Rada
Unii Europejskiej

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

12468/19

Międzyinstytucjonalny numer referencyjny: 2019/0168(NLE)

SCH-EVAL 157
DATAPROTECT 216
COMIX 427

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	20 września 2019 r.
Do:	Delegacje
Nr poprz. dok.:	11904/19
Dotyczy:	Decyzja wykonawcza Rady ustanawiająca zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2018 r. oceny stosowania przez **Litwę** 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 Litwę dorobku Schengen w dziedzinie ochrony danych. Decyzję tę Rada przyjęła 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. zalecenie to 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 Litwę 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 Litwie 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) 5700 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 uznaje się między innymi: fakt, że organ ochrony danych udziela porad i wskazówek osobom indywidualnym, które się do niego zwracają, zamiast po prostu przekazać wnioski dalej; zapewnienie wzorów pism w sprawie wykonywania praw osób, których dotyczą dane, w odniesieniu do systemu informacyjnego Schengen II (SIS II) i wizowego systemu informacyjnego (VIS); środki bezpieczeństwa wdrożone w pomieszczeniach Departamentu Technologii Informacyjnych i Komunikacji (DTIiK – mieszczą się w nim N.VIS i N.SIS) w Ministerstwie Spraw Wewnętrznych (MSW) zasadniczo spełniają wysokie standardy, zapewniając bezpieczne środowisko do przechowywania danych i zapobiegania ewentualnym incydentom; szkolenia dla użytkowników końcowych VIS, w szczególności dla personelu konsularnego przed oddelegowaniem do ambasad/konsulatów, są dobrze przygotowane; zaangażowanie w szkolenie i rozwój personelu, w szczególności dobrze rozwinięte są szkolenia dla użytkowników końcowych N.SIS i personelu biura SIRENE, obejmujące m.in.. kwestie ochrony danych; informacje umieszczone przez organ ochrony danych na jego stronie internetowej w odniesieniu do SIS II i VIS są bardzo szczegółowe, przydatne i przystępnie sformułowane (dostępne w kilku językach); broszury organu ochrony danych „Ochrona danych osobowych w systemie informacyjnym Schengen" oraz „Ochrona danych osobowych w wizowym systemie informacyjnym" dostarczają bardzo dobrych i przystępnych informacji na temat przetwarzana danych w obu bazach danych oraz powiązanych praw osób, których dane dotyczą; duże zaangażowanie organu ochrony danych w wiele konferencji, szkoleń i innych wydarzeń podnoszących świadomość, w tym skierowanych do pracowników zajmujących się przetwarzaniem danych SIS II i VIS.

(3) W świetle znaczenia, jakie ma przestrzeganie dorobku Schengen w dziedzinie ochrony danych, w szczególności w celu zapewnienia pełnej niezależności organu ochrony danych, priorytetowo należy potraktować wdrożenie zalecenia 1.

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

ZALECA,

by Litwa

Organ nadzorczy ds. ochrony danych

1. w celu lepszego zapewnienia pełnej niezależności Państwowego Inspektoratu Ochrony Danych (zwanego dalej organem ochrony danych) zniosła wymóg zatwierdzania przez ministra sprawiedliwości strategicznego planu działań organu ochrony danych oraz wymóg przeprowadzania konsultacji z ministrem sprawiedliwości na temat rocznego planu działań przed zatwierdzeniem tego planu przez dyrektora organu ochrony danych; jest to istotne również dla zapewnienia, by procedura budżetowa nie wiązała się z ryzykiem naruszenia niezależności organu ochrony danych;

2. w celu lepszego zapewnienia pełnej niezależności organu ochrony danych organizowała regularne dwustronne spotkania między ministrem sprawiedliwości a dyrektorem organu ochrony danych w taki sposób, aby nie mogły one spowodować ryzyka wywierania bezpośredniego lub pośredniego wpływu przez rząd na organ ochrony danych, który to wpływ mógłby zagrozić niezależności organu ochrony danych;

3. zniosła wszystkie te elementy odpowiedzialności dyrektora organu ochrony danych wobec rządu i wobec ministra sprawiedliwości, które mogłyby spowodować ryzyko bezpośredniego lub pośredniego wywierania wpływu przez rząd i ministra sprawiedliwości i mogłyby zagrozić niezależności organu ochrony danych;

4. zapewniła, by organ ochrony danych częściej monitorował legalność przetwarzania danych osobowych w systemie SIS II;

5. zapewniła, by organ ochrony danych przeprowadzał audyt operacji przetwarzania danych w N.SIS co najmniej raz na cztery lata;

6. zapewniła, by organ ochrony danych monitorował legalność przetwarzania danych osobowych w systemie VIS. Podczas kontrolowania ambasad organ ochrony danych powinien kontrolować również operacje przetwarzania danych i bezpieczeństwo danych u usługodawców zewnętrznych; taka możliwość powinna być określona w umowie pomiędzy Ministerstwem Spraw Zagranicznych (MSZ) a usługodawcą zewnętrznym;

7. zapewniła, by organ ochrony danych przeprowadzał audyt operacji przetwarzania danych w N.VIS co najmniej raz na cztery lata;

