Raad van de
Europese Unie

Brussel, 25 januari 2021
(OR. en)

5534/21

Interinstitutioneel dossier:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
aan:	de delegaties
nr. vorig doc.:	14250/20
Betreft:	Uitvoeringsbesluit van de Raad met een aanbeveling voor het verhelpen van de tekortkomingen die zijn geconstateerd bij de in 2019 verrichte evaluatie van de wijze waarop **Slowakije** het Schengenacquis inzake **gegevensbescherming** toepast

Voor de delegaties gaat hierbij het uitvoeringsbesluit van de Raad met een aanbeveling voor het verhelpen van de tekortkomingen die zijn geconstateerd bij de in 2019 verrichte evaluatie van de wijze waarop Slowakije het Schengenacquis op het gebied van gegevensbescherming toepast, zoals dat op 21 januari 2021 volgens de schriftelijke procedure is vastgesteld.

Overeenkomstig artikel 15, lid 3, van Verordening (EU) nr. 1053/2013 van de Raad van 7 oktober 2013 zal deze aanbeveling aan het Europees Parlement en de nationale parlementen worden toegezonden.

Uitvoeringsbesluit van de Raad met een

AANBEVELING

voor het verhelpen van de tekortkomingen die zijn geconstateerd bij de in 2019 verrichte evaluatie van de wijze waarop Slowakije het Schengenacquis inzake gegevensbescherming toepast

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 1053/2013 van de Raad van 7 oktober 2013 betreffende de instelling van een evaluatiemechanisme voor de controle van en het toezicht op de toepassing van het Schengenacquis en houdende intrekking van het Besluit van 16 september 1998 tot oprichting van de Permanente Schengenbeoordelings- en toepassingscommissie[1], en met name artikel 15,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) Dit besluit is gericht tot de Slowaakse Republiek en heeft betrekking op maatregelen om de tekortkomingen te verhelpen die zijn geconstateerd bij de in 2019 verrichte Schengen-evaluatie op het gebied van gegevensbescherming. Na de evaluatie heeft de Commissie bij Uitvoeringsbesluit C(2020) 8160 een verslag vastgesteld met haar bevindingen en beoordelingen en met een opsomming van de bij de evaluatie geconstateerde beste praktijken en tekortkomingen.

[1] PB L 295 van 6.11.2013, blz. 27.

(2) Als goede praktijk wordt onder meer beschouwd dat de gegevensbeschermingsautoriteit sinds de laatste Schengenevaluatie in 2012 regelmatig SIS II-toezichtactiviteiten heeft uitgevoerd volgens een jaarlijkse planning en dat er een concept voor de SIS II-inspecties voor de volgende vier jaar is uitgewerkt; dat de gegevensbeschermingsautoriteit een aanzienlijk aantal VIS-inspecties van consulaten heeft verricht; dat de gegevensbeschermingsautoriteit en het ministerie van Binnenlandse Zaken zich inspannen om aan betrokkenen informatie te verstrekken in elektronische en gedrukte vorm; dat de informatie over met Schengen verband houdende onderwerpen op de website van de gegevensbeschermingsautoriteit en in de brochures in meerdere talen beschikbaar is; dat de gegevensbeschermingsautoriteit modellen biedt voor verzoeken van betrokkenen in verband met het SIS en het VIS; dat de reacties van het Sirene-bureau op verzoeken, niet alleen in het Slowaaks, maar ook in het Engels zijn gesteld; dat de Slowaakse autoriteiten de betrokkenen informeren indien er geen gegevens over hen in SIS II zijn opgeslagen; dat de inspectieafdeling van het bureau van de inspectiedienst van het ministerie van Binnenlandse Zaken VIS- en SIS II-logbestanden zeer actief controleert; dat de twee personeelsleden binnen de afdeling veiligheid van het ministerie van Buitenlandse en Europese Zaken die zich bezighouden met kwesties op het gebied van gegevensbescherming, een zeer actieve rol spelen; dat het ministerie van Buitenlandse en Europese Zaken zijn personeel opleiding op het gebied van gegevensbescherming biedt, met name voorafgaand aan tijdelijke detachering voor consulaire taken, en dat de afdeling veiligheid (als bureau van de functionaris voor gegevensbescherming) deze opleiding verstrekt; dat de procedurele en fysieke beveiliging die is ingesteld voor de bescherming van SIS II-gegevens, op een hoog niveau ligt; dat de functionaris voor gegevensbescherming en de plaatsvervangend functionaris voor gegevensbescherming van de afdeling gegevensbescherming van de inspectie-eenheid van het bureau van de inspectiedienst van het ministerie van Binnenlandse Zaken, een zeer actieve rol spelen, onder meer op het gebied van richtsnoeren en de controle van logbestanden inzake SIS II, en dat het ministerie van Binnenlandse Zaken alle N.SIS II-eindgebruikers opleiding op het gebied van gegevensbescherming biedt.

(3) Gezien het belang van de naleving van het Schengenacquis op het gebied van gegevensbescherming met betrekking tot het VIS moet voorrang worden gegeven aan de aanbevelingen 7 en 24.

(4) Dit besluit dient te worden doorgezonden aan het Europees Parlement en de parlementen van de lidstaten. Binnen drie maanden na de aanneming van het besluit moet de Slowaakse Republiek krachtens artikel 16, lid 1, van Verordening (EU) nr. 1053/2013 een actieplan opstellen met alle aanbevelingen om de in het evaluatieverslag vastgestelde tekortkomingen te verhelpen en dat actieplan bij de Commissie en de Raad indienen,

BEVEELT AAN:

dat de Slowaakse Republiek

Gegevensbeschermingsautoriteit

1. ervoor zorgt dat de gegevensbeschermingsautoriteit nog meer financiële en personele middelen krijgt met het oog op een verbetering van haar resultaten en doeltreffendheid;

2. ervoor zorgt dat duidelijk zichtbaar is welk deel van de totale overheidsbegroting voor de gegevensbeschermingsautoriteit is bestemd, teneinde te waarborgen dat de gegevens-beschermingsautoriteit over een eigen, openbare jaarlijkse begroting te beschikt;

3. ervoor zorgt dat de nationale raad tijdens de begrotingsprocedure op de hoogte is van het standpunt van de gegevensbeschermingsautoriteit over haar begrotingsbehoeften en van de besprekingen tussen de gegevensbeschermingsautoriteit en het ministerie van Financiën over de begroting;

4. maatregelen neemt om ervoor te zorgen dat het ministerie van Financiën geen verband kan leggen tussen de begroting en het bedrag van de door de gegevensbeschermingsautoriteit te innen boeten, aangezien dit gevolgen kan hebben voor de aard en prioritering van de werkzaamheden van de gegevensbeschermingsautoriteit en zo haar onafhankelijkheid kan aantasten. Er moet worden gewaarborgd dat de begroting van de gegevensbeschermings-autoriteit tijdens het kalenderjaar niet kan worden verlaagd in een situatie waarin de geraamde geldboeten niet volledig door de gegevensbeschermingsautoriteit zijn geïnd;

5. ervoor zorgt dat alle taken en bevoegdheden van gegevensbeschermingsautoriteiten uit hoofde van de artikelen 57 en 58 van de algemene verordening gegevensbescherming aan de gegevensbeschermingsautoriteit worden toegekend;

6. ervoor zorgt dat de gegevensbeschermingsautoriteit naast de reguliere toezichthoudende activiteiten die op het N.SIS-bureau en het Sirene-bureau worden verricht, op een groter aantal autoriteiten die als eindgebruikers toegang tot SIS II hebben, toezicht houdt;

7. ervoor zorgt dat de toezichthoudende activiteiten van de gegevensbeschermingsautoriteit inzake het VIS de inspectie van de centrale visumautoriteit omvatten met betrekking tot de gegevensverwerkingsactiviteiten in het N.VIS. Aangezien de uiterste termijn voor de eerste audit van het nationale visumsysteem oktober 2015 was, moet de gegevens-beschermingsautoriteit dit nog ontbrekende onderdeel van de audit zo spoedig mogelijk uitvoeren;

8. ervoor zorgt dat de gegevensbeschermingsautoriteit ook de externe dienstverleners regelmatig controleert;

Rechten van betrokkenen

9. een passende wijze vindt waarop de gegevensbeschermingsautoriteit, het ministerie van Binnenlandse Zaken en het ministerie van Buitenlandse en Europese Zaken betrokkenen informeren over de mogelijke risico's van het indienen van kopieën van identiteitskaarten en van gevoelige informatie via het open internet. Het ministerie van Binnenlandse Zaken en het ministerie van Buitenlandse en Europese Zaken wordt verzocht te overwegen om betrokkenen een beveiligd elektronisch transmissiekanaal aan te bieden voor het indienen van dergelijke documenten;

10. ervoor zorgt dat de termijn van 60 dagen voor het beantwoorden van verzoeken van betrokkenen in verband met SIS II zoals neergelegd in artikel 41, lid 6, van de SIS II-verordening en in artikel 58, lid 6, van het SIS II-besluit in acht wordt genomen tot het volledig van toepassing worden (uiterlijk op 28 december 2021) van het nieuwe SIS II-acquis[1], waarin wordt verwezen naar de uiterste datum voor het beantwoorden van verzoeken van betrokkenen als voorzien in de algemene verordening gegevensbescherming (30 dagen, met de mogelijkheid om indien nodig de termijn met nog eens twee maanden te verlengen);

11. overweegt om een deel van de gedrukte informatie (folders, borden enz.) voor betrokkenen in de lokalen van de politiebureaus aan te bieden en om deze zichtbaar en gemakkelijk toegankelijk te maken;

12. overweegt om bijvoorbeeld een informele Engelse versie aan te bieden van de besluiten van de gegevensbeschermingsautoriteit over klachten over verzoeken van betrokkenen in verband met SIS II; dit zou betrokkenen helpen het besluit beter te begrijpen en aldus de rechten van de betrokkenen versterken;

13. ervoor zorgt dat de informatie over de rechten van betrokkenen in verband met het VIS op de website van het ministerie van Buitenlandse en Europese Zaken gemakkelijker te vinden is; de website dient ook modellen te bieden voor de uitoefening van de rechten van betrokkenen in verband met het VIS;

---

[1] Verordening (EU) 2018/1862 van het Europees Parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengen-informatiesysteem (SIS) op het gebied van politiële en justitiële samenwerking in strafzaken, tot wijziging en intrekking van Besluit 2007/533/JBZ van de Raad en tot intrekking van Verordening (EG) nr. 1986/2006 van het Europees Parlement en de Raad en Besluit 2010/261/EU van de Commissie (PB L 312 van 7.12.2018, blz. 56; zie met name de artikelen 66 t/m 71); Verordening (EU) 2018/1861 van het Europees Parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles, tot wijziging van de Overeenkomst ter uitvoering van het Akkoord van Schengen en tot wijziging en intrekking van Verordening (EG) nr. 1987/2006 (PB L 312 van 7.12.2018, blz. 14; zie met name de artikelen 51 t/m 57).

14. ervoor zorgt dat het visumaanvraagformulier duidelijke informatie bevat over de verschillende autoriteiten die persoonsgegevens verwerken in het kader van het nationale visumsysteem. Met name moet worden vermeld dat het ministerie van Buitenlandse en Europese Zaken de verwerkingsverantwoordelijke is;

15. betrokkenen in verband met het VIS fysieke informatie (folders, borden enz.) verstrekt in de lokalen van luchthavens en andere plaatsen waar grenscontroles plaatsvinden en deze zichtbaar en gemakkelijk toegankelijk maakt;

16. ervoor zorgt dat de antwoorden die betrokkenen ontvangen met betrekking tot persoons-gegevens in verband met het VIS, informatie verschaffen over de mogelijkheid om tegen het antwoord in beroep te gaan bij de gegevensbeschermingsautoriteit en de bevoegde rechter;

17. de nodige maatregelen neemt om de verantwoordelijkheden van het ministerie van Buitenlandse en Europese Zaken en de centrale visumautoriteit (Ministerie van Binnenlandse Zaken) voor de behandeling van verzoeken van betrokkenen in verband met het VIS te verduidelijken en om beide entiteiten interne of methodologische richtsnoeren te geven; deze informatie moet voor betrokkenen toegankelijk zijn;

Visuminformatiesysteem

18. de nodige maatregelen neemt om het beveiligingsniveau te verhogen voor de toegang tot de overheidsomgeving, en in het bijzonder tot de nationale visumaanvragen bij de het ministerie van Buitenlandse en Europese Zaken en het Ministerie van Binnenlandse Zaken (centrale visumautoriteit), met name door toegang tot de nationale visumdatabanken door middel van multifactortechnologie;

19. de nodige maatregelen neemt om de fysieke en organisatorische veiligheid in het N.VIS-datacentrum van het ministerie van Buitenlandse en Europese Zaken te verbeteren, met name wat de volgende aspecten betreft:

    – aanwezigheid van een bezoekerslogboek aan de ingang van het datacentrum voor ICT-personeelsleden, bezoekers of leveranciers die maar beperkt toegang mogen hebben;

    – installatie van een systeem voor blussen met gas (aragoniet);

    – installatie van een waterlekkagedetectiesysteem;

    – het zorgen voor een stofvrije en ordelijke vloer;

    – het afsluiten van de afscherming van de EU-servers;

20. de procedure versnelt voor het opzetten van een nieuw N.VIS-datacentrum op een andere locatie en de hervestiging van het datacentrum;

21. overweegt om de lokale bewaartermijn van de N.VIS-logbestanden bij de diplomatieke en consulaire missies te wijzigen door van een tijdsperiode en niet meer van de hoeveelheid MB uit te gaan;

22. overweegt om bij het ministerie van Buitenlandse en Europese Zaken automatische log-controlesystemen te gebruiken;

23. de nodige maatregelen neemt om ervoor te zorgen dat diplomatieke missies of het ministerie van Buitenlandse en Europese Zaken de externe dienstverleners regelmatig inspecteren;

24. de nodige maatregelen neemt om het plaatselijke consulaire personeel systematischer en op uniforme wijze opleiding op het gebied van gegevensbescherming te bieden;

25. ervoor zorgt dat bij de elektronische visumaanvraag dezelfde informatie wordt gevraagd als op het papieren visumaanvraagformulier (zoals vastgesteld in bijlage I bij de EU-Visumcode[1]);

Schengeninformatiesysteem II

26. de nodige maatregelen neemt om het beveiligingsniveau voor de toegang tot het N.SIS II te verhogen, met name door voor de toegang tot het N.SIS II gebruik te maken van meervoudige authenticatie en uitsluitend https-verbindingen;

27. ervoor zorgt dat het ministerie van Binnenlandse Zaken de gegevensbeschermingsautoriteit informeert over elke inbreuk in verband met gegevens die waarschijnlijk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Voorts dient het Ministerie van Binnenlandse Zaken een register van inbreuken in verband met persoonsgegevens op te stellen;

---

1 Verordening (EG) nr. 810/2009 van het Europees Parlement en de Raad van 13 juli 2009 tot vaststelling van een gemeenschappelijke visumcode (Visumcode). PB L 243 van 15.9.2009, blz. 1.

Publieksvoorlichting

28. overweegt om de brochures van de gegevensbeschermingsautoriteit voor betrokkenen ook ter beschikking te stellen op toegankelijkere plaatsen zoals politiebureaus, plaatsen waar grenscontroles plaatsvinden en consulaten;

29. overweegt om presentaties, seminars en opendeurevenementen van de gegevens-beschermingsautoriteit ook toegankelijk te maken voor het grote publiek en met name betrokkenen, aangezien de informatie over SIS II en VIS voor hen van belang is.

Gedaan te Brussel,

Voor de Raad
De voorzitter