Rada
Unii Europejskiej

Bruksela, 2 grudnia 2021 r.
(OR. en)

14666/21

Międzyinstytucjonalny numer referencyjny:
2021/0392 (NLE)

LIMITE

SCH-EVAL 158
DATAPROTECT 279
COMIX 605

PUBLIC

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	1 grudnia 2021 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2021) 910 final
Dotyczy:	Wniosek dotyczący DECYZJI WYKONAWCZEJ RADY ustanawiającej 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 dokument COM(2021) 910 final.

Zał.: COM(2021) 910 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 1.12.2021 r.
COM(2021) 910 final

2021/0392 (NLE)
SENSITIVE*

Wniosek

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

* Distribution only on a 'Need to know" basis - Do not read or carry openly in public places. Must be stored securely and encrypted in storage and transmission. Destroy copies by shredding or secure deletion. Full handling instructions https://europa.eu/!db43PX

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

W dniu 7 października 2013 r. Rada przyjęła rozporządzenie (UE) nr 1053/2013[1] w sprawie ustanowienia mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen. Na podstawie tego rozporządzenia Komisja ustanowiła wieloletni program ocen na lata 2014–2019[2] i roczny program ocen na 2019 r.[3], zawierający szczegółowe plany dotyczące kontroli na miejscu w ocenianych państwach członkowskich, dziedzin podlegających ocenie i miejsc, gdzie zostaną przeprowadzone kontrole.

Dziedziny podlegające ocenie obejmują wszystkie aspekty dorobku Schengen: zarządzanie granicami zewnętrznymi, politykę wizową, system informacyjny Schengen (SIS), ochronę danych osobowych, współpracę policyjną, współpracę wymiarów sprawiedliwości w sprawach karnych oraz brak kontroli granicznej na granicach wewnętrznych. Ponadto we wszelkich ocenach brane są pod uwagę kwestie związane z prawami podstawowymi i funkcjonowaniem organów, które stosują poszczególne części dorobku Schengen.

W oparciu o programy wieloletnie i roczne zespół składający się z ekspertów z państw członkowskich i Komisji przeprowadził w dniach od 3 do 8 marca 2019 r. ocenę stosowania przez Polskę przepisów prawa Unii w dziedzinie ochrony danych osobowych. W sprawozdaniu z oceny[4] zespół przedstawił swoje ustalenia i opinie, a także wskazał najlepsze praktyki oraz wszelkie niedociągnięcia stwierdzone w toku oceny.

Wraz ze sprawozdaniem zespół przygotował zalecenia w sprawie działań naprawczych mających na celu wyeliminowanie tych niedociągnięć. Niniejszy wniosek uwzględnia te zalecenia.

W tym kontekście celem bieżącego wniosku dotyczącego decyzji wykonawczej Rady ustanawiającej zalecenie jest zapewnienie prawidłowego i skutecznego stosowania przez Polskę wszystkich przepisów dorobku Schengen w dziedzinie ochrony danych osobowych.

• Spójność z przepisami obowiązującymi w tej dziedzinie polityki

Zalecenia te służą wdrożeniu przepisów obowiązujących w tym obszarze polityki.

• Spójność z innymi politykami Unii

Zalecenia te nie są powiązane z innymi kluczowymi obszarami polityki Unii.

---

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

2 Decyzja wykonawcza Komisji C(2014)3683 z dnia 18 czerwca 2014 r. ustanawiająca wieloletni program oceny na lata 2014–2019 zgodnie z art. 5 rozporządzenia Rady (UE) nr 1053/2013 z dnia 7 października 2013 r. w sprawie ustanowienia mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen.

3 Decyzja wykonawcza Komisji C(2018)7115 z dnia 31 października 2018 r. ustanawiająca pierwszą część rocznego programu ocen na 2019 r. zgodnie z art. 6 rozporządzenia Rady (UE) nr 1053/2013 w sprawie ustanowienia mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen.

4 C(2021)9100

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

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.

- **Pomocniczość (w przypadku kompetencji niewyłącznych)**

W art. 15 ust. 2 rozporządzenia Rady (UE) nr 1053/2013 nakłada się na Komisję obowiązek przedłożenia Radzie wniosku w sprawie przyjęcia zaleceń dotyczących działań naprawczych mających na celu wyeliminowanie wszelkich niedociągnięć stwierdzonych w toku oceny. Działania na poziomie Unii są niezbędne, by zwiększyć wzajemne zaufanie między państwami członkowskimi oraz zapewnić lepszą koordynację na szczeblu UE i w ten sposób zagwarantować, że wszystkie przepisy dorobku Schengen będą skutecznie stosowane przez państwa członkowskie.

- **Proporcjonalność**

Art. 15 ust. 2 rozporządzenia Rady (UE) nr 1053/2013 jest odzwierciedleniem uprawnień szczególnych nadanych Radzie w zakresie wzajemnej oceny wprowadzania w życie polityk Unii w obszarze wolności, bezpieczeństwa i sprawiedliwości.

3. WYNIKI OCEN EX POST, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- **Oceny ex post/oceny adekwatności obowiązującego prawodawstwa**

nie dotyczy

- **Konsultacje z zainteresowanymi stronami**

Zgodnie z art. 14 ust. 5 i art. 21 ust. 2 rozporządzenia Rady (UE) nr 1053/2013 państwa członkowskie wyraziły pozytywną opinię na temat tego sprawozdania z oceny w dniu 6 sierpnia 2021 r. (w drodze procedury pisemnej).

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

nie dotyczy

- **Ocena skutków**

nie dotyczy

- **Sprawność regulacyjna i uproszczenie**

nie dotyczy

- **Prawa podstawowe**

W procesie oceny wzięto pod uwagę ochronę praw podstawowych podczas stosowania dorobku Schengen.

4. WPŁYW NA BUDŻET

nie dotyczy

5. ELEMENTY FAKULTATYWNE

nie dotyczy

2021/0392 (NLE)

Wniosek

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

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[5], w szczególności z 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, wskazujące najlepsze praktyki oraz niedociągnięcia stwierdzone w toku tej oceny.

(2) W świetle wyników oceny należy zalecić Polsce podjęcie pewnych działań naprawczych w celu wyeliminowania stwierdzonych niedociągnięć.

(3) Jako dobrą praktykę odnotowano w szczególności: krajowe ramy prawne, które umożliwiają Prezesowi Urzędu Ochrony Danych Osobowych (UODO) niezależne powoływanie zastępców, a także członków Rady do Spraw Ochrony Danych Osobowych; fakt, że 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, dla 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) W świetle znaczenia, jakie ma przestrzeganie 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] Dz.U. L 295 z 6.11.2013, s. 27.

(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 jej przyjęcia opracować plan działania zawierający wszystkie zalecenia mające na celu wyeliminowanie niedociągnięć wymienionych w sprawozdaniu z oceny, i przekazać ten plan Komisji i Radzie,

ZALECA:

Polska powinna:

Prawodawstwo

1. jednoznaczne wyjaśnić kwestię zastosowania 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, by UODO lepiej planował i organizował liczne kontrole N.SIS II w sposób zapewniający uwzględnienie wszystkich operacji przetwarzania danych N.SIS II i 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, by UODO przeprowadzał kompleksowe kontrole N.VIS w celu pełnego wypełnienia swoich 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 by rozróżniano w nich skargi od wniosków, system, do którego się odnoszą (SIS lub VIS), przedmiot oraz rodzaju wniosku (korekta, usunięcie, dostęp);

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

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

Wizowy system informacyjny

8. zapewnić, by 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, by – w celu pełnego wykorzystania przechowywanych rejestrów – 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, by 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, by – 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, by 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 przy pomocy logów audytu;

19. zapewnić, by 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, by – 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, by dostęp do tych danych miały wyłącznie instytucje, które go potrzebują ze względu na swoje uprawnienia i praktyczne potrzeby;

Informowanie społeczeństwa

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

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodnicząca