Rada
Unii Europejskiej

Bruksela, 25 stycznia 2021 r.
(OR. en)

5534/21

Międzyinstytucjonalny numer referencyjny: 2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Do:	Delegacje
Nr poprz. dok.:	14250/20
Dotyczy:	Decyzja wykonawcza Rady ustanawiająca zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2019 r. oceny stosowania przez **Słowację** dorobku Schengen w dziedzinie **ochrony danych**

Delegacje otrzymują w załączeniu decyzję wykonawczą Rady ustanawiającą zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2019 r. oceny stosowania przez Słowację dorobku Schengen w dziedzinie ochrony danych, przyjętą w procedurze pisemnej w dniu 21 stycznia 2021 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 2019 r. oceny stosowania przez Słowację 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) Celem niniejszej decyzji jest zalecenie Republice Słowackiej działań naprawczych mających wyeliminować niedociągnięcia stwierdzone w toku przeprowadzonej w 2019 r. oceny stosowania dorobku Schengen w dziedzinie ochrony danych. W wyniku przeprowadzonej oceny decyzją wykonawczą Komisji C(2020)8160 przyjęto sprawozdanie zawierające ustalenia i opinie, wymieniające najlepsze praktyki oraz wskazujące niedociągnięcia stwierdzone w toku tej oceny.

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

(2) Za dobre praktyki uważa się m.in.: fakt, że od czasu ostatniej oceny stosowania dorobku Schengen przeprowadzonej w 2012 r. organ ochrony danych regularnie przeprowadzał działania nadzorcze w odniesieniu do SIS II zgodnie z planami rocznymi oraz że opracowano koncepcję kontroli SIS II na kolejne cztery lata; fakt, że organ ochrony danych przeprowadził znaczną liczbę kontroli VIS w konsulatach; starania organu ochrony danych oraz Ministerstwa Spraw Wewnętrznych (MSW) o zapewnienie osobom, których dane dotyczą, informacji w postaci materiałów cyfrowych i drukowanych; udostępnienie wielojęzycznych informacji dotyczących Schengen na stronie internetowej organu ochrony danych oraz ulotek; udostępnienie przez organ ochrony danych wzorów wniosków składanych przez osoby, których dotyczą dane przechowywane w SIS i VIS; fakt, że biuro SIRENE udziela odpowiedzi na otrzymane wnioski nie tylko w języku słowackim, lecz również angielskim; fakt, że władze słowackie informują obywateli, jeśli w SIS II nie przechowuje się żadnych danych na ich temat; bardzo aktywne kontrole rejestrów w systemach VIS i SIS II prowadzone przez odpowiedni dział Biura Kontroli w MSW; bardzo aktywna rola dwóch pracowników Departamentu Bezpieczeństwa Ministerstwa Spraw Zagranicznych i Europejskich (MSZE) zajmujących się kwestiami ochrony danych; fakt, że MSZE zapewnia pracownikom szkolenia w zakresie ochrony danych, w szczególności przed ich czasowym oddelegowaniem do zadań konsularnych, oraz że szkolenia te organizuje Departament Bezpieczeństwa (pełniący funkcję biura inspektora ochrony danych); wysoki poziom bezpieczeństwa proceduralnego i fizycznego służącego ochronie danych SIS II; bardzo aktywna rola inspektora ochrony danych i jego zastępcy w Departamencie Ochrony Danych Działu Kontroli w Biurze Kontroli w MSW, m.in. w zakresie doradztwa i kontroli rejestrów w odniesieniu do SIS II; fakt, że MSW zapewnia wszystkim użytkownikom końcowym N.SIS II szkolenia w zakresie ochrony danych.

(3) W świetle znaczenia, jakie ma przestrzeganie dorobku Schengen w zakresie ochrony danych w odniesieniu do VIS, priorytetowo należy potraktować wdrożenie zaleceń 7 i 24.

(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 momentu, gdy decyzja zostanie przyjęta, Republika Słowacka powinna opracować plan działań, w którym wyszczególnione zostaną wszystkie zalecenia w celu wyeliminowania wszelkich niedociągnięć wymienionych w sprawozdaniu z oceny, i przekazać go Komisji i Radzie,

ZALECA:

Republika Słowacka powinna:

Organ ochrony danych

1. zapewnić dalsze zwiększenie budżetu i liczby personelu organu ochrony danych w celu poprawy jego wyników i skuteczności;

2. zapewnić, by środki przewidziane w ramach ogólnego budżetu państwa na potrzeby organu ochrony danych były jasno wyodrębnione, tak aby organ ten dysponował własnym budżetem rocznym zasilanym ze środków publicznych;

3. dopilnować, aby w trakcie procedury budżetowej Rada Narodowa zapoznała się ze stanowiskiem organu ochrony danych w zakresie jego potrzeb budżetowych oraz z przebiegiem rozmów budżetowych prowadzonych przez ten organ z Ministerstwem Finansów (MF);

4. wprowadzić środki uniemożliwiające MF uzależnianie budżetu od kwoty kar nakładanych przez organ ochrony danych, ponieważ mogłoby to wpłynąć na charakter i priorytety prac tego organu i tym samym osłabić jego niezależność. Należy dopilnować, by budżet organu ochrony danych nie mógł być zmniejszany w ciągu roku kalendarzowego w sytuacji, w której organ ten nie zebrał pełnej szacowanej kwoty kar;

5. zapewnić, by organowi ochrony danych przydzielono wszystkie zadania i nadano wszystkie uprawnienia przewidziane w art. 57 i art. 58 RODO;

6. zapewnić, by – obok regularnych działań nadzorczych prowadzonych w stosunku do biura N.SIS i biura SIRENE – organ ochrony danych nadzorował większą liczbę organów mających dostęp do SIS II i będących użytkownikami końcowymi;

7. dopilnować, by działania nadzorcze organu ochrony danych w odniesieniu do VIS obejmowały kontrole Centralnego Urzędu Wizowego (CUW) w zakresie operacji przetwarzania danych w krajowym wizowym systemie informacyjnym (N.VIS). Ponieważ termin pierwszego audytu N.VIS. upłynął w październiku 2015 r., organ ochrony danych powinien jak najszybciej uzupełnić tę zaległą część audytu;

8. zapewnić, by organ ochrony danych przeprowadzał regularne kontrole usługodawców zewnętrznych;

Prawa osób, których dane dotyczą

9. określić odpowiedni sposób, w jaki organ ochrony danych, MSW i MSZE powinny informować osoby, których dane dotyczą, o potencjalnych zagrożeniach, jakie wiążą się z przedkładaniem kopii dokumentów tożsamości oraz informacji szczególnie chronionych za pośrednictwem otwartego internetu. MSW i MSZE proszone są o rozważenie zapewnienia osobom, których dane dotyczą, zabezpieczonego elektronicznego kanału do składania takich dokumentów;

10. zapewnić, by przestrzegano 60-dniowego terminu na udzielenie odpowiedzi na wnioski składane przez osoby, których dotyczą dane przechowywane w SIS II, określonego w art. 41 ust. 6 rozporządzenia SIS II oraz w art. 58 ust. 6 decyzji SIS II, dopóki nie zaczną w pełni obowiązywać nowe przepisy dotyczące SIS[1] (mające wejść w życie najpóźniej do dnia 28 grudnia 2021 r.), w których zawarto odniesienia do terminu na udzielenie odpowiedzi na takie wnioski przewidzianego w RODO (30 dni z możliwością przedłużenia w razie konieczności o kolejne dwa miesiące);

11. rozważyć możliwość zapewnienia osobom, których dane dotyczą, niektórych informacji w formie drukowanej (np. w postaci ulotek lub tablic informacyjnych) na posterunkach policji, jak również zadbania, by były one widoczne i łatwo dostępne;

12. rozważyć możliwość zapewnienia np. nieoficjalnych tłumaczeń na język angielski decyzji organu ochrony danych w sprawie skarg dotyczących wniosków składanych przez osoby, których dotyczą dane przechowywane w SIS II. Pomogłoby to takim osobom w lepszym zrozumieniu tych decyzji, a tym samym wzmocniłoby prawa osób, których dane dotyczą;

13. zapewnić, by łatwiej było można odszukać na stronie internetowej MSZE informacje na temat praw przysługujących osobom, których dotyczą dane przechowywane w VIS. Na stronie tej należy również zamieścić wzory wniosków umożliwiających osobom, których dotyczą dane przechowywane w VIS, korzystanie z przysługujących im praw;

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE, Dz.U. L 312 z 7.12.2018, s. 56 (zob. w szczególności art. 66–71); rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006, Dz.U. L 312 z 7.12.2018, s. 14 (zob. w szczególności art. 51–57).

