Europeiska unionens råd

Bryssel den 17 juni 2022
(OR. en)

10396/22

Interinstitutionellt ärende:
2021/0224(NLE)

SCH-EVAL 83
DATAPROTECT 197
COMIX 324

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	17 juni 2022
till:	Delegationerna
Föreg. dok. nr:	7788/22
Ärende:	Rådets genomförandebeslut om fastställande av en rekommendation om åtgärder för att avhjälpa de brister som konstaterats vid 2020 års utvärdering av **Österrikes** 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 i 2020 års utvärdering av Österrikes tillämpning av Schengenregelverket i fråga om dataskydd, som antogs av rådet vid mötet den 17 juni 2022.

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 2020 års utvärdering av Österrikes 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) En Schengenutvärdering på dataskyddsområdet genomfördes med avseende på Österrike i november 2020. Efter utvärderingen antogs genom kommissionens genomförandebeslut C(2021) 9200 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 exempel på god praxis betraktas särskilt att personalen vid den österrikiska dataskyddsmyndigheten har förstärkts och kommer att fortsätta förstärkas och att budgeten har höjts sedan den senaste utvärderingen, att avtalen mellan personuppgiftsansvariga och personuppgiftsbiträden när det gäller VIS-uppgifter ger ett starkt uppgiftsskydd och säkerställer att alla parter som omfattas av behandlingen av VIS-uppgifter har infört relevanta dataskyddsgarantier, att inrikesministeriet och ministeriet för Europafrågor och internationella frågor (MEIA) utbildar sin personal i uppgiftsskyddsfrågor som rör VIS, att MEIA har en strategi för att granska viseringsförfarandet ur flera olika synvinklar, att den information som dataskyddsmyndigheten tillhandahåller om SIS II och VIS är mycket detaljerad och lättillgänglig, att det finns informationsavsnitt om SIS och VIS på inrikesministeriets webbplats och att inrikesministeriet snabbt besvarar framställningar om åtkomst till SIS II eller VIS.

(3) Rekommendationer bör lämnas om vilka åtgärder Österrike ska vidta för att avhjälpa de brister som konstaterades under utvärderingen. Med tanke på vikten av att följa Schengenregelverket om skydd av personuppgifter bör prioritet ges åt genomförandet av rekommendationerna 1, 6, 7 och 13 i enlighet med detta beslut.

(4) Detta beslut bör överlämnas till Europaparlamentet och medlemsstaternas nationella parlament. Inom tre månader från beslutets antagande bör Österrike 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 Österrike bör göra följande:

Lagstiftning

1. Genomföra artikel 79 i den allmänna dataskyddsförordningen[1] och införliva artikel 54 i direktiv (EU) 2016/680 (LED)[2] i österrikisk nationell lagstiftning i syfte att föreskriva rätten till ett effektivt rättsmedel mot ett beslut som fattats av personuppgiftsansvariga eller personuppgiftsbiträden som är offentliga myndigheter.

Dataskyddsmyndigheten

2. I lag fastställa skälen för entledigande av chefen och biträdande chefen för den österrikiska dataskyddsmyndigheten, för att undvika risken för att deras förordnanden sägs upp i förtid av andra skäl än på grund av allvarlig försummelse eller för att de inte längre uppfyller de villkor som ställs för att de ska kunna fullgöra sitt uppdrag.

3. Säkerställa att den it-expert som nyligen rekryterats av dataskyddsmyndigheten och eventuella ytterligare it-experter är eller kommer att vara mycket väl insatta i Schengens informationssystem II (SIS II) och Informationssystemet för viseringar (VIS) samt i hanteringen av informationssäkerhet, så att dessa experter också kan delta aktivt i tillsynen av SIS och VIS. Dataskyddsmyndigheten bör dessutom fortsätta att anlita externa it-experter i inspektionerna till dess att den kan utföra alla it-relaterade inspektionsuppgifter med sin egen personal.

---

1 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), EUT L 119, 4.5.2016, s. 1.

2 Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, EUT L 119, 4.5.2016, s. 89.

4. Säkerställa att dataskyddsmyndigheten genomför kontrollbesök vid Sirenekontoret, inspektioner av vissa av systemets slutanvändarmyndigheter, såsom polisen, samt regelbundna kontroller och analyser av loggfilerna, för att fullgöra sitt ansvar att på ett heltäckande sätt övervaka behandlingen av personuppgifter i SIS II.

5. Säkerställa att dataskyddsmyndighetens tillsynsverksamhet i samband med VIS även omfattar alla säkerhetsaspekter, inklusive loggar, genom regelbundna kontroller på grundval av analys av loggfiler och att dataskyddsmyndigheten ingående inspekterar serverrummen och även inspekterar vissa andra slutanvändare av VIS-systemet, såsom polisen.

6. Säkerställa att dataskyddsmyndigheten slutför den andra revisionen av N-VIS så snart som covid-19-situationen tillåter detta.

7. Säkerställa att dataskyddsmyndigheten genomför en granskning av uppgiftsbehandlingen i N-VIS minst vart fjärde år.

Schengens informationssystem

8. Säkerställa att all utrustning som ger åtkomst till SIS II-uppgifter använder tvåfaktorsautentisering.

9. Säkerställa att alla dokument från de ledningssystem för informationssäkerhet som finns för båda datacentralerna oftare granskas och att de standarder som används alltid är i linje med den senaste kunskapsnivån.

10. Säkerställa att säkerhetsplanen för SIS II ses över regelbundet och uppdateras vid behov och att säkerhetsåtgärder fastställs för att säkra varaktig stabilitet utöver konfidentialitet, integritet och tillgänglighet, särskilt genom att se till att den personuppgiftsansvariga beaktar den tekniska utvecklingen för att säkerställa att de säkerhetsåtgärder som antas fortsätter att uppfylla dessa mål.

11. Klargöra huruvida den centrala clearingmyndigheten är en integrerad del av inrikesministeriet eller en extern databehandlare.

12. Säkerställa förbättringar när det gäller hanteringen av fall av missbruk av identitet i samband med den information som lämnas till den registrerade och de formulär för samtycke som används, och att de formulär som lämnas till den registrerade innehåller information om registrerades rättigheter, dataskyddsombudets kontaktuppgifter, den rättsliga grunden för behandlingen och information om den period under vilken personuppgifterna kommer att lagras.

Informationssystemet för viseringar

13. Säkerställa att loggar över all uppgiftsbehandling i VIS sparas på nationell nivå i enlighet med artikel 34 i förordning (EG) nr 767/2008 (VIS-förordningen) (under en period av ett år efter den lagringsperiod som avses i artikel 23.1 i VIS-förordningen).

Allmänhetens medvetenhet och de registrerades rättigheter

14. Säkerställa att inrikesministeriet även tillhandahåller andra språkversioner (än tyska), t.ex. engelska, av sin webbplats om behandlingen av SIS II- och VIS-uppgifter och de registrerades rättigheter, och gör informationen på sin webbplats om registrerades rättigheter med avseende på SIS II- och VIS-uppgifter mer lättillgänglig.

15. Säkerställa att inrikesministeriet på sin webbplats tillhandahåller formulär för utövande av rätten till åtkomst, rättelse och radering, både på tyska och på andra språk, t.ex. engelska.

16. Göra pappersversioner av SIS-informationsbroschyrer tillgängliga och lätt åtkomliga hos offentliga myndigheter.

17. Säkerställa att inrikesministeriet, för att stärka de registrerades rättigheter, tillhandahåller en inofficiell översättning, t.ex. till engelska, av svaren till de registrerade.

18. Säkerställa att provinspolisdirektoratens webbplatser ger information om SIS II och VIS, inbegripet om relaterad behandling av personuppgifter, och innehåller länkar till dataskyddsmyndighetens webbplats.

19. Säkerställa att information om behandlingen av personuppgifter i VIS tillhandahålls på ett lättillgängligt sätt på MEIA:s och konsulatens och ambassadernas webbplatser, och att dessa webbplatser innehåller länkar till dataskyddsmyndighetens webbplats.

20. Säkerställa att dataskyddsmyndigheten på sin webbplats (på tyska och engelska) samt i formulären för den registrerades begäran om åtkomst tillhandahåller samma information om den registrerades skyldighet att styrka sin identitet.

21. Säkerställa att dataskyddsmyndigheten på sin webbplats (på tyska och engelska) tillhandahåller särskilda standardformulär för framställningar om rättelse och radering av uppgifter i SIS och VIS.

22. Se till att dataskyddsmyndigheten tillhandahåller information om tidsfristen för att lämna in ett klagomål, i enlighet med artikel 24.4 i dataskyddslagen, på den engelska versionen av sin webbplats.

Utfärdat i Bryssel den

På rådets vägnar
Ordförande