Rådet for
Den Europæiske Union

Bruxelles, den 25. januar 2021
(OR. en)

5534/21

Interinstitutionel sag:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
til:	delegationerne
Tidl. dok. nr.:	14250/20
Vedr.:	Rådets gennemførelsesafgørelse om fastlæggelse af en henstilling om afhjælpning af de mangler, der blev konstateret ved evalueringen i 2019 af **Slovakiets** anvendelse af Schengenreglerne på området **databeskyttelse**

Vedlagt følger til delegationerne Rådets gennemførelsesafgørelse om fastlæggelse af en henstilling om afhjælpning af de mangler, der blev konstateret ved evalueringen i 2019 af Slovakiets anvendelse af Schengenreglerne på området databeskyttelse, som blev vedtaget ved skriftlig procedure den 21. januar 2021.

I overensstemmelse med artikel 15, stk. 3, i Rådets forordning (EU) nr. 1053/2013 af 7. oktober 2013 fremsendes denne henstilling til Europa-Parlamentet og de nationale parlamenter.

Rådets gennemførelsesafgørelse om fastlæggelse af en

HENSTILLING

om afhjælpning af de mangler, der blev konstateret ved evalueringen i 2019 af Slovakiets anvendelse af Schengenreglerne på området databeskyttelse

RÅDET FOR DEN EUROPÆISKE UNION,

som henviser til traktaten om Den Europæiske Unions funktionsmåde,

som henviser til Rådets forordning (EU) nr. 1053/2013 af 7. oktober 2013 om indførelse af en evaluerings- og overvågningsmekanisme til kontrol af anvendelsen af Schengenreglerne og om ophævelse af Eksekutivkomitéens afgørelse af 16. september 1998 om nedsættelse af et stående udvalg for evaluering og anvendelse af Schengenreglerne[1], særlig artikel 15,

som henviser til forslag fra Europa-Kommissionen, og

som tager følgende i betragtning:

(1) Formålet med denne afgørelse er at fremsætte henstillinger til Den Slovakiske Republik om foranstaltninger til afhjælpning af de mangler, der blev konstateret under evalueringen i 2019 af anvendelsen af Schengenreglerne på området databeskyttelse. Efter evalueringen vedtog Kommissionen ved gennemførelsesafgørelse C(2020) 8160 en rapport om resultaterne og vurderingen heraf, som indeholder en liste over bedste praksis og mangler konstateret under evalueringen.

[1] EUT L 295 af 6.11.2013, s. 27.

(2) Som eksempler på god praksis er blandt andet, at databeskyttelsesmyndigheden siden den seneste Schengenevaluering i 2012 regelmæssigt har foretaget kontrol i overensstemmelse med en årlig planlægning, og at der er udarbejdet et koncept for SIS II-tilsyn for de næste fire år, at datatilsynsmyndigheden har foretaget et betydeligt antal tilsyn vedrørende VIS på konsulater, at datatilsynsmyndigheden og indenrigsministeriet har gjort en indsats for at stille oplysninger i elektronisk og trykt form til rådighed for de registrerede, at der er stillet flersprogede udgaver af oplysningerne om Schengenrelaterede emner til rådighed på databeskyttelsesmyndighedens websted og i folderne, at datatilsynet stiller en standardmodel for anmodninger til rådighed for personer, der er registreret i SIS og VIS, at SIRENE-kontoret ikke kun besvarer anmodninger på slovakisk, men også på engelsk, at de slovakiske myndigheder underretter de registrerede, hvis der ikke lagres oplysninger om dem i SIS II, at tilsynsenheden i tilsynstjenesten i indenrigsministeriet foretager en meget aktiv kontrol af VIS- og SIS II-logfiler, at to medarbejdere i sikkerhedsdepartement under ministeriet for udenrigsanliggender og EU-spørgsmål spiller en meget aktiv rolle i forbindelse med spørgsmål vedrørende databeskyttelse, at ministeriet for udenrigsanliggender og EU-spørgsmål tilbyder sit personale uddannelse vedrørende databeskyttelse, navnlig før midlertidig udstationering med henblik på udførelse af konsulære opgaver, og at sikkerhedsdepartement (i sin rolle som databeskyttelsesrådgiver) tilbyder sådan uddannelse, at den proceduremæssige og fysiske sikkerhed i forbindelse med beskyttelse af SIS II-data er høj, at databeskyttelsesrådgiveren og den stedfortrædende databeskyttelsesrådgiver i departementet for databeskyttelse under tilsynsenheden i tilsynstjenesten i indenrigsministeriet spiller en meget aktiv rolle, bl.a. i forbindelse med vejledning og logfilkontrol vedrørende SIS II, og at indenrigsministeriet tilbyder uddannelse vedrørende databeskyttelse til alle slutbrugere af N.SIS II.

(3) I betragtning af hvor vigtigt det er at overholde Schengenreglerne på området databeskyttelse i forbindelse med VIS, bør det prioriteres at gennemføre henstilling 7 og 24.

(4) Denne afgørelse bør fremsendes til Europa-Parlamentet og medlemsstaternes parlamenter. Senest 3 måneder efter vedtagelsen af denne afgørelse skal Den Slovakiske Republik i henhold til artikel 16, stk. 1, i forordning (EU) nr. 1053/2013 udarbejde en handlingsplan med en oversigt over alle henstillinger til afhjælpning af de mangler, der blev konstateret i evalueringsrapporten, og forelægge handlingsplanen for Kommissionen og Rådet,

HENSTILLER TIL

Den Slovakiske Republik:

Databeskyttelsesmyndighed

1. at sikre, at datatilsynsmyndighedens budget og medarbejderstab øges yderligere for at forbedre dens resultater og effektivitet

2. at sikre, at den del af det samlede statsbudget, der er afsat til databeskyttelsesmyndigheden er synlig, for derved at sikre, at datatilsynsmyndigheden har et særskilt offentligt årligt budget

3. at sikre, at det nationale råd i forbindelse med budgetproceduren bliver opmærksom på databeskyttelsesmyndighedens holdning, hvad angår dens budgetmæssige behov, og drøftelserne mellem databeskyttelsesmyndigheden og finansministeriet om budgettet

4. at træffe foranstaltninger for at sikre, at finansministeriet ikke kan skabe sammenhæng mellem budgettet og de bødebeløb, databeskyttelsesmyndigheden opkræver, da det kan påvirke arten af databeskyttelsesmyndighedens arbejde og dens prioritering og dermed dens uafhængighed. Det bør sikres, at databeskyttelsesmyndighedens budget ikke kan reduceres i løbet af kalenderåret i en situation, hvor databeskyttelsesmyndigheden ikke fuldt ud har opkrævet de anslåede bøder

5. at sikre, at databeskyttelsesmyndigheden får overdraget alle de opgaver og beføjelser, databeskyttelsesmyndighederne skal have overdraget i henhold til persondataforordningens artikel 57 og 58

6. at sikre, at datatilsynsmyndigheden ud over de regelmæssige tilsynsaktiviteter, der gennemføres på N.SIS-kontoret og SIRENE-kontoret, fører tilsyn med de slutbrugermyndigheder, der har adgang til SIS II

7. at sikre, at datatilsynsmyndighedens tilsynsaktiviteter i forbindelse med VIS omfatter tilsyn med den centrale visummyndighed, hvad angår databehandlingen i N.VIS. Da fristen for den første audit af det nationale visumsystem var i oktober 2015, bør databeskyttelsesmyndigheden hurtigst muligt foretage denne del af auditten, som stadig mangler

8. at sikre, at databeskyttelsesmyndigheden regelmæssigt også fører tilsyn med de eksterne tjenesteydere

De registreredes rettigheder

9. at finde en passende måde for datatilsynsmyndigheden, indenrigsministeriet og ministeriet for udenrigsanliggender og EU-spørgsmål at informere de registrerede om de potentielle risici ved at indgive kopier af ID-kort og følsomme oplysninger via det åbne internet. Indenrigsministeriet og ministeriet for udenrigsanliggender og EU-spørgsmål opfordres til at overveje at stille en sikret elektronisk dataoverførselskanal til rådighed for de registrerede med henblik på indgivelse af sådanne dokumenter

10. at sikre, at fristen på 60 dage for besvarelse af anmodninger fra personer, der er registreret i SIS II, jf. artikel 41, stk. 6, i forordningen om SIS II og artikel 58, stk. 6, i afgørelsen om SIS II, overholdes, indtil de nye SIS-regler[1] finder fuld anvendelse (senest den 28. december 2021), hvori der er krydshenvisninger til fristen for besvarelse af de registreredes anmodninger i henhold til persondataforordningen (30 dage med mulighed for om nødvendigt at forlænge fristen med yderligere to måneder)

11. at overveje at give de registrerede nogle af oplysningerne i trykt form (foldere/skilte m.m.) i politistationernes lokaler og gøre dem synlige og lettilgængelige

12. at overveje at stille f.eks. en uformel engelsk udgave af databeskyttelsesmyndighedens afgørelser i klagesager baseret på anmodninger fra registrerede i SIS II til rådighed; dette ville hjælpe de registrerede til bedre at forstå afgørelserne og dermed styrke deres rettigheder

13. at sikre, at det er lettere at finde oplysningerne om de i VIS registreredes rettigheder på webstedet for ministeriet for udenrigsanliggender og EU-spørgsmål; webstedet bør også indeholde modeller for udøvelse af de i VIS registreredes rettigheder

---

[1] Europa-Parlamentets og Rådets forordning (EU) 2018/1862 af 28. november 2018 om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området politisamarbejde og strafferetligt samarbejde, om ændring og ophævelse af Rådets afgørelse 2007/533/RIA og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 1986/2006 og Kommissionens afgørelse 2010/261/EU (EUT L 312 af 7.12.2018, s. 56) (se navnlig artikel 66-71). Europa-Parlamentets og Rådets forordning (EU) 2018/1861 af 28. november 2018 om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området ind- og udrejsekontrol, om ændring af konventionen om gennemførelse af Schengenaftalen og om ændring og ophævelse af forordning (EF) nr. 1987/2006 (EUT L 312 af 7.12.2018, s. 14) (se navnlig artikel 51-56).

14. at sikre, at visumansøgningsskemaet indeholder klare oplysninger om de forskellige myndigheder, der behandler personoplysninger som en del af det nationale visumsystem. Det bør navnlig indeholde oplysninger om, at det er ministeriet for udenrigsanliggender og EU-spørgsmål, der er dataansvarlig

15. at stille fysiske oplysninger (foldere/skilte m.m.) til rådighed for de i VIS registrerede i lufthavne og ved grænsekontrolsteder og gøre dem synlige og let tilgængelige

16. at sikre, at svarene til de registrerede vedrørende personoplysninger i VIS indeholder oplysninger om muligheden for at klage over svaret til databeskyttelsesmyndigheden eller indbringe sagen for den kompetente domstol

17. at træffe de nødvendige foranstaltninger for at præcisere, hvilket ansvar ministeriet for udenrigsanliggender og EU-spørgsmål og den centrale visummyndighed (indenrigsministeriet) har for behandlingen af de i VIS registreredes anmodninger, og at stille intern eller metodologisk vejledning til rådighed for begge; disse oplysninger bør være tilgængelige for de registrerede

Visuminformationssystemet

18. at træffe de nødvendige foranstaltninger for at øge sikkerhedsniveauet i forbindelse med adgang til det statslige miljø og navnlig de nationale visumansøgninger i ministeriet for udenrigsanliggender og EU-spørgsmål og hos den centrale visummyndighed (indenrigsministeriet), navnlig ved adgang til de nationale visumdatabaser via multifaktor-teknologi

19. at træffe de nødvendige foranstaltninger for at forbedre den fysiske og organisatoriske sikkerhed i N.VIS-datacentret i ministeriet for udenrigsanliggender og EU-spørgsmål, navnlig følgende aspekter:

    – fremlæggelse ved indgangen til datacentret af en logbog for IKT-personale, besøgende eller leverandører, hvis adgang bør begrænses

    – installation af et brandslukningssystem med gas (aragonit)

    – installation af system til opdagelse af vandlækager

    – sikring af et støvfrit og opryddet gulv

    – aflåsning af sikkerhedshegnet om EU-servere

20. at fremskynde proceduren for oprettelse af et nyt N.VIS-datacenter et andet sted og flytningen af det nuværende datacenter

21. at overveje at ændre den lokale lagringsperiode for N.VIS-logfilerne på de diplomatiske og konsulære repræsentationer ved at fastsætte en tidsfrist i stedet for MB-størrelsen

22. at overveje at anvende automatiske logkontrolsystemer i ministeriet for udenrigsanliggender og EU-spørgsmål

23. at træffe de nødvendige foranstaltninger for at sikre, at de diplomatiske repræsentationer eller ministeriet for udenrigsanliggender og EU-spørgsmål regelmæssigt fører tilsyn med de eksterne tjenesteydere

24. at træffe de nødvendige foranstaltninger for at sikre, at lokalt konsulært personale mere systematisk og på ensartet vis tilbydes uddannelse vedrørende databeskyttelse

25. at sikre, at der i forbindelse med elektroniske visumansøgninger indhentes de samme oplysninger som i forbindelse med visumansøgninger i papirform (som fastsat i bilag I til EU-visumkodeksen[1])

Schengeninformationssystem II

26. at træffe de nødvendige foranstaltninger for at forbedre sikkerhedsniveauet for adgang til N.SIS II, navnlig ved at anvende multifaktorautentificering og udelukkende https-forbindelser for adgang til N.SIS II

27. at sikre, at indenrigsministeriet underretter datatilsynsmyndigheden om alle brud på datasikkerheden, som kan forventes at indebære en risiko for fysiske personers rettigheder og frihedsrettigheder. Derudover bør indenrigsministeriet oprette et register over brud på persondatasikkerheden

[1] Europa-Parlamentets og Rådets forordning (EF) nr. 810/2009 af 13. juli 2009 om en fællesskabskodeks for visa (visumkodeks) EFT af 15.9.2009, L243/1.

Information til offentligheden

28. at overveje også at stille foldere til rådighed for de registrerede på mere tilgængelige steder såsom politistationer, grænsekontrolområder og konsulater

29. at overveje også at gøre datatilsynsmyndighedens præsentationer, seminarer og åbenhus-arrangementer tilgængelige for den brede offentlighed, navnlig de registrerede, da oplysningerne om SIS II og VIS er af betydning for dem.

Udfærdiget i Bruxelles, den … .

På Rådets vegne
Formand