Rada
Unii Europejskiej

Bruksela, 24 września 2019 r.
(OR. en)

12469/19

Międzyinstytucjonalny numer referencyjny:
2019/0169(NLE)

SCH-EVAL 158
DATAPROTECT 217
COMIX 428

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	20 września 2019 r.
Do:	Delegacje
Nr poprz. dok.:	11906/1/19 REV 1
Dotyczy:	Decyzja wykonawcza Rady ustanawiająca zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2018 r. oceny dotyczącej stosowania przez Łotwę dorobku Schengen w dziedzinie ochrony danych

Delegacje otrzymują w załączeniu decyzję wykonawczą Rady ustanawiającą zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2018 r. oceny stosowania przez Łotwę dorobku Schengen w dziedzinie ochrony danych. Decyzja ta została przyjęta przez Radę na posiedzeniu w dniu 20 września 2019 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.

Decyzja wykonawcza Rady ustanawiająca

ZALECENIE

w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2018 r. oceny stosowania przez Łotwę 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 Łotwie w celu wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2018 r. oceny stosowania dorobku Schengen w dziedzinie ochrony danych. W wyniku przeprowadzonej oceny decyzją wykonawczą Komisji C(2019) 5720 przyjęto sprawozdanie zawierające ustalenia i opinie, wymieniające najlepsze praktyki oraz wskazujące niedociągnięcia stwierdzone w toku tej oceny.

(2) Za dobre praktyki uznaje się między innymi skuteczne wykorzystanie finansowania przyznawanego przez Komisję Europejską w celu zwiększenia świadomości społecznej oraz fakt, że odpowiedzi z biura SIRENE są dostępne w różnych językach i zazwyczaj udziela się ich w krótkim czasie.

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

(3) W świetle znaczenia, jakie ma przestrzeganie dorobku Schengen w dziedzinie ochrony danych w związku z systemem informacyjnym Schengen II (SIS II), należy priorytetowo potraktować zalecenia 15 do 18.

(4) W świetle znaczenia, jakie ma przestrzeganie dorobku Schengen w dziedzinie ochrony danych w związku z wizowym systemem informacyjnym (VIS), należy priorytetowo potraktować zalecenia 9 i 11.

(5) 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 niniejszej decyzji Łotwa powinna opracować plan działania, w którym wyszczególnione zostaną wszystkie zalecenia w celu wyeliminowania niedociągnięć wskazanych w sprawozdaniu z oceny, i przekazać ten plan Komisji i Radzie,

ZALECA:

aby Łotwa

Organ nadzorczy ds. ochrony danych

1. zapewniła całkowitą niezależność organu ochrony danych przez przyjęcie przepisów krajowych zgodnych z rozdziałem VI ogólnego rozporządzenia o ochronie danych (zwanego dalej „RODO”), w szczególności w zakresie procedury odwoływania dyrektora;

2. zapewniła wystarczające finansowanie organu ochrony danych oraz zapewniła odpowiedni poziom zatrudnienia, tak aby organ mógł wypełniać wszelkie zadania powierzone mu na mocy dorobku prawnego dotyczącego systemu informacyjnego Schengen II (zwanego dalej „SIS II”) i wizowego systemu informacyjnego (zwanego dalej „VIS”);

3. zapewniła, by audyt operacji przetwarzania danych w ramach systemu N.SIS, zgodnie z wymogiem określonym w art. 44 ust. 2 rozporządzenia w sprawie SIS II i art. 60 ust. 2 decyzji Rady w sprawie SIS II, był przeprowadzany terminowo;

4. zapewniła, by audyt operacji przetwarzania danych w ramach systemu NVIS był przeprowadzany zgodnie z wymogami art. 41 ust. 2 rozporządzenia w sprawie VIS i art. 8 ust. 6 decyzji Rady w sprawie VIS;

5. zapewniła, by przyszłe audyty systemów SIS II i VIS były w pełni kompleksowe i przeprowadzane z uwzględnieniem międzynarodowych standardów audytu, zgodnie z wymogami dorobku prawnego dotyczącego systemów SIS II i VIS, oraz by do przeprowadzania tych audytów wykorzystywano niezbędną wiedzę ekspercką w dziedzinie IT;

6. zapewniła, by działania nadzorcze organu ochrony danych w odniesieniu do SIS II obejmowały regularne kontrole wpisów do SIS II;

7. zapewniła, by działania nadzorcze organu ochrony danych w odniesieniu do VIS obejmowały regularne kontrole urzędów konsularnych;

8. zapewniła, by przygotowywany przez organ ochrony danych wieloletni plan inspekcji obejmował działania kontrolne wykraczające poza obowiązkowe audyty SIS II i VIS;

Wizowy system informacyjny

9. zapewniła regularną analizę logów w celu monitorowania legalności operacji przetwarzania danych zgodnie z art. 34 ust. 1 i 2 rozporządzenia w sprawie VIS;

10. doprecyzowała funkcję (podmiot przetwarzający dane lub współadministrator) Ministerstwa Spraw Zagranicznych (zwanego dalej „MSZ”) – w odniesieniu do Urzędu ds. Obywatelstwa i Migracji (zwanego dalej „UOM”);

11. zapewniła częstsze kontrole przez UOM własnych operacji przetwarzania danych w VIS;

12. zmieniła umowy z usługodawcami zewnętrznymi w celu dostosowania umów do wymogów określonych w RODO i zapewnienia zgodności z tymi wymogami;

13. jasno określiła zadania i uprawnienia inspektorów ochrony danych w UOM i MSZ;

14. zapewniła, by formularze online wykorzystywane w kontekście wniosku wizowego zawierały notę na temat ochrony danych informującą osoby, których dane dotyczą, o działaniach z zakresu przetwarzania danych i mających zastosowanie prawach indywidualnych;

System informacyjny Schengen

15. zapewniła, by policja prowadziła regularne kontrole własnej działalności, w szczególności monitorowała własne logi;

16. stworzyła krajowe logi SIS II na szczeblu centralnym i zapewniła możliwość ustalenia uzasadnienia kwerendy na podstawie logu;

17. zapewniła regularny przegląd logów w celu sprawdzenia, czy przetwarzanie danych jest zgodne z art. 12 ust. 2 rozporządzenia w sprawie SIS II i decyzją Rady w sprawie SIS II;

18. obniżyła ryzyko związane z bezpieczeństwem stwarzane przez aplikację mobilną umożliwiającą dostęp do SIS II, np. dzięki umożliwieniu dostępu wyłącznie za pośrednictwem usługi VPN;

19. wprowadziła dwuelementowy system uwierzytelniania;

20. zapewniła, by dane dotyczące produkcji nie były wykorzystywane do celów testowych oraz by tylko należycie upoważnieni użytkownicy mogli prowadzić wyszukiwanie w NSIS;

21. jasno określiła zadania i uprawnienia inspektora ochrony danych w policji, w tym jego udział w wewnętrznych działaniach monitorujących, takich jak monitorowanie skuteczności środków bezpieczeństwa;

Prawa osób, których dane dotyczą, oraz zwiększanie świadomości

22. regularnie przekazywała organowi ochrony danych statystyki na temat wykonywania praw osób, których dane dotyczą, w odniesieniu do systemu SIS II i VIS;

23. ułatwiła dostęp do materiałów informacyjnych, takich jak broszura „Dane osobowe w systemie informacyjnym Schengen", w portach lotniczych i innych miejscach publicznych.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodniczący