Rada
Unii Europejskiej

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

5533/21

Międzyinstytucjonalny numer referencyjny:
2020/0307(NLE)

SCH-EVAL 10
DATAPROTECT 13
COMIX 41

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Do:	Delegacje
Nr poprz. dok.:	14247/20
Dotyczy:	Decyzja wykonawcza Rady ustanawiająca zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku przeprowadzonej w 2019 r. oceny stosowania przez **Węgry** 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 Węgry 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 Węgry 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 Węgrom 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)8170 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) Do dobrych praktyk zalicza się m.in.: fakt, że stale zwiększany jest budżet krajowego organu ds. ochrony danych i wolności informacji („NAIH”); fakt, że biuro SIRENE wykonało zalecenia z poprzedniej oceny stosowania dorobku Schengen w dziedzinie ochrony danych z 2012 r. i obecnie informuje osoby, których dane dotyczą, o możliwości wniesienia skargi do NAIH; fakt że Ministerstwo Spraw Zagranicznych i Handlu („MFAT”) wskazuje na możliwość skorzystania ze środka zaskarżenia; fakt, że informacje zamieszczone na stronie internetowej NAIH są wyczerpujące, użyteczne, łatwo dostępne i jasno sformułowane; fakt, że MFAT podjęło starania w celu zajęcia się różnymi kwestiami bezpieczeństwa informacji i sformalizowania tych kwestii; fakt, że MFAT przyjęło rzetelny i kompleksowy plan bezpieczeństwa oraz udostępnia w różnych językach (węgierskim, angielskim, niemieckim, francuskim i rosyjskim) formularze umożliwiające korzystanie z praw przysługujących osobom, których dotyczą dane zapisane w systemie SIS II.

(3) Nie należy wskazywać priorytetów w wykonywaniu zaleceń.

(4) Niniejszą decyzję należy przekazać Parlamentowi Europejskiemu i parlamentom państw członkowskich. Zgodnie z art. 16 ust. 8 rozporządzenia (UE) nr 1053/2013 w terminie sześciu miesięcy od momentu, gdy decyzja zostanie przyjęta, Węgry powinny przedstawić Komisji ocenę (możliwych) usprawnień i opis wymaganych działań,

ZALECA:

Węgry powinny:

Organ ochrony danych (NAIH)

1. zapewnić, by NAIH przeprowadzał – w ramach nadzorowania przestrzegania przepisów dotyczących SIS II – regularne kontrole wpisów do tego systemu;

2. dopilnować, by NAIH podejmował działania następcze w odniesieniu do ustaleń i zaleceń wydanych w toku kontroli i audytów SIS II przeprowadzonych w związku z wcześniejszymi działaniami nadzorczymi oraz by wspomniane ustalenia i zalecenia zostały uwzględnione również w planach kontroli z 2019 r.;

3. zapewnić, by NAIH w kompleksowy sposób kontrolował faktyczne wykonanie zaleceń sformułowanych w toku działań nadzorczych dotyczących wizowego systemu informacyjnego („VIS”);

4. zapewnić, by działania nadzorcze NAIH w zakresie VIS uwzględniały wszystkie aspekty ochrony danych w krajowym systemie wizowym, w tym przetwarzanie danych przez usługodawców zewnętrznych;

Prawa osób, których dane dotyczą

5. rozszerzyć zakres załącznika 9 do dekretu rządowego 15/2013 (w którym ustanowiono szczegółowy wzór wniosku umożliwiającego skorzystanie z prawa dostępu do danych przez osoby, których dane dotyczą), tak aby obejmował również wzory dokumentów umożliwiających takim osobom skorzystanie z innych przysługujących im praw, takich jak prawo do skorygowania danych lub ich usunięcia;

6. zapewnić, by organy krajowe (dyrekcja generalna policji ds. cudzoziemców – OIF) doprecyzowały swoje procedury związane z oceną wniosków składanych przez osoby, których dane dotyczą, w szczególności w przypadku ograniczenia prawa do skorygowania lub usunięcia danych, oraz by dostosowały te procedury do obowiązujących przepisów unijnych i krajowych;

Wizowy system informacyjny

7. zapewnić, by uprzywilejowani użytkownicy VIS byli w wystarczającym stopniu monitorowani: w tym celu może być wymagane wprowadzenie środków organizacyjnych i technicznych;

8. zwiększyć częstotliwość testów planu zarządzania ciągłością działania / przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, w szczególności w MFAT;

9. zapewnić w perspektywie krótkoterminowej, by do czasu zapewnienia drugiego ośrodka IT wszystkie kopie zapasowe nie były przechowywane w tej samej lokalizacji co serwerownia, lecz poza nią;

10. zwiększyć bezpieczeństwo dostępu do szaf rackowych;

11. dokonywać regularnych przeglądów bezpieczeństwa wewnętrznego systemu szyfrowania (MFAT);

System Informacyjny Schengen

12. zwiększyć bezpieczeństwo fizyczne budynku, w którym znajduje się ośrodek przetwarzania danych, poprzez objęcie monitoringiem wizyjnym również drugiego wejścia/wyjścia oraz poprawić bezpieczeństwo fizyczne szaf rackowych w serwerowni;

13. dokonywać regularnych przeglądów bezpieczeństwa systemu zarządzania dostępem użytkowników do SIS II;

14. zapewnić stosowanie jednorodnego zbioru wytycznych i wskazówek dotyczących bezpieczeństwa informacji w przypadku N.SIS (np. zasady stosowania haseł itp.);

15. zapewnić, by biuro SIRENE zbadało – we współpracy z archiwum narodowym – możliwości częstszego stosowania procedur selekcji w odniesieniu do przechowywania danych;

16. zwiększyć częstotliwość testów planu zarządzania ciągłością działania / przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej;

17. zapewnić, by węgierska Komenda Główna Policji (ORFK), a w szczególności biuro N.SIS oraz biuro SIRENE, wprowadziły rozwiązania umożliwiające monitorowanie uprzywilejowanych użytkowników;

18. zapewnić, by biuro SIRENE odgrywało bardziej aktywną rolę w koordynacji weryfikacji jakości informacji wprowadzanych do SIS II opisanej w punkcie 1.15 podręcznika SIRENE;

Informowanie społeczeństwa

19. dopilnować, by MFAT wyraźnie wskazało administratora / administratorów danych na potrzeby VIS. Aby zapewnić przejrzystość oraz umożliwić osobom fizycznym korzystanie z przysługujących im praw, należy przekazywać im odpowiednie informacje na temat obowiązków poszczególnych administratorów danych;

20. zapewnić, aby ORFK regularnie aktualizowała angielską wersję zawierającą sekcję poświęconą SIS.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodniczący