Europeiska unionens råd

Bryssel den 24 september 2019
(OR. en)

12469/19

Interinstitutionellt ärende:
2019/0169(NLE)

SCH-EVAL 158
DATAPROTECT 217
COMIX 428

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	20 september 2019
till:	Delegationerna
Föreg. dok. nr:	11906/1/19 REV 1
Ärende:	Rådets genomförandebeslut om fastställande av en rekommendation om åtgärder för att avhjälpa de brister som konstaterats vid 2018 års utvärdering av **Lettlands** 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 2018 års utvärdering av Lettlands tillämpning av Schengenregelverket i fråga om dataskydd, som antogs av rådet vid mötet den 20 september 2019.

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 2018 års utvärdering av Lettlands 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,

av följande skäl:

(1) Syftet med detta beslut är att rekommendera åtgärder som Lettland bör vidta för att avhjälpa de brister som konstaterades under 2018 års Schengenutvärdering i fråga om dataskydd. Efter utvärderingen antogs genom kommissionens genomförandebeslut C(2019)5720 en rapport som innehåller resultat och bedömningar samt en redogörelse för bästa praxis och brister som konstaterades under utvärderingen.

(2) Som god praxis ses bland annat att finansiering från Europeiska kommissionen har använts på ett framgångsrikt sätt för att öka medvetenheten bland allmänheten och att Sirenekontorets svar finns tillgängliga på olika språk och i allmänhet ges snabbt.

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

(3) Med tanke på vikten av att följa Schengenregelverket om dataskydd i fråga om Schengens informationssystem II (SIS II) bör prioritet ges åt rekommendationerna 15–18.

(4) Med tanke på vikten av att följa Schengenregelverket om dataskydd i fråga om Informationssystemet för viseringar (VIS) bör prioritet ges åt rekommendationerna 9 och 11.

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

HÄRIGENOM REKOMMENDERAS

att Lettland bör göra följande:

Datatillsynsmyndigheten

1. Säkerställa att datatillsynsmyndigheten är fullständigt oberoende genom att anta nationell lagstiftning som är förenlig med kapitel VI i den allmänna dataskyddsförordningen, i synnerhet förfarandet för avsättande av direktören.

2. Säkerställa att datatillsynsmyndigheten får tillräcklig finansiering och en tillräcklig personalstyrka så att den kan fullgöra alla uppgifter som den tilldelats genom regelverket om Schengens informationssystem II (nedan kallat *SIS II*) och Informationssystemet för viseringar (nedan kallat *VIS*).

3. Säkerställa att sådan granskning av behandlingen av uppgifter i N.SIS som krävs enligt artikel 44.2 i SIS II-förordningen och artikel 60.2 i rådets SIS II-beslut utförs i tid.

4. Säkerställa att granskningen av behandlingen av uppgifter i NVIS utförs såsom krävs enligt artikel 41.2 i VIS-förordningen och artikel 8.6 i rådets VIS-beslut.

5. Säkerställa att framtida granskningar av SIS II och VIS är uttömmande och utförs i enlighet med sådana internationella standarder för granskning som krävs enligt regelverket om SIS II och VIS, och säkerställa att nödvändig it-kunskap finns att tillgå vid granskningarna.

6. Säkerställa att datatillsynsmyndighetens tillsynsverksamhet avseende SIS II omfattar regelbundna kontroller av SIS II-registreringar.

7. Säkerställa att datatillsynsmyndighetens tillsynsverksamhet avseende VIS omfattar regelbundna inspektioner av konsulära beskickningar.

8. Säkerställa att datatillsynsmyndighetens fleråriga inspektionsplan omfattar annan inspektionsverksamhet än de obligatoriska granskningarna av SIS II och VIS.

Informationssystemet för viseringar

9. Säkerställa att loggfiler analyseras regelbundet för övervakning av att uppgifterna behandlas på ett lagligt sätt i enlighet med artikel 34.1 och 34.2 i VIS-förordningen.

10. Klargöra utrikesministeriets roll (personuppgiftsbiträde eller gemensam personuppgiftsansvarig) i förhållande till byrån för medborgarskaps- och migrationsfrågor.

11. Säkerställa att byrån för medborgarskaps- och migrationsfrågor oftare utför egenrevision av uppgiftsbehandlingen i VIS.

12. Se över avtalen med externa tjänsteleverantörer för att följa och anpassa dem till kraven i den allmänna dataskyddsförordningen.

13. Tydligt fastställa uppgifter och befogenheter för dataskyddsombudet vid byrån för medborgarskaps- och migrationsfrågor respektive utrikesministeriet.

14. Säkerställa att onlineformulär som används i samband med viseringsansökningar omfattar ett meddelande om dataskydd som informerar registrerade personer om uppgiftsbehandlingen och tillämpliga personliga rättigheter.

Schengens informationssystem

15. Säkerställa att polisen regelbundet utför egenrevision, i synnerhet egenkontroll av loggar.

16. Generera nationella SIS II-loggar på central nivå och säkerställa att skälen till sökningen framgår av loggen.

17. Säkerställa att loggfiler ses över regelbundet för att kontrollera att uppgiftsbehandlingen sker i enlighet med artikel 12.2 i SIS II-förordningen och rådets SIS II-beslut.

18. Minimera säkerhetsriskerna med den mobilapplikation som möjliggör åtkomst till SIS II genom att till exempel att åtkomst endast görs möjlig genom en VPN-tjänst.

19. Införa ett system för tvåfaktorsautentisering.

20. Säkerställa att produktionsuppgifter inte används för testningsändamål och att endast vederbörligen auktoriserade användare kan genomföra sökningar i N.SIS.

21. Tydligt fastställa uppgifter och befogenheter för polisens dataskyddsombud, inbegripet dennes deltagande i intern övervakningsverksamhet, till exempel övervakning av säkerhetsåtgärders effektivitet.

Registrerades rättigheter och informationsverksamhet

22. Tillhandahålla datatillsynsmyndigheten regelbunden statistik över registrerades utövande av sina rättigheter i fråga om SIS II och VIS.

23. Göra mer informationsmaterial, såsom broschyren ”Personuppgifter i Schengens informationssystem”, tillgängligt på flygplatsen och andra offentliga platser.

Utfärdat i Bryssel den

På rådets vägnar
Ordförande