Rada
Unii Europejskiej

Bruksela, 8 marca 2019 r.
(OR. en)

7281/19

Międzyinstytucjonalny numer referencyjny: 2019/0024(NLE)

SCH-EVAL 50
DATAPROTECT 84
COMIX 148

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	7 marca 2019 r.
Do:	Delegacje
Nr poprz. dok.:	6399/19
Dotyczy:	Decyzja wykonawcza Rady ustanawiająca zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2018 r. oceny stosowania przez **Szwajcarię** dorobku Schengen w dziedzinie **ochrony danych**

Delegacje otrzymują w załączeniu decyzję wykonawczą Rady ustanawiającą zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku oceny z 2018 r. dotyczącej stosowania przez Szwajcarię dorobku Schengen w dziedzinie ochrony danych. Decyzję tę przyjęła Rada na posiedzeniu w dniu 7 marca 2019 r.

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

ZAŁĄCZNIK

Decyzja wykonawcza Rady ustanawiająca

ZALECENIE

w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2018 r. oceny stosowania przez Szwajcarię 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 Szwajcarii w celu wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2018 r. oceny stosowania dorobku Schengen w dziedzinie ochrony danych. Po dokonaniu oceny decyzją wykonawczą Komisji C(2019)200 zostało przyjęte sprawozdanie obejmujące ustalenia i opinie, zawierające optymalne rozwiązania oraz wymieniające niedociągnięcia stwierdzone podczas oceny.

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

(2) Za dobre praktyki uznaje się między innymi: przewodnik „Monitorowanie stosowania Systemu Informacyjnego Schengen (SIS)", który został opracowany przez grupę koordynacyjną ds. Schengen ustanowioną przez szwajcarskie organy ds. ochrony danych; fakt, iż strona internetowa Biura Federalnego Komisarza ds. Ochrony Danych i Informacji (zwanego dalej „FDPIC") zawiera bardzo szczegółowe konkretne wzory pism dotyczące wykonywania praw osób, których dane dotyczą, w związku z Systemem Informacyjnym Schengen (zwanym dalej „SIS II") i wizowym systemem informacyjnym (zwanym dalej „VIS"), oraz że informacje w najczęściej zadawanych pytaniach dotyczących SIS II „Schengen ... a Twoje dane osobowe" i VIS „Wiza Schengen a Twoje dane osobowe" są bardzo pomocne; szybkość odpowiedzi przez Federalny Urząd Policji (fedpol) na wnioski osób, których dane dotyczą, w szczególności w obliczu dużej liczby wpływających wniosków; fakt, iż środki ochrony wprowadzone w serwerowni ośrodka usług informatycznych ISC-FDJP (wykorzystywanej do celów obsługi N-VIS i SIS II) są na wysokim poziomie oraz zapewniają bezpieczne środowisko dla przechowywania danych i zapobiegania ewentualnym incydentom; szeroko zakrojone działania fedpolu dotyczące szkoleń i pogłębiania wiedzy jego pracowników, w tym na tematy związane z ochroną danych; aktywny udział inspektorów ochrony danych fedpolu, polegający w szczególności na prowadzeniu szkoleń i udzielaniu porad na temat wszystkich kwestii dotyczących ochrony danych oraz na rozpatrywaniu wszystkich wniosków osób, których dane dotyczą.

(3) W świetle znaczenia, jakie ma przestrzeganie dorobku Schengen dotyczącego ochrony danych w odniesieniu do SIS II i VIS, priorytetowo należy potraktować wdrożenie zaleceń 12 i 15 wymienionych poniżej.

(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 Szwajcaria powinna opracować plan działania, w którym wyszczególnione zostaną wszystkie zalecenia w celu wyeliminowania niedociągnięć wymienionych w sprawozdaniu z oceny, i przekazać go Komisji i Radzie,

ZALECA:

by Szwajcaria

Organy nadzorcze ds. ochrony danych

1. w celu lepszego zapewnienia całkowitej niezależności FDPIC, rozważyła zniesienie – w ramach zmiany federalnej ustawy o ochronie danych – możliwości posiadania przez Federalnego Komisarza ds. Ochrony Danych i Informacji (FDPIC) drugiego miejsca zatrudnienia;

2. w celu lepszego zapewnienia całkowitej niezależności organu ochrony danych (DPA) w kantonie Lucerna, zniosła możliwość zwolnienia Komisarza ds. Ochrony Danych w Lucernie „z uzasadnionych powodów” (powody te mogą być inne niż poważne uchybienie);

3. wzmocniła uprawnienia wykonawcze FDPIC, aby umożliwić mu bezpośrednie podejmowanie wiążących prawnie decyzji;

4. wzmocniła uprawnienia wykonawcze kantonalnych organów ochrony danych przez nadanie im prawa do bezpośredniego podejmowania wiążących prawnie decyzji;

5. przeznaczyła na potrzeby FDPIC wystarczające zasoby finansowe i ludzkie, aby organ ten był w stanie wypełniać wszystkie zadania powierzone mu w ramach dorobku prawnego dotyczącego SIS II oraz VIS;

6. przeznaczyła na potrzeby DPA w kantonie Lucerna wystarczające zasoby finansowe i ludzkie, aby organ ten był w stanie wypełniać wszystkie zadania powierzone mu w ramach dorobku prawnego dotyczącego SIS II oraz VIS;

7. w celu lepszego zapewnienia całkowitej niezależności DPA w kantonie Lucerna, umożliwiła temu organowi samodzielne zatrudnianie pracowników zgodnie z jego zapotrzebowaniem;

8. w celu lepszego zapewnienia całkowitej niezależności FDPIC, dokonała reformy procedury budżetowej w taki sposób, aby organ ten miał rzeczywisty wpływ na projekt swojego budżetu, zanim wniosek w sprawie budżetu ogólnego zostanie przesłany do parlamentu do dyskusji i przyjęcia, jak również aby wniosek budżetowy FDPIC był przedstawiany parlamentowi;

9. w celu lepszego zapewnienia całkowitej niezależności DPA w kantonie Lucerna, dokonała reformy procedury budżetowej w taki sposób, aby organ ten miał rzeczywisty wpływ na projekt swojego budżetu, zanim wniosek w sprawie budżetu ogólnego zostanie przesłany do parlamentu do dyskusji i przyjęcia; organowi DPA w kantonie Lucerna należy przyznać autonomię budżetową, a tym samym prawo wpływu na dotyczące go decyzje budżetowe oraz prawo do ich kontroli;

10. zapewniła, aby FDPIC częściej monitorował legalność przetwarzania danych osobowych w SIS II. Kontrole te nadal powinny obejmować sprawdzanie danych logowania, ale powinny również dotyczyć innych zagadnień z zakresu ochrony danych związanych ze strukturą i funkcjonowaniem N-SIS II;

11. zapewniła, aby DPA w kantonie Lucerna częściej monitorował legalność przetwarzania danych osobowych w SIS II;

12. zapewniła, aby FDPIC przeprowadzał audyt operacji przetwarzania danych w N.SIS co najmniej raz na cztery lata; audyt ten powinien obejmować również operacje przetwarzania danych w N-SIS II przez administratora danych N-SIS II, czyli fedpol, w tym na serwerze SIRENE B i N-SIS; zważywszy na fakt, że termin pierwszego audytu upłynął w kwietniu 2017 r., należy podjąć działania, by możliwie jak najszybciej wypełnić to zobowiązanie;

13. zapewniła, aby FDPIC częściej monitorował legalność przetwarzania danych osobowych w VIS;

14. zapewniła, aby DPA w kantonie Lucerna częściej monitorował legalność przetwarzania danych osobowych w wizowym systemie informacyjnym (dalej zwanym VIS);

15. zapewniła, aby FDPIC przeprowadzał audyt operacji przetwarzania danych w krajowym systemie VIS (ORBIS) co najmniej raz na cztery lata. Ponieważ nie dotrzymano terminu pierwszego audytu (październik 2015 r.), należy podjąć działania, by możliwie jak najszybciej wypełnić to zobowiązanie i dokończyć audyt;

Prawa osób, których dane dotyczą

16. dokładnie rozważyła, w jaki sposób można skuteczniej wykonywać związane z SIS II prawa osób, których dane dotyczą i które mieszkają za granicą, gdyż według prawa szwajcarskiego urzędowe decyzje (w sprawach dotyczących odmowy dostępu do danych osobowych) należy przesyłać na adres w Szwajcarii;

17. zamieściła na stronach internetowych fedpolu i FDPIC informacje o przysługującej osobom, których dane dotyczą, możliwości skorzystania ze środków ochrony prawnej przed sądem w przypadkach, gdy nie dotrzymano terminu odpowiedzi na wniosek osoby, której dane dotyczą, w związku z SIS II (60 dni);

18. zapewniła, aby na wszystkich stronach internetowych kantonalnych organów policji zamieszczone zostały podstawowe informacje na temat ochrony danych oraz bezpośredni link do stron internetowych kantonalnego DPA;

19. zapewniła, aby różne organy nadzorcze ds. ochrony danych, na szczeblu federalnym i kantonalnym, dysponowały odpowiednimi zasobami umożliwiającymi im wypełnianie wszystkich obowiązków polegających na gwarantowaniu i wspieraniu wykonywania praw osób, których dane dotyczą, w tym przyjmowaniu skarg złożonych przez osoby fizyczne;

20. zamieściła informacje na temat podstawy prawnej do złożenia skargi związanej z wykonywaniem praw osób, których dane dotyczą, – w tym informacje na temat tego, co może stanowić powtarzalny lub stanowiący nadużycie wniosek – w sekcji zawierającej często zadawane pytania dotyczące Schengen oraz na stronach internetowych fedpolu, FDPIC, DPA w kantonie Lucerna oraz misji zagranicznych/konsulatów;

Wizowy system informacyjny

21. dodała zagadnienia związane z ochroną danych do programu intensywnego dwumiesięcznego szkolenia organizowanego przez Sekretariat Stanu ds. Migracji dla pracowników rozpatrujących wnioski wizowe;

22. zapewniła, aby Sekretariat Stanu ds. Migracji aktywnie i regularnie sprawdzał dane logowania, aby monitorować legalność przetwarzania danych osobowych w VIS;

23. zapewniła, aby Sekretariat Stanu ds. Migracji ogólnie usprawnił środki kontroli wewnętrznej, zgodnie z wymogami art. 32 ust. 2 lit. k) rozporządzenia w sprawie VIS i art. 9 ust. 2 lit. k) decyzji Rady w sprawie VIS;

System informacyjny Schengen

24. zapewniła, aby fedpol wprowadził środki techniczne w celu zapobiegania korzystaniu z portów USB na stanowiskach roboczych z dostępem do N-SIS II;

25. zapewniła, aby misje zagraniczne, porty lotnicze, posterunki policji i kantonalne urzędy ds. migracji udostępniały obywatelom papierową wersję ulotki „Schengen a Twoje dane osobowe” w swoich obiektach;

26. sprawdziła i określiła, czy upoważnieni użytkownicy N-SIS II mają techniczną możliwość jednoczesnego logowania się do systemu za pomocą różnych urządzeń (np. na stacjonarnym stanowisku roboczym i przez urządzenie mobilne); zaktualizowała wewnętrzne dokumenty dotyczące bezpieczeństwa informacji, aby zapobiec jednoczesnemu logowaniu się do N-SIS II za pomocą różnych urządzeń;

27. zapewniła, aby fedpol aktywnie i regularnie sprawdzał dane logowania, aby monitorować legalność przetwarzania danych osobowych w SIS II;

28. zapewniła, aby fedpol ogólnie usprawnił środki kontroli wewnętrznej, zgodnie z wymogami art. 10 ust. 1 lit. k) rozporządzenia w sprawie SIS II i art. 10 ust. 1 lit. k) decyzji Rady w sprawie SIS II;

Informowanie społeczeństwa

29. zapewniła, aby materiały informacyjne na temat praw osób, których dotyczą dane w systemie VIS, można było łatwiej odszukać oraz aby były one wyraźniej oznaczone poza stroną FDPIC, również przez stworzenie angielskiej wersji językowej stron internetowych Sekretariatu Stanu ds. Migracji, policji kantonalnej i DPA kantonalnego;

30. zapewniła, aby misje zagraniczne, porty lotnicze, posterunki policji i kantonalne urzędy ds. migracji udostępniały obywatelom papierową wersję ulotki „Schengen a Twoje dane osobowe" w swoich obiektach;

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodniczący