnięcia stwierdzone podczas oceny, zostało przyjęte decyzją wykonawczą Komisji [C (2018)1190].

(2) Za dobrą praktykę zespół prowadzący kontrolę na miejscu uznał ciągłe inwestycje organu ochrony danych w szkolenie swojego personelu technicznego.

[1] Dz.U. L 295 z 6.11.2013, s. 27.

(3) W świetle znaczenia, jakie ma przestrzeganie dorobku Schengen, w szczególności wymogu zapewnienia i przeprowadzenia skutecznego nadzoru oraz zapewnienia niezbędnych środków bezpieczeństwa, priorytetowo należy potraktować wdrożenie poniższych zaleceń nr 1, 4, 14, 17 i 22.

(4) Niniejszą decyzję należy przekazać Parlamentowi Europejskiemu i parlamentom państw członkowskich. Zgodnie z art. 16 ust. 1 rozporządzenia (UE) nr 1053/2013 w terminie trzech miesięcy od przyjęcia zalecenia Portugalia opracowuje plan działania w celu wyeliminowania niedociągnięć wymienionych w sprawozdaniu z oceny i przekazuje go Komisji i Radzie,

NINIEJSZYM ZALECA

Portugalii, by:

**Organ nadzorczy ds. ochrony danych**

1. przeznaczyła na potrzeby organu ochrony danych wystarczające zasoby finansowe i ludzkie, aby organ ten był w stanie wypełniać wszystkie zadania powierzone mu w ramach systemu informacyjnego Schengen II (zwanego dalej „SIS II") oraz wizowego systemu informacyjnego (zwanego dalej „VIS"), także w perspektywie rozszerzenia jego obowiązków w przyszłości;

2. w celu lepszego zapewnienia zupełnej niezależności organu ochrony danych zagwarantowała mu niezależność finansową w zakresie wykonania budżetu rocznego, a także autonomię w zakresie rekrutacji pracowników przez co najmniej dostosowanie odpowiednich przepisów do przepisów mających zastosowanie do innych niezależnych organów w Portugalii;

3. zapewniła niezwłoczne sfinalizowanie przez organ ochrony danych procedur przyjęcia sprawozdań z kontroli dotyczących przetwarzania danych osobowych w SIS II;

4. zapewniła niezwłoczne zakończenie przez organ ochrony danych audytu VIS;

**Prawa osób, których dane dotyczą**

5. zapewniła, by osoby, których dane dotyczą, były informowane o swoich prawach w odniesieniu do SIS II na stronie internetowej Serviço de Estrangeiros e Fronteiras (urząd ds. cudzoziemców i granic, zwany dalej „SEF”);

6. zapewniła, by osoby, których dane dotyczą, po złożeniu wniosku o dostęp do ich danych osobowych były informowane o kategorii danych przetwarzanych w SIS II;

7. zapewniła, by osoby, których dane dotyczą, były wyraźnie informowane o tożsamości administratora danych zajmującego się przetwarzaniem ich danych osobowych w ramach wydawania wiz Schengen;

**Wizowy system informacyjny**

8. wyjaśniła sytuację w zakresie sprawowania kontroli nad przetwarzaniem danych osobowych w N.VIS (z uwzględnieniem aplikacji stosowanych zarówno przez Ministerstwo Spraw Zagranicznych (zwane dalej „MSZ”), jak i SEF oraz powiązane ośrodki przetwarzania danych), w szczególności poprzez czytelne zdefiniowanie roli MSZ i podziału obowiązków związanych z przetwarzaniem danych osobowych pomiędzy SEF a MSZ;

9. zapewniła, by MSZ przeprowadzało systematyczne działania nadzorcze umożliwiające wnikliwą ocenę aspektów związanych z przetwarzaniem danych osobowych przez zewnętrznego usługodawcę. W tym kontekście zachęca się Portugalię do rozszerzenia kwestionariusza, jaki MSZ wysyła do zewnętrznego usługodawcy, tak by obejmował on w bardziej szczegółowy sposób aspekty ochrony danych, oraz do wzmocnienia działań nadzorczych MSZ związanych z ochroną danych zapewnianą przez usługodawcę zewnętrznego i podwykonawcę, w zależności od danego przypadku;

10. ustanowiła procedurę umożliwiającą weryfikację trafień uzyskanych w ramach wyszukiwania w SIS II w trakcie procedury wydawania wiz;

11. zapewniła, by hasła wszystkich użytkowników N.VIS były zaszyfrowane;

12. zapewniła, by SEF i MSZ analizowały regularnie dane logowania w celu zapewnienia monitorowania ochrony danych;

13. zapewniła, by MSZ regularnie przeprowadzał monitorowanie własnej działalności w zakresie przetwarzania danych osobowych w systemie RPV i powiązanym centrum danych;

14. zapewniła, by MSZ niezwłocznie przyjął plan bezpieczeństwa dla systemu RPV i powiązanego centrum danych;

15. w pełni wdrożyła decyzję Rady 2008/633/WSiSW z dnia 23 czerwca 2008 r. w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania oraz zapewniła, by dostęp do danych w N-VIS odbywał się zgodnie z określonymi w tej decyzji wymogami i procedurą;

16. zapewniła, by usługodawca zewnętrzny usuwał dane osobowe wnioskodawców przechowywane w swoich systemach zgodnie z terminami określonymi w załączniku X, część A, lit. d) kodeksu wizowego, i ustanowiła wymóg, by takie dane były usuwane natychmiast po ich przekazaniu do konsulatu;

**System informacyjny Schengen II**

17. stworzyła pełne centrum wsparcia dla N.SIS II, które oferuje wszystkie potrzebne funkcje, w tym przyłączenie do infrastruktury komunikacyjnej s-TESTA;

18. sprecyzowała zakres odpowiedzialności stron zaangażowanych w przetwarzanie danych w N.SIS II, to znaczy administratora danych i organów mających dostęp do SIS II (organy wykorzystujące dane) pod względem bezpieczeństwa IT, kontroli i monitorowania własnej działalności, na przykład poprzez zawieranie umów między administratorem danych a organami mającymi dostęp do SIS II;

19. wdrożyła zarządzanie użytkownikami pozwalające na skuteczne monitorowanie własnej działalności na podstawie centralnych rejestrów przez administratora danych N.SIS II bez konieczności konsultowania rejestrów w organach wykorzystujących dane;

20. zapewniła, by SEF regularnie analizował dane logowania w celu zapewnienia monitorowania ochrony danych;

21. zapewniła, by środowisko IT, którym posługują się użytkownicy o szerokich prawach dostępu lub edytowania danych w N.SIS II (tacy jak członkowie biura SIRENE), było pod względem logicznym i fizycznym oddzielone od dostępu do internetu;

22. zapewniła, by administrator danych szyfrował zapasowe taśmy i twarde dyski N.SIS;

23. zapewniła, by profile użytkowników o szerokich prawach dostępu lub edytowania danych w N.SIS II (takich jak członkowie biura SIRENE), były zabezpieczone przy użyciu obowiązkowej metody uwierzytelniania dwuskładnikowego;

24. zapewniła, by SEF zintensyfikował swoje działania dotyczące monitorowania własnej działalności w zakresie przetwarzania danych osobowych w N.SIS i regularnie prowadził takie monitorowanie; zachęca się Portugalię do zapewnienia SEF wystarczających zasobów finansowych i ludzkich, aby mógł on prowadzić skuteczną i ciągłą kontrolę własną i bezpieczeństwa IT, w szczególności przez obsadzenie stanowiska pracownika ds. bezpieczeństwa informatycznego w dziale technologii informacyjnych SEF;

**Informowanie społeczeństwa**

25. zapewniła, by na stronie internetowej SEF znajdowały się odpowiednie linki do strony internetowej organu ochrony danych.

Sporządzono w Brukseli dnia […] r.

*W imieniu Rady*
*Przewodniczący*