Rada
Unii Europejskiej

Bruksela, 22 lutego 2022 r.
(OR. en)

6426/22

Międzyinstytucjonalny numer referencyjny: 2021/0392(NLE)

SCH-EVAL 21
DATAPROTECT 42
COMIX 87

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	21 lutego 2022 r.
Do:	Delegacje
Nr poprz. dok.:	5893/22
Dotyczy:	Decyzja wykonawcza Rady ustanawiająca zalecenie w sprawie wyeliminowania niedociągnięć stwierdzonych w toku oceny z 2019 r. dotyczącej stosowania przez **Polskę** 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 Polskę dorobku Schengen w dziedzinie ochrony danych, która to decyzja została przyjęta przez Radę na posiedzeniu w dniu 21 lutego 2022 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 Polskę 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) Zgodnie z rozporządzeniem (UE) nr 1053/2013 w 2019 r. przeprowadzono ocenę w celu weryfikacji stosowania w Polsce dorobku Schengen w dziedzinie ochrony danych osobowych. W wyniku przeprowadzonej oceny decyzją wykonawczą Komisji C(2021)9100 przyjęto sprawozdanie zawierające ustalenia i opinie, wymieniające najlepsze praktyki oraz wskazujące niedociągnięcia stwierdzone w toku tej oceny.

(2) W świetle wyników tej oceny należy zalecić Polsce pewne działania naprawcze mające na celu wyeliminowanie stwierdzonych niedociągnięć.

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

(3) Za dobre praktyki uznano w szczególności: krajowe ramy prawne, które umożliwiają Prezesowi Urzędu Ochrony Danych Osobowych (UODO) niezależne powoływanie swoich zastępców, a także członków Rady do Spraw Ochrony Danych Osobowych; praktykę, zgodnie z którą kandydaci na stanowisko Prezesa Urzędu Ochrony Danych Osobowych muszą wziąć udział w wysłuchaniu publicznym w Sejmie, które jest również transmitowane za pośrednictwem oficjalnego kanału Sejmu w internecie; częste działania kontrolne w odniesieniu do usługodawców zewnętrznych, z udziałem inspektora ochrony danych, oraz częste kontrole konsulatów; zaangażowanie w szkolenie i rozwój personelu, obejmujące m.in. kwestie ochrony danych, skierowane do użytkowników końcowych krajowego systemu informacyjnego Schengen (N.SIS) i personelu Biura SIRENE; środki bezpieczeństwa wprowadzone w obu ośrodkach przetwarzania danych świadczących usługi hostingu systemu N.SIS i krajowego wizowego systemu informacyjnego (N.VIS).

(4) Z uwagi na znaczenie przestrzegania dorobku Schengen w dziedzinie ochrony danych osobowych w odniesieniu do wizowego systemu informacyjnego (VIS) i systemu informacyjnego Schengen (SIS), priorytetowo należy potraktować wdrożenie zaleceń 11, 12, 13, 20, 21 i 22 określonych w niniejszej decyzji.

(5) Zgodnie z rozporządzeniem (UE) nr 1053/2013 niniejszą decyzję należy przekazać Parlamentowi Europejskiemu i parlamentom państw członkowskich, a Polska powinna w terminie trzech miesięcy od przyjęcia niniejszej decyzji opracować plan działania, w którym wyszczególnione zostaną wszystkie zalecenia mające na celu wyeliminowanie wszelkich niedociągnięć wymienionych w sprawozdaniu z oceny, i przekazać ten plan Komisji i Radzie,

ZALECA:

Polska powinna:

Prawodawstwo

1. jednoznaczne wyjaśnić kwestię możliwości stosowania rozporządzenia 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 – RODO) w kontekście przetwarzania danych osobowych, w stosownych przypadkach, w odniesieniu do N.VIS i N.SIS;

Urząd Ochrony Danych Osobowych

2. zapewnić, aby art. 174 ustawy z 2018 r. o ochronie danych osobowych oraz art. 106 ustawy z 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, w których określono maksymalny limit wydatków na dany rok, nie ograniczały budżetu UODO do kwot niższych niż kwoty przyznane w budżecie państwa na dany rok;

3. zapewnić, aby UODO lepiej planował i organizował liczne kontrole N.SIS II w sposób gwarantujący uwzględnianie wszystkich operacji przetwarzania danych N.SIS II i uwzględnianie wszystkich właściwych podmiotów oraz aby wynikiem kontroli był kompleksowy audyt N.SIS II, jak przewidziano w art. 44 ust. 2 rozporządzenia (WE) nr 1987/2006;

4. zapewnić, aby UODO przeprowadzał kompleksowe kontrole N.VIS w celu pełnego wykonania jego zadań zgodnie z art. 41 ust. 2 rozporządzenia (WE) nr 767/2008;

Prawa osób, których dane dotyczą

5. zapewnić poprawę danych statystycznych UODO dotyczących wykonywania praw osób, których dane dotyczą, oraz zapewnić, aby rozróżniano w nich skargi od wniosków, system, do którego się odnoszą (SIS lub VIS), przedmiot oraz rodzaju wniosku (korekta, usunięcie, dostęp);

6. zapewnić, aby administrator danych przyjął aktywniejsze podejście do udzielania informacji na temat praw osób, których dane dotyczą, w odniesieniu do danych VIS;

7. zapewnić, aby administrator danych SIS i VIS (Centralny Organ Techniczny Krajowego Systemu Informatycznego – Komendant Główny Policji (COT KSI)) publikował standardowe formularze wniosków o wykonanie praw przysługujących osobom, których dane dotyczą;

Wizowy system informacyjny

8. zapewnić, aby rejestry dostępu do VIS zawierały również informacje na temat uzasadnienia takiego dostępu;

9. dokonać przeglądu wykazu organów mających dostęp do VIS oraz ich praw dostępu do danych VIS pod kątem ich uprawnień i wykorzystywania takich danych w praktyce;

10. z uwagi na dużą liczbę administratorów danych VIS ustanowionych na mocy przepisów krajowych i postanowień umownych oraz dużą liczbę zaangażowanych podmiotów, wyjaśnić stosunki między organami uczestniczącymi w procesie wydawania wiz i organami przetwarzającymi dane VIS, a także obowiązki tych organów w zakresie przetwarzania danych;

11. zapewnić, aby – w celu pełnego wykorzystania przechowywanych logów – logi VIS były poddawane regularnej analizie do celów monitorowania ochrony danych;

12. przyjąć plan bezpieczeństwa VIS obejmujący bezpieczeństwo fizyczne drugiego ośrodka przetwarzania danych, a także inne aspekty bezpieczeństwa informatycznego krajowego systemu informatycznego, w tym systemu N.VIS;

13. dostosować okres przechowywania logów dotyczących wniosków związanych z VIS (w szczególności w aplikacjach „Pobyt" i „ZSE 6") do terminów określonych w art. 34 ust. 2 rozporządzenia (WE) nr 767/2008 i art. 16 decyzji Rady 2008/633/WSiSW;

System informacyjny Schengen II

14. zapewnić, aby administrator N.SIS II ustanowił centralny system zarządzania użytkownikami, który umożliwiałby skuteczne monitorowanie własnej działalności bez konieczności przeglądania logów w instytucjach będących użytkownikami końcowymi systemu N.SIS II;

15. zapewnić, aby – w celu pełnego wykorzystania przechowywanych logów – logi SIS były poddawane regularnej analizie do celów monitorowania ochrony danych;

16. zapewnić automatyczne powiadamianie o zdarzeniach związanych z bezpieczeństwem IT oraz o działaniach administratora danych w zakresie monitorowania własnej działalności w celu dalszej poprawy bezpieczeństwa;

17. zapewnić, aby środki techniczne obejmowały również blokowanie korzystania z urządzeń USB lub pamięci USB przez zablokowanie wszystkich portów USB na stanowiskach pracy SIS;

18. rozważyć aktywny i regularny udział inspektora ochrony danych z Ministerstwa Spraw Wewnętrznych w monitorowaniu przetwarzania danych SIS i VIS za pomocą logów audytu;

19. zapewnić, aby administrator danych SIS udostępniał UODO profile personelu wszystkich organów mających dostęp do SIS;

20. dostosować okres przechowywania logów w aplikacjach umożliwiających dostęp do danych SIS do przepisów art. 12 ust. 4 rozporządzenia (WE) nr 1987/2006 i art. 12 ust. 4 decyzji Rady 2007/533/WSiSW;

21. zapewnić, aby – zgodnie z art. 10 rozporządzenia (WE) nr 1987/2006 i art. 10 decyzji Rady 2007/533/WSiSW – administrator danych SIS przyjął plan bezpieczeństwa SIS;

22. zapewnić przegląd szerokiego kręgu instytucji mających dostęp do danych SIS II, tak aby zagwarantować, że dostęp do tych danych mają wyłącznie instytucje, które go potrzebują ze względu na swoje uprawnienia i praktyczne potrzeby;

Informowanie społeczeństwa

23. zapewnić, aby strony internetowe UODO i policji dostarczały informacji na temat praw przysługujących osobom, których dane dotyczą, w odniesieniu do danych VIS.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodniczący