Rådet for
Den Europæiske Union

Bruxelles, den 22. februar 2022
(OR. en)

6426/22

Interinstitutionel sag:
2021/0392(NLE)

SCH-EVAL 21
DATAPROTECT 42
COMIX 87

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
dato:	21. februar 2022
til:	delegationerne
Tidl. dok. nr.:	5893/22
Vedr.:	Rådets gennemførelsesafgørelse om fastlæggelse af en henstilling om afhjælpning af de mangler, der blev konstateret ved evalueringen i 2019 af **Polens** 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 Polens anvendelse af Schengenreglerne på området databeskyttelse, som Rådet vedtog på samlingen den 21. februar 2022.

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 Polens 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) I overensstemmelse med forordning (EU) nr. 1053/2013 blev der i 2019 foretaget en evaluering med henblik på at kontrollere anvendelsen af Schengenreglerne på området beskyttelse af personoplysninger i Polen. Efter evalueringen vedtog Kommissionen ved gennemførelsesafgørelse C(2021)9100 en rapport med resultaterne og vurderingen heraf, som indeholder en liste over bedste praksis og mangler, der blev konstateret under evalueringen.

(2) På baggrund af resultaterne af evalueringen bør der fremsættes henstillinger til Polen om visse foranstaltninger til afhjælpning af de mangler, der blev konstateret.

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

(3) Den nationale retlige ramme, der giver formanden for den polske databeskyttelsesmyndighed mulighed for uafhængigt at udnævne sine stedfortrædere samt medlemmerne af det rådgivende råd, kravet om, at kandidaterne til stillingen som formand for databeskyttelsesmyndigheden skal gennemgå en offentlig høring i parlamentet, som også sendes via parlamentets officielle kanal på internettet, hyppige kontrolaktiviteter for så vidt angår eksterne tjenesteydere med inddragelse af databeskyttelsesrådgiveren og hyppig kontrol fra konsulaternes side, tilsagnet om uddannelse og udvikling af personale, herunder om databeskyttelse, for slutbrugere af det nationale Schengeninformationssystem (N.SIS) og SIRENE-kontorets personale samt de sikkerhedsforanstaltninger, der er gennemført i lokaler tilhørende begge datacentre, der huser N.SIS og det nationale visuminformationssystem (N.VIS), anses for at være god praksis.

(4) I betragtning af hvor vigtigt det er at overholde Schengenreglerne på området beskyttelse af personoplysninger i forbindelse med visuminformationssystemet (VIS) og Schengeninformationssystemet (SIS), bør det prioriteres at gennemføre denne afgørelses henstilling 11, 12, 13, 20, 21 og 22.

(5) I medfør af forordning (EU) nr. 1053/2013 bør denne afgørelse sendes til Europa-Parlamentet og medlemsstaternes parlamenter, og Polen bør inden for en frist på tre måneder fra vedtagelsen fastsætte en handlingsplan, der indeholder en liste over alle henstillinger, for at afhjælpe de mangler, der blev konstateret i evalueringsrapporten, og forelægge handlingsplanen for Kommissionen og Rådet,

HENSTILLER TIL

Polen:

Lovgivning

1. udtrykkeligt at præcisere, hvordan 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) anvendes i forbindelse med behandling af personoplysninger i N.VIS og N.SIS, hvor det er relevant

Databeskyttelsesmyndighed

2. at sikre, at artikel 174 i databeskyttelsesloven fra 2018 og artikel 106 i loven om databeskyttelse på retshåndhævelsesområdet fra 2018, som fastsætter den maksimale udgiftsgrænse pr. år, ikke begrænser den polske databeskyttelsesmyndigheds budget til mindre end de beløb, der er afsat i statsbudgettet for et givet år

3. at sikre, at databeskyttelsesmyndigheden forbedrer planlægningen og tilrettelæggelsen af adskillelige inspektioner af N.SIS II for at sikre, at alle behandlingsaktiviteter i N.SIS II og alle relevante enheder er omfattet, og at inspektionerne resulterer i en omfattende audit af N.SIS II i overensstemmelse med artikel 44, stk. 2, i forordning (EF) nr. 1987/2006

4. at sikre, at databeskyttelsesmyndigheden foretager en omfattende audit af N.VIS for fuldt ud at udføre sine opgaver i overensstemmelse med artikel 41, stk. 2, i forordning (EF) nr. 767/2008

