Europeiska unionens råd

Bryssel den 25 januari 2021
(OR. en)

5534/21

Interinstitutionellt ärende:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

LÄGESRAPPORT

från:	Rådets generalsekretariat
till:	Delegationerna
Föreg. dok. nr:	14250/20
Ärende:	Rådets genomförandebeslut om fastställande av en rekommendation om åtgärder för att avhjälpa de brister som konstaterats vid 2019 års utvärdering av **Slovakiens** 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 2019 års utvärdering av Slovakiens tillämpning av Schengenregelverket i fråga om dataskydd, som antogs genom skriftligt förfarande den 21 januari 2021.

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.

Rådets genomförandebeslut om fastställande av en

REKOMMENDATION

om åtgärder för att avhjälpa de brister som konstaterats vid 2019 års utvärdering av Slovakiens 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,

med beaktande av Europeiska kommissionens förslag, och

av följande skäl:

(1) Syftet med detta beslut är att rekommendera åtgärder som Slovakien bör vidta för att avhjälpa de brister som konstaterades under 2019 års Schengenutvärdering i fråga om dataskydd. Efter utvärderingen antogs genom kommissionens genomförandebeslut C(2020) 8160 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 bland annat att dataskyddsmyndigheten sedan den senaste Schengenutvärderingen 2012 har utfört regelbunden tillsyn över SIS II i enlighet med en årlig planering och att ett koncept för SIS II-inspektionerna för de kommande fyra åren har utarbetats; att dataskyddsmyndigheten har genomfört ett betydande antal VIS-inspektioner vid konsulat; dataskyddsmyndighetens och inrikesministeriets insatser för att tillhandahålla information till registrerade med hjälp av elektroniskt och tryckt material; de flerspråkiga versionerna av informationen om Schengenrelaterade ämnen på dataskyddsmyndighetens webbplats och i broschyrerna; att dataskyddsmyndigheten tillhandahåller mallar för begäranden från de registrerade i SIS och VIS; att Sirenekontoret besvarar begäranden inte bara på slovakiska utan även på engelska; att de slovakiska myndigheterna informerar de registrerade om det inte finns några uppgifter om dem i SIS II; den mycket aktiva loggkontroll för VIS och SIS II som utförs av kontrollavdelningen vid inrikesministeriets inspektionsavdelning; den mycket aktiva roll som intas av de två anställda som arbetar med dataskyddsfrågor inom säkerhetsavdelningen vid ministeriet för utrikes frågor och europeiska frågor (*utrikesministeriet*); att utrikesministeriet ordnar med dataskyddsutbildning för personalen, i synnerhet inför tillfällig utstationering för konsulära uppgifter, och att utbildningen ges av säkerhetsavdelningen (i dess roll som dataskyddsombud); att de procedurmässiga och fysiska säkerhetsåtgärder som införts för att skydda SIS II-uppgifter håller hög nivå; den mycket aktiva rollen för dataskyddsombudet och det biträdande dataskyddsombudet i dataskyddsavdelningen vid inrikesministeriets inspektionsavdelning, även när det gäller vägledning och loggkontroll avseende SIS II; samt att inrikesministeriet ordnar med dataskyddsutbildning för alla slutanvändare av N.SIS II.

(3) Med tanke på vikten av att följa Schengenregelverket om dataskydd i samband med VIS, bör prioritet ges åt genomförandet av rekommendationerna 7 och 24.

(4) Detta beslut bör överlämnas till Europaparlamentet och medlemsstaternas parlament. Inom tre månader från beslutets antagande bör Slovakien i enlighet med artikel 16.1 i förordning (EU) nr 1053/2013 utarbeta en handlingsplan som omfattar alla rekommendationer för hur de brister som har konstaterats i utvärderingsrapporten ska avhjälpas och lägga fram den för kommissionen och rådet.

HÄRIGENOM REKOMMENDERAS

att Slovakien bör göra följande:

Dataskyddsmyndigheten

1. Säkerställa att dataskyddsmyndighetens budget och personal ökas ytterligare för att förbättra dess resultat och effektivitet.

2. Säkerställa att det är tydligt vilken del av den allmänna statsbudgeten som anslagits till dataskyddsmyndigheten för att garantera att myndigheten har en separat, offentlig årsbudget.

3. Säkerställa att det nationella rådet i budgetförfarandet görs medvetet om dataskyddsmyndighetens ståndpunkt om sina budgetbehov och budgetdiskussionerna mellan dataskyddsmyndigheten och finansministeriet.

4. Vidta åtgärder så att finansministeriet inte kan göra några kopplingar mellan budgeten och det bötesbelopp som ska uppbäras av dataskyddsmyndigheten, eftersom detta kan påverka karaktären på och prioriteringen av myndighetens arbete och därmed påverka dess oberoende. Det bör garanteras att dataskyddsmyndighetens budget inte kan minskas under kalenderåret i en situation där myndigheten inte har uppburit hela det uppskattade bötesbeloppet.

5. Säkerställa att dataskyddsmyndigheten tilldelas alla uppgifter och befogenheter som anges för dataskyddsmyndigheter i artiklarna 57 och 58 i den allmänna dataskyddsförordningen.

6. Säkerställa att dataskyddsmyndigheten, utöver den regelbundna tillsynsverksamhet som utförs vid N.SIS-kontoret och Sirenekontoret, övervakar fler slutanvändarmyndigheter som har åtkomst till SIS II.

7. Säkerställa att dataskyddsmyndighetens tillsynsverksamhet i fråga om VIS omfattar inspektion av den centrala viseringsmyndigheten med avseende på uppgiftshanteringen i N.VIS. Eftersom tidsfristen för den första granskningen av det nationella viseringssystemet var oktober 2015 bör dataskyddsmyndigheten göra denna del av granskningen, som fortfarande saknas, så snart som möjligt.

8. Säkerställa att dataskyddsmyndigheten regelbundet inspekterar även de externa tjänsteleverantörerna.

Registrerades rättigheter

9. Hitta ett lämpligt sätt för dataskyddsmyndigheten, inrikesministeriet och utrikesministeriet att informera registrerade om de potentiella riskerna med att lämna in kopior av id-kort och känslig information okrypterat på internet. Inrikesministeriet och utrikesministeriet uppmanas att överväga att erbjuda registrerade en säker elektronisk kanal för att lämna in sådana handlingar.

10. Säkerställa att den tidsfrist på 60 dagar för att svara på begäranden från registrerade i SIS II, vilken fastställs i artikel 41.6 i SIS II-förordningen och artikel 58.6 i SIS II-beslutet, iakttas fram till dess att det nya SIS-regelverket[1] blir helt tillämpligt (senast den 28 december 2021), där det finns korshänvisningar till den tidsfrist för att svara på registrerades begäranden som fastställs i den allmänna dataskyddsförordningen (30 dagar med möjlighet till förlängning med ytterligare två månader om så är nödvändigt).

11. Överväga att tillhandahålla en del av den tryckta informationen (broschyrer, skyltar osv.) för registrerade även på polisstationerna för att göra den synlig och lättillgänglig.

12. Överväga att tillhandahålla t.ex. en informell engelsk version av dataskyddsmyndighetens beslut om klagomål avseende begäranden från registrerade i SIS II; detta skulle hjälpa de registrerade att förstå beslutet bättre och därmed stärka de registrerades rättigheter.

13. Säkerställa att informationen om rättigheterna för registrerade i VIS är lättare att hitta på utrikesministeriets webbplats; på webbplatsen bör det också finnas mallar som registrerade i VIS kan använda för att utöva sina rättigheter.

---

[1] Europaparlamentets och rådets förordning (EU) 2018/1862 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU, EUT L 312, 7.12.2018, s. 56 (se i synnerhet artiklarna 66–71); Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller, om ändring av konventionen om tillämpning av Schengenavtalet och om ändring och upphävande av förordning (EG) nr 1987/2006, EUT L 312, 7.12.2018, s. 14 (se i synnerhet artiklarna 51–57).

14. Säkerställa att formuläret för viseringsansökan innehåller tydlig information om de olika myndigheter som behandlar personuppgifter som en del av det nationella viseringssystemet. I synnerhet bör det anges att utrikesministeriet är personuppgiftsansvarig.

15. Tillhandahålla fysisk information (broschyrer, skyltar osv.) för de VIS-registrerade på flygplatserna och andra gränskontrollställen samt göra den synlig och lättillgänglig.

16. Säkerställa att svaren till registrerade avseende personuppgifter i VIS innehåller information om möjligheten att överklaga svaret till dataskyddsmyndigheten och behörig domstol.

17. Vidta nödvändiga åtgärder för att förtydliga utrikesministeriets och den centrala viseringsmyndighetens (inrikesministeriet) ansvar för hanteringen av begäranden från VIS-registrerade och för att ge båda enheterna intern eller metodisk vägledning. Denna information bör vara tillgänglig för de registrerade.

Informationssystemet för viseringar (VIS)

18. Vidta nödvändiga åtgärder för att höja säkerhetsnivån för åtkomst till regeringsmiljön och i synnerhet de nationella viseringsansökningarna vid utrikesministeriet och inrikesministeriet (central viseringsmyndighet), i synnerhet genom åtkomst till de nationella viseringsdatabaserna via multifaktorteknik.

19. Vidta nödvändiga åtgärder för att förbättra den fysiska och organisatoriska säkerheten i utrikesministeriets N.VIS-datacentrum, i synnerhet följande:

    – Tillhandahålla en besökslogg vid ingången till datacentrumet för IKT-personal, besökare och leverantörer vars tillträde bör begränsas.

    – Installera ett brandsläckarsystem med gas (aragonit).

    – Installera vattenläckagedetektion.

    – Säkerställa att golvet är dammfritt och städat.

    – Låsa skyddsstängslet runt EU-servrarna.

20. Påskynda förfarandet med att inrätta ett nytt N.VIS-datacentrum på en annan plats och flytta datacentrumet dit.

21. Överväga att ändra den lokala lagringsperioden för N.VIS-loggfiler vid de diplomatiska och konsulära beskickningarna genom att fastställa en tidsperiod i stället för en mängd MB.

22. Överväga att använda automatiska loggkontrollsystem vid utrikesministeriet.

23. Vidta de åtgärder som krävs för att diplomatiska beskickningar eller utrikesministeriet regelbundet ska inspektera de externa tjänsteleverantörerna.

24. Vidta nödvändiga åtgärder för att mer systematiskt och på ett enhetligt sätt ordna dataskyddsutbildning för den lokala konsulära personalen.

25. Säkerställa att samma information ska ifyllas i den elektroniska viseringsansökan som i pappersformuläret (i enlighet med bilaga I till EU:s viseringskodex[1]).

Schengens informationssystem II

26. Vidta de åtgärder som krävs för att förbättra säkerhetsnivån för åtkomst till N.SIS II, i synnerhet genom att använda multifaktorautentisering och endast https-anslutningar för åtkomst till N.SIS II.

27. Säkerställa att inrikesministeriet informerar dataskyddsmyndigheten om alla dataintrång som sannolikt medför en risk för fysiska personers rättigheter och friheter. Inrikesministeriet bör dessutom upprätta ett register över intrång i personuppgifter.

[1] Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex) (EUT, 15.9.2009, L 243, s. 1).

Allmän kännedom

28. Överväga att lägga ut dataskyddsmyndighetens informationsbroschyrer till de registrerades förfogande även på mer tillgängliga platser, såsom polisstationer, gränskontrollområden och konsulära lokaler.

29. Överväga att göra dataskyddsmyndighetens presentationer, seminarier och öppna evenemang tillgängliga också för allmänheten, i synnerhet registrerade, eftersom de berörs av informationen om SIS II och VIS.

Utfärdat i Bryssel den

På rådets vägnar
Ordförande