Prawa osób, których dotyczą dane

8. zapewniła przestrzeganie 60-dniowego terminu na udzielenie odpowiedzi osobom, których dotyczą dane w SIS II, określonego w art. 41 ust. 6 rozporządzenia w sprawie SIS II i w art. 58 ust. 6 decyzji w sprawie SIS II, do momentu pełnego obowiązywania nowego dorobku prawnego w zakresie SIS[2] (najpóźniej do dnia 28 grudnia 2021 r.), w którym zawarto odniesienia do terminów na udzielenie odpowiedzi na wnioski osób, których dotyczą dane, przewidziane w ogólnym rozporządzeniu o ochronie danych (RODO)[3] (30 dni z możliwością przedłużenia w razie potrzeby o kolejne dwa miesiące);

9. doprecyzowała procedury wewnętrzne dotyczące odpowiedzialności właściwych organów za zajmowanie się prawami osób, których dotyczą dane w SIS II; dzięki temu pracownicy będą również wiedzieć, do kogo przekazywać odpowiednie wnioski;

---

[2] 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).

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

10. zapewniła, by MSW było konsekwentne we wszystkich ostatecznych odpowiedziach kierowanych do osób indywidualnych chcących skorzystać ze swoich praw jako osób, których dotyczą dane w SIS II, tak aby przekazywano im informacje na temat prawa do odwołania się do organu ochrony danych, jak również prawa do skierowania sprawy na drogę sądową;

11. doprecyzowała procedury wewnętrzne dotyczące odpowiedzialności właściwych organów za zajmowanie się prawami osób, których dotyczą dane w VIS; dzięki temu pracownicy będą również wiedzieć, do kogo przekazywać odpowiednie wnioski;

12. zapewniła, by MSW było konsekwentne we wszystkich ostatecznych odpowiedziach kierowanych do osób indywidualnych chcących skorzystać ze swoich praw jako osób, których dotyczą dane w VIS, tak aby przekazywano im informacje na temat prawa do odwołania się do organu ochrony danych, jak również prawa do skierowania sprawy na drogę sądową;

Wizowy system informacyjny

13. podęła niezbędne kroki w celu zapewnienia, by umowy między MSZ a usługodawcami zewnętrznymi regulowały kwestię tego, w jaki sposób litewski organ ochrony danych może być zaangażowany w inspekcje przeprowadzane przez ambasady/konsulaty oraz MSZ;

14. poprawiła monitorowanie własnych działań dzięki proaktywnemu regularnemu sprawdzaniu logów w celu monitorowania legalności przetwarzania danych osobowych w VIS. MSW powinno w dalszym stopniu rozwijać system SIEM do automatycznej kontroli logów;

15. zapewniła, by inspektor ochrony danych w MSZ był bardziej zaangażowany w opracowywanie i zapewnianie szkoleń w zakresie ochrony danych dla pracowników MSZ, w tym personelu oddelegowanego do ambasad/konsulatów;

System informacyjny Schengen II

16. zlikwidowała możliwość logowania się przez użytkowników końcowych do N.SIS za pośrednictwem przeglądarki POLIS równocześnie na kilku urządzeniach;

17. zapewniła wprowadzenie elektronicznych kart dostępowych do stacji roboczych użytkowników N.SIS w policji w celu podniesienia poziomu i standardu bezpieczeństwa;

18. zapewniła pełne wykorzystanie i okresowe kontrolowanie istniejących środków technicznych uniemożliwiających korzystanie z pamięci USB na stacjach roboczych biura SIRENE;

19. poprawiła monitorowanie własnych działań dzięki proaktywnemu regularnemu sprawdzaniu logów użytkowników końcowych SIS II we wszystkich właściwych organach w celu monitorowania legalności przetwarzania danych osobowych w SIS II; MSW powinno w dalszym stopniu rozwijać system SIEM do automatycznej kontroli logów;

20. poszerzała wiedzę pracowników na temat ochrony danych w odniesieniu do przetwarzania danych w SIS II i VIS poprzez regularne szkolenia przypominające;

21. zapewniła, by szkolenia i poszerzanie wiedzy pracowników mających dostęp do N.SIS były dziedziną, w której przewodnią rolę odgrywa grupa inspektorów ochrony danych w MSW. Dzięki temu można by zapewnić trwałą strukturę i ciągłe planowanie rozwoju pracowników;

Informowanie społeczeństwa

22. zapewniła regularną aktualizację linków na stronie internetowej organu ochrony danych dotyczącej SIS II i VIS;

23. zapewniła, by strony internetowe prowadzone przez organy, które mają kontakty z obywatelami innych państw, takie jak MSW, policja, państwowa straż graniczna, MSZ i urzędy konsularne, zawierały przystępne i jasne informacje na temat SIS II i VIS oraz powiązanych praw osób, których dotyczą dane, również w języku angielskim;

24. zapewniła, by łatwiej można było znaleźć na stronach internetowych istniejące informacje w języku angielskim na temat SIS II i VIS oraz powiązanych praw osób, których dotyczą dane;

25. zapewniła spójność informacji na temat wykonywania praw osób, których dotyczą dane, w odniesieniu do N.SIS II i VIS, dostępnych na stronach internetowych instytucji, które stosują te systemy;

26. dodała informacje na temat przetwarzania danych i powiązanych praw osób, których dotyczą dane w VIS, na portalu elektronicznego modułu składania wniosków (EPM), za pomocą którego wnioskodawcy przekazują szczegółowe informacje podczas ubiegania się o wizę.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodniczący