Europeiska unionens råd

Bryssel den 22 februari 2022
(OR. en)

6426/22

Interinstitutionellt ärende:
2021/0392 (NLE)

SCH-EVAL 21
DATAPROTECT 42
COMIX 87

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	21 februari 2022
till:	Delegationerna
Föreg. dok. nr:	5893/22
Ärende:	Rådets genomförandebeslut om fastställande av en rekommendation om åtgärder för att avhjälpa de brister som konstaterats i 2019 års utvärdering av **Polens** 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 2019 års utvärdering av Polens tillämpning av Schengenregelverket i fråga om dataskydd, som antogs av rådet vid mötet den 21 februari 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 i 2019 års utvärdering av Polens 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) I enlighet med förordning (EU) nr 1053/2013 genomfördes under 2019 en utvärdering för att kontrollera tillämpningen av Schengenregelverket i fråga om skydd av personuppgifter i Polen. Efter utvärderingen antogs genom kommissionens genomförandebeslut C(2021)9100 en rapport som innehåller resultat och bedömningar samt en redogörelse för bästa praxis och brister som konstaterades under utvärderingen.

(2) Mot bakgrund av resultaten av utvärderingen bör Polen rekommenderas att vidta vissa åtgärder för att avhjälpa de brister som konstaterats.

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

(3) Som god praxis betraktas särskilt den nationella rättsliga ramen, som gör det möjligt för ordföranden för den polska dataskyddsmyndigheten att självständigt utse sina ställföreträdare samt ledamöterna i den rådgivande nämnden, att kandidaterna till posten som ordförande för dataskyddsmyndigheten måste genomgå en offentlig utfrågning i parlamentet, som också sänds via parlamentets officiella kanal på internet, de täta kontrollerna av externa tjänsteleverantörer, under medverkan av dataskyddsombudet, och de täta kontrollerna av konsulaten, satsningarna på utbildning och kompetensutveckling för slutanvändare av den nationella delen av Schengens informationssystem (N.SIS) och Sirenekontorets personal, bland annat i dataskydd, samt säkerhetsåtgärderna i lokalerna hos såväl de datacentrum som hyser N.SIS som hos det nationella informationssystemet för viseringar (N.VIS).

(4) Mot bakgrund av vikten av att följa Schengenregelverket om skydd av personuppgifter i samband med Informationssystemet för viseringar (VIS) och Schengens informationssystem (SIS) bör prioritet ges åt genomförandet av rekommendationerna 11, 12, 13, 20, 21 och 22 i enlighet med detta beslut.

(5) I enlighet med förordning (EU) nr 1053/2013 bör detta beslut översändas till Europaparlamentet och medlemsstaternas parlament, och Polen bör inom tre månader från beslutets antagande utarbeta en handlingsplan som omfattar alla rekommendationer för att avhjälpa de brister som konstaterats i utvärderingsrapporten och lägga fram den för kommissionen och rådet.

HÄRIGENOM REKOMMENDERAS

att Polen bör göra följande:

Lagstiftning

1. Vid behov uttryckligen förklara tillämpligheten av 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) på behandlingen av personuppgifter i N.VIS och N:SIS.

Dataskyddsmyndigheten

2. Säkerställa att artikel 174 i 2018 års dataskyddslag och artikel 106 i 2018 års lag om skydd av uppgifter inom brottsbekämpningen, där den högsta utgiftsgränsen per år fastställs, inte begränsar den polska dataskyddsmyndighetens budget under de belopp som anslagits i statsbudgeten för ett visst år.

3. Säkerställa att dataskyddsmyndigheten bättre planerar och organiserar sina många inspektioner av N.SIS II för att säkerställa att all behandling av N.SIS II och alla relevanta enheter omfattas och att inspektionerna leder till en omfattande granskning av N.SIS II i enlighet med artikel 44.2 i förordning (EG) nr 1987/2006.

4. Säkerställa att dataskyddsmyndigheten genomför en omfattande inspektion av N.VIS för att fullgöra sina uppgifter i enlighet med artikel 41.2 i förordning (EG) nr 767/2008.

De registrerades rättigheter

5. Säkerställa att dataskyddsmyndighetens statistik om utövandet av de registrerades rättigheter förbättras och gör åtskillnad mellan klagomål och framställningar, vilket system som avses (SIS eller VIS) samt vad framställan gäller och vilken typ av framställan det rör sig om (korrigering, radering, åtkomst).

6. Säkerställa att den personuppgiftsansvariga använder ett mer proaktivt tillvägagångssätt när det gäller att tillhandahålla information om de registrerades rättigheter i samband med VIS-uppgifter.

7. Säkerställa att den personuppgiftsansvariga för SIS och VIS (den nationella polska polisen – central teknisk myndighet för det nationella it-systemet (CTA NITS)) offentliggör standardformulär för framställningar om utövande av de registrerades rättigheter.

Informationssystemet för viseringar (VIS)

8. Säkerställa att registren över åtkomst till VIS även innehåller information om skälen till denna åtkomst.

9. Ompröva förteckningen över myndigheter med åtkomst till VIS och deras åtkomsträttigheter till VIS-uppgifter, med hänsyn till deras befogenheter och användning av sådana uppgifter i praktiken.

10. Mot bakgrund av det stora antalet personuppgiftsansvariga för VIS som inrättats genom nationella lagar och avtalsbestämmelser, och med hänsyn till det stora antalet berörda aktörer, klargöra förhållandet mellan de myndigheter som medverkar i utfärdandet av viseringar och de myndigheter som behandlar VIS-uppgifter, samt dessa myndigheters ansvar för uppgiftsbehandlingen,

11. Säkerställa att sparade VIS-loggfiler tas tillvara på bästa sätt genom att regelbundet underställa dem analyser för att kontrollera dataskyddet.

12. Anta en säkerhetsplan för VIS som omfattar den fysiska säkerheten för den andra datalagringsplatsen samt andra it-säkerhetsaspekter rörande det nationella it-systemet, inbegripet N.VIS-systemet.

13. Anpassa lagringstiden för loggar över ansökningar som rör VIS (särskilt i ansökningar i kategorierna ”Pobyt” och ”ZSE 6”) till tidsfristerna i artikel 34.2 i förordning (EG) nr 767/2008 och artikel 16 i rådets beslut 2008/633/RIF.

Andra generationen av Schengens informationssystem (SIS II)

14. Säkerställa att den personuppgiftsansvariga för N.SIS II inrättar ett centralt system för användaradministration som möjliggör en effektiv egenkontroll utan behov av att konsultera loggar vid de institutioner som är slutanvändare av N.SIS II-systemet.

15. Säkerställa att sparade SIS-loggfiler tas tillvara på bästa sätt genom att regelbundet underställa dem analyser för att kontrollera dataskyddet.

16. Säkerställa automatisk anmälan av it-säkerhetshändelser och den personuppgiftsansvarigas egenkontroll för att förbättra säkerheten ytterligare.

17. Säkerställa att de tekniska åtgärderna även omfattar förhindrande av användningen av USB-enheter eller USB-minnen, genom att alla USB-portar på SIS-arbetsstationer blockeras.

18. Överväga att låta inrikesministeriets dataskyddsombud delta aktivt och regelbundet i övervakningen av behandlingen av SIS- och VIS-uppgifter genom övervakning av logginformation.

19. Säkerställa att den personuppgiftsansvariga för SIS förser dataskyddsmyndigheten med personalprofilerna för alla myndigheter med åtkomst till SIS.

20. Anpassa lagringstiden för loggar i applikationer med åtkomst till SIS-uppgifter i enlighet med artikel 12.4 i förordning (EG) nr 1987/2006 och artikel 12.4 i rådets beslut 2007/533/RIF.

21. Säkerställa att den personuppgiftsansvariga för SIS, i enlighet med artikel 10 i förordning (EG) nr 1987/2006 och artikel 10 i rådets beslut 2007/533/RIF, antar en dataskyddsplan för SIS.

22. Säkerställa att det breda spektrum av institutioner som har tillgång till SIS II-uppgifter ses över för att säkerställa att endast institutioner som med hänsyn till sina befogenheter och praktiska behov behöver det kan få tillgång till uppgifterna,

Allmän kännedom

23. Säkerställa att dataskyddsmyndighetens och polisens webbplatser tillhandahåller information om registrerades rättigheter i samband med VIS-uppgifter.

Utfärdat i Bryssel den

På rådets vägnar
Ordförande