De registreredes rettigheder

5. at sikre, at databeskyttelsesmyndighedens statistikker vedrørende udøvelsen af de registreredes rettigheder forbedres og differentierer klager fra anmodninger, det system, de vedrører (SIS eller VIS), sagsgenstanden samt typen af anmodning (rettelse, sletning, adgang)

6. at sikre, at den dataansvarlige anvender en mere proaktiv tilgang med hensyn til at oplyse om de registreredes rettigheder i forbindelse med VIS-oplysninger

7. at sikre, at den dataansvarlige for SIS og VIS (det nationale polske politis centrale tekniske myndighed for det nationale IT-system (CTA NITS) offentliggør standardformularer til anmodninger om udøvelse af de registreredes rettigheder

Visuminformationssystemet

8. at sikre, at registrene over adgang til VIS også indeholder oplysninger om begrundelsen for den pågældende adgang

9. at revurdere listen over myndigheder med adgang til VIS og deres adgangsrettigheder til VIS-oplysninger på baggrund af deres kompetencer og anvendelse af sådanne oplysninger i praksis

10. i lyset af de mange forskellige VIS-dataansvarlige, der er indført i kraft af de nationale love og kontraktbestemmelser, og i betragtning af de mange involverede aktører at præcisere forholdet mellem de myndigheder, der er involveret i visumudstedelsesprocessen, og de myndigheder, der behandler VIS-oplysninger, samt disse myndigheders ansvar for databehandlingen

11. at sikre, at VIS-logfilerne analyseres regelmæssigt for at overvåge databeskyttelsen og gøre fuld brug af de opbevarede logfiler

12. at vedtage en sikkerhedsplan for VIS, der omfatter fysisk sikkerhed på det andet datasite samt andre IT-sikkerhedsaspekter af det nationale IT-system, herunder N.VIS-systemet

13. at bringe opbevaringsperioden for logfiler i forbindelse med VIS (navnlig i applikationerne "Pobyt" og "ZSE 6") i overensstemmelse med fristerne i artikel 34, stk. 2, i forordning (EF) nr. 767/2008 og artikel 16 i Rådets afgørelse 2008/633/RIA

Schengeninformationssystem II

14. at sikre, at den dataansvarlige for N.SIS II opretter et centralt brugerstyringssystem, der muliggør en effektiv egenkontrol, uden at det er nødvendigt at konsultere logfiler i de institutioner, der er slutbrugere af N.SIS II-systemet

15. at sikre, at SIS-logfilerne analyseres regelmæssigt for at overvåge databeskyttelsen og gøre fuld brug af de opbevarede logfiler

16. at sikre en automatiseret indberetning af IT-sikkerhedshændelser og den dataansvarliges egenovervågningsaktiviteter med henblik på yderligere at forbedre sikkerheden

17. at sikre, at tekniske foranstaltninger også omfatter blokering af brugen af USB-udstyr eller -nøgler ved at blokere alle USB-porte på SIS-arbejdsstationer

18. at overveje at lade indenrigsministeriets databeskyttelsesrådgiver deltage proaktivt og regelmæssigt i overvågningen af behandlingen af SIS- og VIS-oplysninger gennem overvågning af auditlogfiler

19. at sikre, at den dataansvarlige for SIS giver databeskyttelsesmyndigheden personaleprofilerne fra alle myndigheder med adgang til SIS

20. at bringe opbevaringsperioden for logfiler i applikationerne med adgang til SIS-data i overensstemmelse med artikel 12, stk. 4, i forordning (EF) nr. 1987/2006 og artikel 12, stk. 4, i Rådets afgørelse 2007/533/RIA

21. at sikre, at den dataansvarlige for SIS i overensstemmelse med artikel 10 i forordning (EF) nr. 1987/2006 og artikel 10 i Rådets afgørelse 2007/533/RIA vedtager en sikkerhedsplan for SIS

22. at sikre, at den brede vifte af institutioner, der har adgang til SIS II-oplysninger, gennemgås for at sikre, at kun de institutioner, der har brug for adgang i betragtning af deres kompetencer og praktiske behov, kan få adgang til oplysningerne

Oplysninger til offentligheden

23. at sikre, at databeskyttelsesmyndighedens og politiets websteder indeholder oplysninger om de registreredes rettigheder i forbindelse med VIS-oplysninger.

Udfærdiget i Bruxelles, den […].

På Rådets vegne

Formand