



Bruxelles, den 26. november 2018
(OR. en)

14763/18

Interinstitutionel sag:
2018/0338(NLE)

SCH-EVAL 228
DATAPROTECT 258
COMIX 648

RESULTAT AF DRØFTELSENE

fra: Generalsekretariatet for Rådet

dato: 26. november 2018

til: delegationerne

Tidl. dok. nr.: 14114/18

Vedr.: Rådets gennemførelsesafgørelse om fastlæggelse af en henstilling om afhjælpning af de mangler, der blev konstateret ved evalueringen i 2017 af Norges anvendelse af Schengenreglerne på området **dataskyttelse**

Vedlagt følger til delegationerne Rådets gennemførelsesafgørelse om en henstilling om afhjælpning af de mangler, der blev konstateret ved evalueringen i 2017 af Norges anvendelse af Schengenreglerne på området dataskyttelse, som Rådet vedtog på samlingen den 26. november 2018.

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 2017 af Norges 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 Schengenreglerne¹, 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 Norge for at afhjælpe de mangler, der blev konstateret under evalueringen i 2017 af landets anvendelse af Schengenreglerne på området databeskyttelse. Efter evalueringen vedtog Kommissionen ved gennemførelsesafgørelse C(2018) 4145 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 opfattes bl.a. som god praksis, at der findes veludviklede uddannelseskurser for slutbrugere af NORVIS, at det norske udenrigsministerium har et omfattende sæt procedurer, herunder brugen af fastlagte tjeklister, for overvågning af konsulære repræsentationer og informering af disse om praksis med hensyn til overvågning af eksterne tjenesteydere, at Kripos (den nationale enhed for bekæmpelse af organiseret og anden alvorlig kriminalitet) og politidistrikterne har gjort en omfattende indsats, hvad angår uddannelse og bevidstgørelse af deres personale, herunder vedrørende databeskyttelsesspørgsmål, at de seks databeskyttelsesmedarbejdere i Kripos er ansvarlige for alle retlige og praktiske aspekter af databeskyttelsen for Kripos og spiller en meget aktiv rolle i organisationen, og at politidistrikternes databeskyttelsesansvarlige har et lignende engagement og er proaktive med hensyn til at fremme et højt databeskyttelsesniveau.
- (3) I lyset af betydningen af at overholde Schengenreglerne vedrørende databeskyttelse i relation til Schengeinformationssystem II og visuminformationssystemet bør det prioriteres at gennemføre henstilling 8, 22, 27, 28 og 29 nedenfor.
- (4) Denne afgørelse bør forelægges Europa-Parlamentet og de nationale parlamenter. Inden tre måneder efter vedtagelsen af denne afgørelse bør Norge 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

at Norge:

Tilsynsmyndigheden for databeskyttelse (Datatilsynet)

1. for i højere grad at sikre, at Datatilsynet er fuldstændig uafhængigt, ændrer bestemmelserne i retningslinjerne vedrørende økonomi og drift og tilsagnsskrivelsen på en sådan måde, at de ikke indebærer en risiko for, at regeringen direkte eller indirekte påvirker Datatilsynet, hvilket kunne bringe sidstnævntes uafhængighed i fare

2. for i højere grad at sikre, at Datatilsynet er fuldstændig uafhængigt, tilrettelægger uformelle møder mellem chefen for Datatilsynet og Kommunal- og moderniseringsdepartementet på en sådan måde, at de ikke indebærer en risiko for, at regeringen direkte eller indirekte påvirker Datatilsynet, hvilket kunne bringe sidstnævntes uafhængighed i fare
3. afskaffer alle de elementer i Datatilsynets underordnede stilling i forhold til kongen og Kommunal- og moderniseringsdepartementet, som kan indebære en risiko for, at regeringen direkte eller indirekte kan påvirke Datatilsynet og således bringe dets uafhængighed i fare
4. for i højere grad at sikre, at Datatilsynet er fuldstændig uafhængigt, reformerer budgetproceduren på en sådan måde, at Datatilsynet har reel indflydelse på forslaget til dets budget, inden det almindelige budget sendes til Stortinget med henblik på drøftelse og vedtagelse, og at Stortinget gøres bekendt med forslaget til Datatilsynets budget
5. øger Datatilsynets beføjelser ved at give det en effektiv måde til at håndhæve sine afgørelser på for så vidt angår ulovlig behandling af personoplysninger fra Schengeninformationssystem II (herefter "SIS II")
6. sikrer, at Datatilsynet kontrollerer lovligheden af personoplysninger fra SIS II, herunder en mere regelmæssig analyse af logfiler
7. sikrer, at Datatilsynet kontrollerer lovligheden af personoplysninger fra visuminformationssystemet (herefter "VIS"), herunder en mere regelmæssig analyse af logfiler
8. sikrer, at Datatilsynet mindst hvert fjerde år foretager revisioner af databehandlingsoperationerne i det nationale VIS-system. Da fristen for den første revision (oktober 2015) ikke blev overholdt, bør der træffes foranstaltninger til så hurtigt som muligt at opfylde denne forpligtelse

De registreredes rettigheder

9. fremlægger klare oplysninger på de relevante websteder (navnlig Datatilsynets og politiets websteder) om de to muligheder for at udøve de rettigheder, som registrerede i SIS II har: De registrerede kan enten indgive en anmodning til Kripos (med mulighed for at indgive en anmodning om efterprøvelse til Politidirektoratet, som træffer afgørelse efter udtalelse fra Datatilsynet), eller de registrerede kan indgive en anmodning til Datatilsynet
10. afskaffer de registreredes pligt til altid at fremlægge en notarielt bekræftet kopi af det dokument, der dokumenterer deres identitet, undtagen i situationer, hvor der er grund til at betvivle den registreredes identitet
11. fremlægger oplysninger på norsk politis websted om fristen for at besvare anmodninger fra de i SIS II registrerede og om muligheden for at indgive en anmodning om efterprøvelse til Politidirektoratet, og om, hvor en sådan anmodning skal sendes hen
12. fremlægger standardbreve for udøvelsen af de i VIS-registreredes rettigheder på Datatilsynets, udenrigsministeriets og konsulære repræsentationers websteder
13. fremlægger oplysninger på Datatilsynets websted om muligheden for at kontakte Datatilsynet direkte vedrørende spørgsmål i forbindelse med VIS, herunder indgive en klage om udøvelsen af de i VIS-registreredes rettigheder

Visuminformationssystemet

14. sikrer, at kontrakten mellem Utlendingsdirektoratet og Sopra Steria (driften og vedligeholdelsen af IT-infrastruktur) indeholder specifikke projektleverancer, således at Sopra Steria kan træffe rutineforanstaltninger med henblik på vedligeholdelsen af systemet, og at Utlendingsdirektoratet sikrer, at de har kontrol over alle Sopra Sterias vedligeholdelsesforanstaltninger

15. forbedrer den fysiske sikkerhed ved NORVIS-serverlokalerne ved at indføre et omfattende sæt kriterier, der skal sikre, at Sopra Steria har tilstrækkelig kontrol over den eksterne leverandør af IT-udstyr og ansvarlige for vedligeholdelsen heraf, navnlig i relation til sikkerhed og adgang til serverrackkabinetter
16. overvejer at oprette et backup-center for NORVIS på en anden lokalitet
17. sikrer, at Utlendingsdirektoratet indfører en procedure for regelmæssig og proaktiv kontrol af NORVIS-logfiler, herunder administratorlogfiler
18. sikrer, at der under overholdelse af kravene i artikel 34 i VIS-forordningen om sletning af logfiler (et år efter, at lagringsperioden for data, der er indlæst i VIS, er udløbet) indføres et system (enten automatisk eller manuelt), der sikrer, at logfilerne regelmæssigt slettes
19. sikrer, at Utlendingsdirektoratet overvejer at ændre placeringen af lagret af backupbånd og sikrer, at dette er placeret i passende afstand fra datacentrene, og at der regelmæssigt foretages test af genoprettelse af systemet
20. sikrer, at der tilbydes yderligere særlig uddannelse til IT-personale i Utlendingsdirektoratet, således at de er bedre informeret med henblik på overvågning af systemet og af udliciteringsvirksomheders aktiviteter
21. sikrer, at Utlendingsdirektoratet udformer en mere struktureret og omfattende procedure for overvågning af forvaltningens adgang til NORVIS-servere, regelmæssig proaktiv logfilkontrol, tilsyn med datacentrene og generelt et mere aktivt overblik over IT-forvaltningsvirksomhedernes aktiviteter
22. sikrer, at Utlendingsdirektoratet med henblik på artikel 32 i VIS-forordningen gennemgår sine aktiviteter og indfører effektive procedurer for logningsaktiviteter i forbindelse med NORVIS-systemet; Utlendingsdirektoratet bør indføre et effektivt system, der skal sikre, at databaseadministratorens/administratorens handlinger logføres, således at Utlendingsdirektoratet kan føre kontrol med og have overblik over disse aktiviteter

Schengeninformationssystemet

23. sikrer, at Kripos indfører tekniske foranstaltninger med henblik på at forhindre brugen af personlige USB-nøgler i SIRENE-arbejdsstationer
24. sikrer, at Kripos indfører tekniske foranstaltninger for at registrere de dokumenter, der udprintes fra en SIRENE-arbejdsstation
25. sikrer, at det norske politi opretter profiler, der beskriver de funktioner og det ansvar, personer, der har fået bemyndigelse til at tilgå, indlæse, ajourføre, slette og søge i data i SIS II (som krævet i artikel 10, stk. 1, litra g), i SIS II-forordningen, og i artikel 10, stk. 1, litra g), i Rådets afgørelse om SIS II). Det skal navnlig sikres, at der ud over SIRENE-personale kun gives adgang til SIS II til de polititjeneste, der med henblik på deres arbejde har brug for at foretage politikontrol
26. sikrer, at et SIS II-datacenter sikres bedre, og at processen med at oprette et nyt og mere sikkert datacenter i fjerde kvartal af 2019 fremskyndes
27. sikrer, at slettede udenlandske filer, som ikke har givet nogen hit, som fastsat i artikel 38, stk. 2, i SIS II-forordningen, slettes et år efter, at den tilknyttede indberetning i SIS II er slettet
28. sikrer, at SIS II-registreringer som fastsat i artikel 12, stk. 4, i SIS II-forordningen, og i artikel 12, stk. 4, i Rådets afgørelse om SIS II slettes tidligst et år og senest tre år efter deres oprettelse
29. sikrer, at logfiler om alle beskeder, der er sendt og modtaget via Schengensystemet (oprettelse, opdatering eller sletning af norske indberetninger) slettes i overensstemmelse med kravene i artikel 12, stk. 4, i SIS II-forordningen, og i artikel 12, stk. 4, i Rådets afgørelse om SIS II

Bevidstgørelse af offentligheden

30. sikrer, at oplysningerne på norsk politis websted om de i SIS II registreredes rettigheder og Datatilsynets ansvar bliver lettere at finde
31. overvejer, om Datatilsynet og de norske politimyndigheder skal stille trykt informationsmateriale om SIS II og de registreredes tilknyttede rettigheder til rådighed for offentligheden
32. sikrer, at der stilles omfattende oplysninger vedrørende behandlingen af personoplysninger i VIS og de registreredes tilknyttede rettigheder til rådighed for offentligheden på Datatilsynets, udenrigsministeriets og de konsulære repræsentationers websteder
33. overvejer, om Datatilsynet og de konsulære repræsentationer skal stille trykt informationsmateriale om VIS og de registreredes tilknyttede rettigheder til rådighed for offentligheden.

Udfærdiget i Bruxelles,

På Rådets vegne

Formand
