Rada
Unii Europejskiej

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

5535/21

Międzyinstytucjonalny numer referencyjny:
2020/0312(NLE)

SCH-EVAL 12
DATAPROTECT 15
COMIX 43

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Do:	Delegacje
Nr poprz. dok.:	14245/20
Dotyczy:	Decyzja wykonawcza Rady ustanawiająca zalecenia w sprawie wyeliminowania niedociągnięć stwierdzonych w toku oceny dotyczącej spełnienia przez **Cypr** warunków koniecznych do stosowania dorobku Schengen w dziedzinie **ochrony danych**

Delegacje otrzymują w załączeniu decyzję wykonawczą Rady ustanawiającą zalecenia w sprawie wyeliminowania niedociągnięć stwierdzonych w toku oceny dotyczącej spełnienia przez Cypr warunków koniecznych do stosowania dorobku Schengen w dziedzinie ochrony danych. Decyzja ta została przyjęta 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 zalecenia zostaną przekazane Parlamentowi Europejskiemu i parlamentom narodowym.

Decyzja wykonawcza Rady ustanawiająca

ZALECENIA

w sprawie wyeliminowania niedociągnięć stwierdzonych w toku oceny dotyczącej spełnienia przez Cypr warunków koniecznych do stosowania 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 ustanawiająca zalecenie ma na celu przedstawienie działań naprawczych, których wdrożenie zaleca się Cyprowi w celu wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2019 r. oceny warunków koniecznych do stosowania dorobku Schengen w dziedzinie ochrony danych. W wyniku przeprowadzonej oceny decyzją wykonawczą Komisji C(2020)8150 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) Zespół prowadzący kontrolę na miejscu z zadowoleniem przyjmuje niedawne zwiększenie zasobów ludzkich i finansowych przydzielonych organowi ochrony danych. Zaangażowanie tego organu w prowadzenie ogólnych działań informacyjnych oraz zamieszczanie prezentacji i przemówień na jego stronie internetowej uważa się za najlepszą praktykę. Za dobrą praktykę uznaje się również wprowadzony przez cypryjską policję program szkoleń dla funkcjonariuszy policji w zakresie przepisów dotyczących SIS II i ochrony danych.

(3) W świetle znaczenia, jakie ma przestrzeganie dorobku Schengen w dziedzinie ochrony danych, priorytetowo należy potraktować wdrożenie zaleceń 1, 3, 5, 6, 8, 9 i 11.

(4) Niniejszą decyzję należy przekazać Parlamentowi Europejskiemu i parlamentom państw członkowskich. Zgodnie z art. 16 rozporządzenia (UE) nr 1053/2013 w terminie trzech miesięcy od jej przyjęcia Cypr powinien opracować plan działań, w którym wyszczególnione zostaną wszystkie zalecenia służące wyeliminowaniu wszelkich niedociągnięć wymienionych w sprawozdaniu z oceny, i przekazać go Komisji i Radzie,

ZALECA:

Cypr powinien:

Organ ochrony danych

1. przedstawić dowody świadczące o podjęciu kroków w celu zapewnienia organowi ochrony danych wystarczających zasobów ludzkich i budżetowych na potrzeby przyszłego monitorowania przetwarzania danych osobowych w ramach dorobku Schengen oraz nadzoru nad tym procesem;

2. wdrożyć plan nadzoru w odniesieniu do cypryjskich systemów SIS i VIS, obejmujący etap rozwoju i wdrażania przez najbliższe trzy lata oraz wszystkie planowane działania nadzorcze na etapie wdrażania obu systemów i po osiągnięciu przez nie operacyjności, a także przedstawić kopię tego planu;

Prawa osób, których dane dotyczą

3. zapewnić, by zamieszczone na stronach policji oraz Ministerstwa Spraw Zagranicznych informacje na temat przetwarzania danych osobowych w SIS II i VIS oraz egzekwowania praw przysługujących osobom, których dane dotyczą, były dostępne również przynajmniej w języku angielskim oraz by takie osoby miały łatwy dostęp do wspomnianych informacji. Policja i ministerstwo powinny w szczególności udostępnić na swoich stronach internetowych specjalne standardowe formularze wniosków/wzory pism w odniesieniu do SIS II i VIS na potrzeby osób, których dane dotyczą;

4. w siedzibie Ministerstwa Spraw Zagranicznych oraz we wszystkich miejscach, w których przetwarza się w jego imieniu dane osobowe w krajowym systemie VIS (N.VIS), takich jak punkty kontroli granicznej i punkty samoobsługi – zamieścić widoczną informację i udostępniać osobom, których dane dotyczą, ulotki informacyjne na temat przysługujących im praw oraz na temat przetwarzania ich danych;

Wizowy system informacyjny

5. zapewnić jak najszybsze ustanowienie krajowych przepisów dotyczących N.VIS;

6. podjąć wszelkie niezbędne działania w celu wdrożenia nowego N.VIS oraz zapewnienia jego zgodności z dorobkiem dotyczącym VIS oraz z wymogami w zakresie ochrony danych;

7. zapewnić, by Ministerstwo Spraw Zagranicznych wdrożyło procedurę dotyczącą gromadzenia i przechowywania rejestrów dostosowaną do wymogów rozporządzenia w sprawie VIS;

8. wprowadzić niezbędne środki w celu zapewnienia stabilności stanowiska inspektora ochrony danych w Ministerstwie Spraw Zagranicznych oraz zapewnić, by osoba pełniąca tę funkcję brała udział w projektowaniu i wdrażaniu nowego N.VIS;

System Informacyjny Schengen

9. zapewnić jak najszybsze przyjęcie krajowych przepisów dotyczących krajowego systemu SIS II (N.SIS II);

10. zapewnić, by wszystkie istotne kwestie związane z ochroną danych osobowych zostały rzetelnie omówione przez wszystkie zainteresowane strony oraz by przed uruchomieniem N.SIS II przeprowadzono ocenę planowanych operacji przetwarzania pod kątem skutków dla ochrony danych;

11. zapewnić, by wprowadzono wszelkie właściwe środki służące zachowaniu jakości danych przez cały cykl życia informacji;

12. przeprowadzić testy mające zapewnić integrację N.SIS II z dotychczasowymi systemami policyjnymi oraz sfinalizować proces wymiany przestarzałego sprzętu komputerowego;

13. zapewnić, by profile personelu były tworzone i dokumentowane zgodnie z art. 10 ust. 1 lit. g) decyzji Rady w sprawie SIS II i z odnośnym rozporządzeniem Rady;

14. przedstawić konkretny plan bezpieczeństwa spełniający obowiązujące wymogi prawne;

15. opracować kompleksową politykę gwarantującą, że działania w zakresie autokontroli w rozumieniu art. 10 ust. 1 lit. k) decyzji Rady w sprawie SIS II i odnośnego rozporządzenia Rady zostaną wprowadzone przed uruchomieniem N.SIS II;

Podnoszenie świadomości

16. przedstawić informacje dotyczące planowanych działań mających na celu zwiększenie poziomu wiedzy społeczeństwa na temat SIS i VIS;

Współpraca międzynarodowa

17. potwierdzić, że organ ochrony danych będzie regularnie uczestniczył w działaniach grupy ds. koordynacji nadzoru nad SIS II oraz grupy ds. koordynacji nadzoru nad VIS utworzonych w toku wdrażania dorobku Schengen, począwszy od 2020 r.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodniczący