Rådet for
Den Europæiske Union

Bruxelles, den 24. september 2019
(OR. en)

12468/19

Interinstitutionel sag:
2019/0168(NLE)

SCH-EVAL 157
DATAPROTECT 216
COMIX 427

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
dato:	20. september 2019
til:	delegationerne
Tidl. dok. nr.:	11904/19
Vedr.:	Rådets gennemførelsesafgørelse om fastlæggelse af en henstilling om afhjælpning af de mangler, der blev konstateret ved evalueringen i 2018 af **Litauens** anvendelse af Schengenreglerne på området **databeskyttelse**

Vedlagt følger til delegationerne Rådets gennemførelsesafgørelse om en henstilling om afhjælpning af de mangler, der blev konstateret ved evalueringen i 2018 af Lithauens anvendelse af Schengenreglerne på området databeskyttelse, som Rådet vedtog på samlingen den 20. september 2019.

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 2018 af Litauens 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 en række henstillinger om foranstaltninger til Litauen for at afhjælpe de mangler, der blev konstateret under evalueringen i 2018 af anvendelsen af Schengenreglerne på området databeskyttelse. Efter evalueringen vedtog Kommissionen ved gennemførelsesafgørelse C(2019) 5700 en rapport om resultaterne og vurderingen heraf, som indeholder en liste over bedste praksis og mangler, der blev konstateret under evalueringen.

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

(2) Det anses bl.a. for god praksis, at databeskyttelsesmyndigheden yder råd og vejledning til enkeltpersoner, der retter henvendelse til den, i stedet for blot at videresende anmodninger; at der foreligger standardbreve til brug ved de registreredes udøvelse af deres rettigheder i forbindelse med Schengeninformationssystem II (SIS II) og visuminformationssystemet (VIS); at de sikkerhedsforanstaltninger, der er truffet i departementet for informationsteknologi og kommunikation under indenrigsministeriet (departementet hoster N.VIS og N.SIS) generelt er af høj standard og sikrer et sikkert miljø for lagring af oplysninger og for forebyggelse af mulige hændelser; at der er god uddannelse af VIS-slutbrugerne, navnlig konsulære medarbejdere, inden de udsendes til ambassader/konsulater; at der lægges vægt på uddannelse og udvikling af personalet, navnlig god uddannelse, herunder vedrørende databeskyttelse, af slutbrugerne af N.SIS og personalet på SIRENE-kontoret; at de oplysninger, som databeskyttelsesmyndigheden giver på sit websted vedrørende SIS II og VIS, er meget omfattende og nyttige og er skrevet i et let tilgængeligt sprog (og findes på flere sprog); at databeskyttelsesmyndighedens brochurer om beskyttelse af personoplysninger i Schengeninformationssystemet og beskyttelse af personoplysninger i visuminformationssystemet indeholder meget gode og tilgængelige oplysninger om databehandlingen i begge databaser og de registreredes rettigheder i forbindelse hermed, og at databeskyttelsesmyndigheden engagerer sig stærkt i mange konferencer, uddannelsesforløb og andre oplysningsarrangementer, bl.a. for personale, der er beskæftiget med databehandling i SIS II og VIS.

(3) I lyset af betydningen af at overholde Schengenreglerne vedrørende databeskyttelse, navnlig at sikre, at databeskyttelsesmyndigheden er helt uafhængig, bør det prioriteres at gennemføre henstilling 1.

(4) Denne afgørelse bør sendes til Europa-Parlamentet og de nationale parlamenter. Inden tre måneder efter vedtagelsen skal Litauen i medfør af artikel 16, stk. 1, i forordning (EU) nr. 1053/2013 udarbejde en handlingsplan med en oversigt over alle henstillinger med henblik på at afhjælpe de mangler, der blev konstateret i evalueringsrapporten, og forelægge handlingsplanen for Kommissionen og Rådet,

HENSTILLER TIL

Litauen:

Databeskyttelsesmyndigheden

1. for i højere grad at sikre, at det statslige databeskyttelsesinspektorat (herefter databeskyttelsesmyndigheden) er helt uafhængigt, at afskaffe kravene om, at databeskyttelsesmyndighedens strategiske handlingsplan skal godkendes af justitsministeriet, og at justitsministeren skal høres om den årlige handlingsplan, før direktøren for databeskyttelsesmyndigheden kan godkende den; dette er også vigtigt for at sikre, at budgetproceduren ikke indebærer nogen risiko for, at databeskyttelsesmyndighedens uafhængighed krænkes

2. for i højere grad at sikre, at databeskyttelsesmyndigheden er helt uafhængig, at tilrettelægge de bilaterale møder, der regelmæssigt afholdes mellem justitsministeren og direktøren for databeskyttelsesmyndigheden, på en sådan måde, at der ikke opstår risiko for, at regeringen direkte eller indirekte påvirker databeskyttelsesmyndigheden, hvilket kunne bringe dens uafhængighed i fare

3. at fjerne alle de elementer i kravet om, at direktøren for databeskyttelsesmyndigheden skal stå til ansvar over for regeringen og justitsministeren, der kan medføre risiko for, at regeringen og justitsministeren udøver direkte eller indirekte indflydelse og bringe databeskyttelsesmyndighedens uafhængighed i fare

4. at sikre, at databeskyttelsesmyndigheden oftere fører kontrol med, at behandlingen af SIS II-oplysninger er lovlig

5. at sikre, at databeskyttelsesmyndigheden som minimum hvert fjerde år gennemfører audit af databehandlingen i N.SIS

6. at sikre, at databeskyttelsesmyndigheden fører kontrol med, at behandlingen af VIS-oplysninger er lovlig. Databeskyttelsesmyndigheden bør også føre tilsyn med databehandlingen og datasikkerheden hos de eksterne tjenesteydere, når den fører tilsyn med ambassader; denne mulighed bør fastsættes i kontrakten mellem udenrigsministeriet og de eksterne tjenesteydere;

7. at sikre, at databeskyttelsesmyndigheden som minimum hvert fjerde år gennemfører audit af databehandlingen i N.VIS

De registreredes rettigheder

8. at sikre, at den frist på 60 dage for at besvare anmodninger fra registrerede i SIS II, der er fastsat i artikel 41, stk. 6, i forordningen om SIS II og artikel 58, stk. 6, i afgørelsen om SIS II vil blive overholdt, indtil de nye SIS-regler[2] finder fuld anvendelse (senest den 28. december 2021); i disse regler er der krydshenvisninger til den frist for at besvare anmodninger fra registrerede, der er fastsat i den generelle forordning om databeskyttelse (GDPR)[3] (30 dage med mulighed for forlængelse med to måneder, hvis det er nødvendigt)

9. at præcisere de interne procedurer vedrørende de involverede myndigheders ansvar for at tage hånd om de i SIS II registreredes rettigheder; på den måde vil personalet også kunne blive opmærksom på, hvem de skal henvise anmodninger til

---

[2] 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) (jf. 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) (jf. navnlig artikel 51-57).

[3] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

10. at sikre, at indenrigsministeriet svarer ensartet i alle endelige svar til enkeltpersoner, der ønsker at udøve deres rettigheder som registrerede i SIS II, således at de får oplysninger om deres ret til at klage til databeskyttelsesmyndigheden samt deres ret til at indbringe sagen for domstolene

11. at præcisere de interne procedurer vedrørende de involverede myndigheders ansvar for at tage hånd om de i VIS registreredes rettigheder; på den måde kan personalet også blive opmærksom på, hvem de skal henvise anmodninger til

12. at sikre, at indenrigsministeriet svarer ensartet i alle endelige svar til enkeltpersoner, der ønsker at udøve deres rettigheder som registrerede i VIS, således at de får oplysninger om deres ret til at klage til databeskyttelsesmyndigheden samt deres ret til at indbringe sagen for domstolene

Visuminformationssystemet

13. at træffe de nødvendige foranstaltninger til at sikre, at det i kontrakterne mellem udenrigsministeriet og de eksterne tjenesteydere fastsættes, hvordan den litauiske databeskyttelsesmyndighed kan involveres i de tilsyn, som ambassader/konsulater og udenrigsministeriet foretager

14. at forbedre egenkontrollen ved proaktivt at tjekke logfiler regelmæssigt for at føre kontrol med, at behandlingen af VIS-personoplysninger er lovlig. Indenrigsministeriet bør videreudvikle SIEM-systemet med henblik på automatisk kontrol af logfiler

15. at sikre, at udenrigsministeriets databeskyttelsesrådgiver involveres mere i udviklingen og gennemførelsen af databeskyttelseuddannelse af medarbejdere i udenrigsministeriet, herunder dem, der er udsendt til ambassader og konsulater

Schengeninformationssystem II

16. at fjerne slutbrugernes mulighed for via POLIS-browseren at logge ind i N.SIS med flere enheder samtidigt

17. at sikre, at der indføres smartkort for at få adgang til N.SIS-brugeres arbejdsstationer hos politiet for derved at forbedre sikkerhedsniveauet og -standarden

18. at sikre, at de tekniske foranstaltninger, der er truffet for at forhindre brugen af USB-nøgler i SIRENE-kontorets arbejdsstationer, anvendes fuldt ud og kontrolleres regelmæssigt

19. at forbedre egenkontrollen ved proaktivt at tjekke SIS II-slutbrugeres logfiler hos alle berørte myndigheder regelmæssigt for at føre kontrol med, at behandlingen af SIS II-personoplysninger er lovlig; indenrigsministeriet bør videreudvikle SIEM-systemet med henblik på automatisk kontrol af logfiler

20. at sikre, at kendskabet til databeskyttelse blandt personalet i forbindelse med håndteringen af SIS II- og VIS-oplysninger forbedres ved hjælp af regelmæssige genopfriskningskurser

21. at sikre, at uddannelsen og bevidstgørelsen af personale med adgang til N.SIS udgør et område, som gruppen af databeskyttelsesrådgivere i indenrigsministeriet står i spidsen for. Herved kan det sikres, at der er en kontinuerlig struktur for og planlægning af udviklingen af personalet

Information til offentligheden

22. at sikre, at links på databeskyttelsesmyndighedens websted vedrørende SIS II og VIS ajourføres regelmæssigt

23. at sikre, at webstederne for organisationer, der har kontakt med statsborgere i andre lande såsom indenrigsministeriet, politiet, det statslige grænsepoliti, udenrigsministeriet og konsulære repræsentationer også giver tilgængelige og klare oplysninger på engelsk om SIS II og VIS og de registreredes rettigheder i forbindelse hermed

24. at sikre, at webstedernes oplysninger på engelsk om SIS II og VIS og de registreredes rettigheder i forbindelse hermed er lettere at finde

25. at sikre ensartethed af de oplysninger om de registreredes udøvelse af deres rettigheder i relation til N.SIS II og VIS, der findes på de institutioners websteder, som arbejder med disse systemer

26. at tilføje oplysninger om databehandling og de registreredes rettigheder i forbindelse med VIS til EPM-portalen, som enkeltpersoner anvender til indgivelse af oplysninger i forbindelse med visumansøgninger.

Udfærdiget i Bruxelles, den […].

På Rådets vegne
Formand