Europeiska unionens råd

Bryssel den 14 maj 2025
(OR. en)

8833/25

**Interinstitutionellt ärende:**
**2024/0126(NLE)**

**SCH-EVAL 29**
**DATAPROTECT 88**
**COMIX 140**
***NO***
***CH***
***IS***
***LI***

**LÄGESRAPPORT**

| | |
|---|---|
| från: | Rådets generalsekretariat |
| till: | Delegationerna |
| Föreg. dok. nr: | 8093/25 |
| Ärende: | Rådets genomförandebeslut om fastställande av en rekommendation om åtgärder för att avhjälpa de brister som konstaterats vid 2021 års utvärdering av Italiens tillämpning av Schengenregelverket i fråga om dataskydd |

För delegationerna bifogas rådets genomförandebeslut om fastställande av en rekommendation om åtgärder för att avhjälpa de brister som konstaterats vid 2021 års utvärdering av Italiens tillämpning av Schengenregelverket i fråga om dataskydd, som antogs av rådet vid mötet den 12 maj 2025.

I enlighet med artikel 15.3 i rådets förordning (EU) nr 1053/2013 av den 7 oktober 2013 kommer denna rekommendation att översändas till Europaparlamentet och de nationella parlamenten.

**BILAGA**

Rådets genomförandebeslut om fastställande av en

**REKOMMENDATION**

**om åtgärder för att avhjälpa de brister som konstaterats vid 2021 års utvärdering av Italiens tillämpning av Schengenregelverket i fråga om dataskydd**

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av rådets förordning (EU) nr 1053/2013 av den 7 oktober 2013 om inrättande av en utvärderings- och övervakningsmekanism för kontroll av tillämpningen av Schengenregelverket och om upphävande av verkställande kommitténs beslut av den 16 september 1998 om inrättande av Ständiga kommittén för genomförande av Schengenkonventionen[1], särskilt artikel 15.3,

med beaktande av Europeiska kommissionens förslag, och

av följande skäl:

(1) En Schengenutvärdering i fråga om skydd av personuppgifter genomfördes med avseende på Italien i september 2021. Efter utvärderingen antogs den 30 maj 2024 genom kommissionens genomförandebeslut C(2024) 1910 en rapport som innehåller resultat och bedömningar samt en redogörelse för bästa praxis och brister som konstaterades under utvärderingen.

1 EUT L 295, 6.11.2013, s. 27.

(2) Som god praxis betraktas i synnerhet de omfattande säkerhetsåtgärderna avseende den fysiska säkerheten kring servern för den nationella delen av Schengens informationssystem (N.SIS); den omfattande utbildning som tillhandahålls personal hos N.SIS och Sirenekontoret samt slutanvändare, i synnerhet om de utbildningsåtgärder och medvetenhetshöjande åtgärder som dataskyddsombudets kansli har vidtagit; de omfattande insatser dataskyddsombudets kansli har gjort för att förbättra dataskyddet och datasäkerheten, inbegripet för N.SIS; de regelbundna inspektioner som ministeriet för utrikes frågor och internationellt samarbete (*utrikesministeriet*) utför vid ambassader och konsulat samt den inspektion vid externa tjänsteleverantörer som ambassaderna och konsulaten utför på grundval av ett vägledningsdokument från utrikesministeriet; de affischer på flygplatser och polisstationer som genom QR-koder ger enkel tillgång till information om Schengens informationssystem (SIS) på flera språk; den användbara och lättillgängliga informationen om rättigheter för personer registrerade i SIS på den nationella polisens (Polizia di Stato) och dataskyddsmyndighetens webbplatser; det förhållandet att inrikesministeriets webbplats har länkar till Polizia di Statos webbplats, vilket ger registrerade möjlighet att enkelt och snabbt utöva sina rättigheter; det förhållandet att Polizia di Stato upplyser registrerade om att deras personuppgifter inte finns i SIS, samt den användbara och lättillgängliga informationen om rättigheter för personer registrerade i informationssystemet för viseringar (VIS) på dataskyddsmyndighetens webbplats.

(3) Rekommendationer bör lämnas om de åtgärder som Italien bör vidta för att avhjälpa de brister som konstaterats under utvärderingen. Med tanke på vikten av att följa Schengenregelverket i fråga om skydd av personuppgifter, i synnerhet dataskyddsmyndighetens tillsyn samt utbildning i SIS och VIS, bör prioritet ges åt genomförandet av rekommendationerna 4 och 6 i detta beslut.

(4) I enlighet med artikel 15.3 i förordning (EU) nr 1053/2013 bör rådet översända detta beslut till Europaparlamentet och medlemsstaternas nationella parlament.

(5) Rådets förordning (EU) 2022/922[2] är tillämplig sedan den 1 oktober 2022. I enlighet med artikel 31.3 i den förordningen bör uppföljningen och övervakningen av utvärderingsrapporter och rekommendationer, från och med inlämnandet av handlingsplanerna, genomföras i enlighet med den förordningen.

(6) Inom två månader från antagandet av detta beslut bör Italien, i enlighet med artikel 21.1 i förordning (EU) 2022/922, utarbeta en handlingsplan för att genomföra alla rekommendationerna och avhjälpa de brister som konstaterats i utvärderingsrapporten. Italien bör lämna in denna handlingsplan till kommissionen och rådet.

---

[2] Rådets förordning (EU) 2022/922 av den 9 juni 2022 om inrättande och användning av en utvärderings- och övervakningsmekanism för att kontrollera tillämpningen av Schengenregelverket och om upphävande av förordning (EU) nr 1053/2013, EUT L 160, 15.6.2022, s. 1.

HÄRIGENOM REKOMMENDERAS

Italien att göra följande:

**Dataskyddsmyndigheten**

1. Säkerställa att dataskyddsmyndigheten deltar formellt i budgetförfarandet, särskilt att den har ett formellt inflytande på förslaget om myndighetens budget innan förslaget till allmän budget översänds till parlamentet för diskussion och antagande.

2. Säkerställa att dataskyddsmyndigheten tilldelas tillräckligt med personal för att kunna utföra tillsynen över SIS och VIS i god tid och på ett verkningsfullt sätt.

3. Utföra regelbundna inspektioner av vissa myndigheter som är slutanvändare av systemet, t.ex. operativa polismyndigheter, inbegripet regelbundna kontroller och analyser av loggfiler så att dataskyddsmyndigheten kan fullgöra sin uppgift att på ett heltäckande sätt övervaka behandlingen av personuppgifter inom SIS.

4. Slutföra den pågående revisionen av behandlingen av uppgifterna i N.SIS snarast möjligt med hänsyn till covid-19-situationen och säkerställa att efterföljande revisioner utförs inom den föreskrivna fyraårscykeln.

5. Säkerställa att även fler myndigheter som är slutanvändare av VIS-systemet, såsom polis, gränsvakter och invandringsmyndigheter, inspekteras regelbundet så att dataskyddsmyndigheten kan fullgöra sin uppgift att på ett heltäckande sätt övervaka behandlingen av personuppgifter inom VIS.

6. Säkerställa att revisionerna av det nationella viseringssystemet utförs inom den föreskrivna fyraårscykeln.

7. Säkerställa att VIS-revisionerna förutom utrikesministeriets revisionsåtgärder även omfattar inrikesministeriet i egenskap av den andra personuppgiftsansvariga för VIS.

**Schengens informationssystem**

8. Säkerställa att den separata anläggningen i Bari för återställande efter datorhaveri tas i drift.

9. Säkerställa att säkerhetskopian av N.SIS-loggfiler förvaras utanför anläggningen, på en annan geografisk plats än Rom, på ett systematiskt sätt och med en lämpligt kort tidsperiod mellan säkerhetskopieringarna.

10. Säkerställa att operativsystemen på vissa arbetsstationer, såsom Sirenekontoret och den lokala polisstationen vid Commissariato Trevi-Campo Marzio, uppdateras så snart som möjligt.

11. Säkerställa att det för övervakningen av SIS-loggfiler antas riktlinjer med kriterier som är tillämpliga på all övervakningspersonal samt införs en programvarumodul för faktiska analyser av SIS-loggfiler med ett automatiskt varningssystem för ovanliga sökningar för att upptäcka missbruk.

12. Säkerställa en högre säkerhetsstandard för åtkomst till databaser, såsom SIS-applikationen, genom ett system för tvåfaktorsautentisering.

13. Säkerställa att dataskyddsmyndigheten och inrikesministeriet utarbetar en gemensam överenskommelse eller ett gemensamt protokoll om kriterierna eller tröskelvärdet för att anmäla N.SIS-dataintrång till dataskyddsmyndigheten.

14. Ompröva och genomföra grupprincipreglerna för automatisk låsning av datorsystem vid inaktivitet på varje arbetsstation med åtkomst till SIS.

15. Fastställa en säkerhets- och dataskyddsstrategi och övervaka praxisen att i en polisdatabas föra in personuppgifter som registreras vid inkvartering i syfte att se till att man genom regelbunden översyn säkerställer att personuppgifterna, efter det att de bevarats för nödvändiga kontroller under den inledande perioden, lagras i en polisdatabas, inom den maximala lagringsperioden, endast så länge det är nödvändigt och proportionerligt för ändamålen enligt artikel 45 i Schengenkonventionen[3].

**Informationssystemet för viseringar**

16. Fastställa en rimlig gräns för antal misslyckade inloggningsförsök, med hänsyn till skrivfel, förväxling osv., på grundval av vilken användaren bör blockeras av systemet vid försök att åtkomma det nationella informationssystemet för viseringar (N.VIS).

17. Genomföra ytterligare åtgärder för att övervaka behörigheter för åtkomst till N.VIS (utöver att N.VIS-användare omfattas av en strikt och regelbunden översyn av deras åtkomstbehörigheter som görs av det kontor de tillhör) för att säkerställa att översynsprocessen är ändamålsenlig och effektiv, såsom automatiskt upphävande av åtkomstbehörighet efter en lång och avvikande tidsperiod utan någon aktivitet i VIS-systemet.

18. Tillhandahålla en högre säkerhetsnivå genom att kombinera passerkortsavläsningen med införande av en personlig PIN-kod, vid de två RFID-läsare som installerats vid ingången till utrikesministeriets datacentralområde och i viseringsserverrummet.

---

[3] Konvention om tillämpning av Schengenavtalet av den 14 juni 1985 mellan regeringarna i Beneluxstaterna, Förbundsrepubliken Tyskland och Franska republiken om gradvis avskaffande av kontroller vid de gemensamma gränserna (EGT L 239, 22.9.2000).

19. Tillämpa samma policy som redan antagits för annan utrustning i N.VIS-serverrummet även för utrustning i låsta skåp.

20. Införa ett lämpligt säkerhetssystem som kan tillhandahålla autentisering för åtkomst till lokaler och händelsegranskning och vidare förse VIS-systemets backupserverrum med ett brandbekämpningssystem för elektrisk utrustning, i likhet med det som installerats i VIS-serverrummet.

21. Införa en infrastruktur för återställning efter datorhaveri på en annan geografisk plats än Farnesinabyggnaden.

22. Granska de processer för säkerhetskopiering som införts vid ambassader och konsulat, med undvikande av att använda minnespinnar eller, om de används, kryptera den lagrade informationen.

23. Införa automatisk loggkontroll av I-VIS-loggar.

24. Lägga till en modul om skydd av personuppgifter i den interna utbildningskurs före utstationeringen som ges till personal som arbetar med att utfärda viseringar.

25. Säkerställa att utrikesministeriet bedömer kritikaliteterna i de lokala varningsförteckningar som lyfts fram av dataskyddsmyndigheten, inte bara på nationell nivå utan även genom att samarbeta med de andra involverade konsulaten, och i god tid informerar dataskyddsmyndigheten om de åtgärder som kan vidtas för att säkerställa full överensstämmelse med kraven på området skydd av personuppgifter.

26. Förstärka dataskyddsombudets kansli inom utrikesministeriet.

**Allmänhetens medvetenhet och registrerades rättigheter**

27. Säkerställa att informationen om SIS på inrikesministeriets webbplats är begriplig även för personer som inte talar italienska.

28. Säkerställa att det finns standardskrivelser på dataskyddsmyndighetens webbplatser om SIS och att knappen på den aktuella webbplatsen, ”Den nya mekanismen för att utöva dataskyddsrättigheter”, görs synligare.

29. Ändra standardsvaret ”inga inreseförbud gäller för den registrerade på Schengenterritoriet” (nr 6), vilket anses vara vilseledande i fall där den registrerade inte får någon information om registreringen, t.ex. på grund av hot mot den allmänna eller nationella säkerheten.

30. Säkerställa att det på utrikesministeriets och inrikesministeriets webbplatser finns en särskild mall för en begäran om åtkomst till VIS-personuppgifter som rör personuppgifter som behandlats inom VIS.

31. Överväga att lämna information om VIS och registrerades rättigheter vid behandling av personuppgifter inom VIS vid gränsövergångsställen såsom flygplatser, på samma sätt som redan görs för SIS genom till exempel affischer, en QR-kod med länk till ytterligare information osv.

Utfärdat i Bryssel den

*På rådets vägnar*
*Ordförande*