14. zapewnić, by formularz wniosku wizowego zawierał jasne informacje na temat poszczególnych organów, które przetwarzają dane osobowe w ramach krajowego systemu wizowego. W szczególności należy zamieścić informację, że administratorem danych jest MSZE;

15. zapewnić w portach lotniczych oraz innych miejscach, w których przeprowadzane są kontrole graniczne, informacje w formie fizycznej (np. w postaci ulotek lub tablic informacyjnych) skierowane do osób, których dotyczą dane przechowywane w VIS. Takie informacje powinny być widoczne i łatwo dostępne;

16. zapewnić, by w odpowiedziach kierowanych do osób, których dane dotyczą, i odnoszących się do danych osobowych przechowywanych w VIS znalazły się informacje o możliwości odwołania się do organu ochrony danych lub właściwego sądu;

17. podjąć niezbędne działania w celu doprecyzowania obowiązków MSZE i CUW (w ramach MSW) w zakresie rozpatrywania wniosków złożonych przez osoby, których dotyczą dane przechowywane w VIS, i w celu zapewnienia obu tym organom wskazówek wewnętrznych lub metodologicznych. Informacje te powinny być dostępne dla osób, których dane dotyczą;

Wizowy system informacyjny

18. podjąć niezbędne działania w celu podniesienia poziomu bezpieczeństwa dostępu do rządowego środowiska informatycznego, a w szczególności do krajowych wniosków wizowych w MSZE i MSW (CUW), przede wszystkim poprzez zabezpieczenie dostępu do krajowych wizowych baz danych za pośrednictwem uwierzytelniania wieloskładnikowego;

19. wprowadzić niezbędne środki w celu poprawy bezpieczeństwa fizycznego i organizacyjnego ośrodka przetwarzania danych N.VIS w MSZE, w szczególności jeśli chodzi o następujące aspekty:

    – udostępnienie przy wejściu do ośrodka przetwarzania danych rejestru użytkowników dla personelu ICT, osób z zewnątrz lub dostawców, których dostęp powinien być ograniczony;

    – zainstalowanie systemu gaśniczego wykorzystującego gaz (argonite);

    – zainstalowanie urządzeń do wykrywania wycieku wody;

    – zapewnienie czystych i niezakurzonych powierzchni podłóg;

    – zamykanie na klucz ogrodzeń zabezpieczających serwery UE;

20. przyspieszyć proces tworzenia nowego ośrodka przetwarzania danych N.VIS w innej lokalizacji oraz przenoszenia tam centrum danych;

21. rozważyć zmianę okresu miejscowego przetrzymywania rejestrów N.VIS w przedstawicielstwach dyplomatycznych i konsulatach poprzez określenie limitu czasu zamiast limitu wielkości przechowywanych danych (MB);

22. rozważyć wykorzystanie w MSZE automatycznych systemów kontroli rejestrów;

23. podjąć niezbędne działania mające zapewnić, by przedstawicielstwa dyplomatyczne lub MSZE przeprowadzały regularne kontrole usługodawców zewnętrznych;

24. podjąć niezbędne działania w celu zapewnienia personelowi miejscowemu w konsulatach bardziej systematycznych i ujednoliconych szkoleń w zakresie ochrony danych osobowych;

25. zapewnić, by we wnioskach wizowych składanych w formie elektronicznej znajdowały się te same informacje co w ich wersji papierowej (jak określono w załączniku I do unijnego kodeksu wizowego[1]);

System Informacyjny Schengen II

26. wprowadzić niezbędne środki w celu podniesienia poziomu bezpieczeństwa dostępu do N.SIS II, w szczególności poprzez wykorzystanie uwierzytelnienia wieloskładnikowego oraz wyłącznie połączeń szyfrowanych (https);

27. zapewnić, by MSW informowało organ ochrony danych o wszelkich przypadkach naruszenia ochrony danych osobowych, które mogą stanowić zagrożenie dla praw i wolności osób fizycznych. Ponadto MSZ powinno utworzyć rejestr takich naruszeń;

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiające Wspólnotowy Kodeks Wizowy (kodeks wizowy); Dz.U. L 243 z 15.9.2009, s. 1.

Informowanie społeczeństwa

28. rozważyć umieszczenie ulotek organu ochrony danych skierowanych do osób, których dane dotyczą, również w łatwiej dostępnych miejscach, takich jak komendy policji, miejsca kontroli granicznej i konsulaty;

29. rozważyć udostępnianie prezentacji, seminariów i wydarzeń typu „dzień otwarty" ogółowi obywateli, a w szczególności podmiotom, których dane dotyczą, ponieważ to właśnie oni są zainteresowani informacjami o SIS II i VIS.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodniczący