Europeiska unionens råd

Bryssel den 14 maj 2018
(OR. en)

8792/18

Interinstitutionellt ärende:
2018/0051 (NLE)

SCH-EVAL 102
COMIX 244

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	14 maj 2018
till:	Delegationerna
Föreg. dok. nr:	8285/18
Ärende:	Rådets genomförandebeslut om fastställande av en rekommendation om åtgärder för att avhjälpa de brister som konstaterats vid 2017 års utvärdering av **Portugals** tillämpning av Schengenregelverket i fråga om **uppgiftsskydd**

För delegationerna bifogas rådets genomförandebeslut om fastställande av en rekommendation om åtgärder för att avhjälpa de brister som konstaterats vid 2017 års utvärdering av Portugals tillämpning av Schengenregelverket i fråga om uppgiftsskydd, som antogs av rådet vid mötet den 14 maj 2018.

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 2017 års utvärdering av Portugals tillämpning av Schengenregelverket i fråga om uppgiftsskydd

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 vilka åtgärder som Portugal bör vidta för att avhjälpa de brister som konstaterades under 2017 års Schengenutvärdering i fråga om dataskydd. Efter utvärderingen antogs genom kommissionens genomförandebeslut C(2018) 1190 en rapport som innehåller resultat och bedömningar samt en redogörelse för bästa praxis och brister som konstaterades under utvärderingen.

(2) Som god praxis välkomnade expertgruppen att dataskyddsmyndigheten fortlöpande fortbildar sin tekniska personal.

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

(3) Mot bakgrund av vikten av att följa Schengenregelverket, i synnerhet skyldigheten att säkerställa och genomföra en ändamålsenlig tillsyn och se till att nödvändiga säkerhetsåtgärder finns, bör genomförandet av rekommendationerna nr 1, 4, 14, 17 och 22 prioriteras.

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

HÄRIGENOM REKOMMENDERAS

att Portugal bör göra följande:

Tillsynsmyndighet för dataskydd

1. Anslå tillräckliga ekonomiska resurser och personalresurser till dataskyddsmyndigheten, så att den kan fullgöra alla uppgifter som pålagts den i enlighet med regelverket för andra generationen av Schengens informationssystem (nedan kallat *SIS II*) respektive informationssystemet för viseringar (nedan kallat *VIS*), även med tanke på ökade framtida ansvarsområden.

2. Ge dataskyddsmyndigheten ekonomiskt självbestämmande vid genomförandet av myndighetens årliga budget och oberoende i personalrekryteringsfrågor genom att åtminstone anpassa respektive regler till de som är tillämpliga på andra oberoende myndigheter i Portugal, och detta i syfte att bättre säkerställa dataskyddsmyndighetens fulla oberoende.

3. Se till att dataskyddsmyndigheten utan dröjsmål slutför förfarandet för antagande av rapporterna från inspektionen avseende behandlingen av personuppgifter inom SIS II.

4. Se till att dataskyddsmyndigheten utan dröjsmål slutför granskningen av VIS.

Registrerades rättigheter

5. Se till att de registrerade underrättas om sina rättigheter när det gäller SIS II på webbplatsen för Serviço de Estrangeiros e Fronteiras (Gräns- och invandringsverket, nedan kallat *SEF*).

6. Se till att de registrerade, efter begäran att få tillgång till sina personuppgifter, informeras om vilka kategorier av uppgifter som faktiskt behandlas i SIS II.

7. Se till att de registrerade får tydlig information om identiteten på den personuppgiftsansvarige för behandlingen av deras personuppgifter inom ramen för utfärdande av Schengenviseringar.

Informationssystemet för viseringar

8. Klargöra situationen angående kontrollen över behandlingen av personuppgifter i N.VIS (som omfattar tillämpningar som används av både utrikesministeriet och SEF, och tillhörande datacenter) i synnerhet genom att klargöra utrikesministeriets roll och genom att klargöra ansvarsfördelningen mellan SEF och utrikesministeriet.

9. Se till att utrikesministeriet genomför systematisk tillsynsverksamhet som möjliggör en meningsfull bedömning av aspekter som rör en extern tjänsteleverantörs behandling av personuppgifter. I detta hänseende uppmuntras Portugal att utöka det frågeformulär som utrikesministeriet sänder till den externa tjänsteleverantören, så att dataskyddsaspekterna täcks mer ingående och så att utrikesministeriets tillsynsverksamhet förbättras när det gäller dataskydd som utförs av den externa tjänsteleverantören och underleverantören, allt efter omständigheterna.

10. Tillhandahålla ett förfarande som tillåter verifiering av träffar i SIS II under viseringsförfarandet

11. Se till att lösenorden är krypterade för alla N.VIS-användare.

12. Se till att SEF och utrikesministeriet regelbundet analyserar loggfilerna för att säkerställa att uppgiftsskyddet övervakas.

13. Se till att utrikesministeriet regelbundet utför egenkontroll av behandlingen av personuppgifter i RPV och tillhörande datacenter.

14. Se till att utrikesministeriet utan dröjsmål antar en säkerhetsplan för RPV och tillhörande datacenter.

15. Till fullo genomföra rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott och se till att åtkomsten till uppgifter i N.VIS respekterar de krav och det förfarande som fastställts i detta beslut.

16. Se till att ESP raderar sökandes personuppgifter som lagras i dess system enligt tidsfristerna i punkt A d i bilaga X till viseringskodexen, som kräver att sådana uppgifter ska raderas omedelbart när de har sänts till konsulatet.

Schengens informationssystem II

17. Skapa en fullständig säkerhetskopieringsenhet för N.SIS II med samtliga funktioner, inklusive förbindelsen med s-TESTA-kommunikationsinfrastrukturen.

18. Klargöra ansvarsförhållandena mellan de parter som deltar i behandling av uppgifter i N.SIS II, dvs. den personuppgiftsansvarige och myndigheterna med tillgång till SIS.II (användarmyndigheter) i fråga om it-säkerhet, kontroll och egenkontroll rörande detta system, t.ex. genom avtal mellan den personuppgiftsansvarige och de myndigheter som har tillgång till SIS II.

19. Införa en användarhantering som möjliggör ändamålsenlig egenkontroll på grundval av centrala loggar av N.SIS II:s personuppgiftsansvarige utan att loggar hos användarmyndigheterna behöver konsulteras.

20. Se till att SEF regelbundet analyserar loggfilerna för att säkerställa dataskyddsövervakningen.

21. Se till att de it-miljöer som används av användare med långtgående tillgång till eller redigeringsrättigheter i N.SIS II (t.ex. medlemmar av Sirenekontoret) är logiskt eller fysiskt avskilda från internettillgång.

22. Se till att den personuppgiftsansvarige krypterar säkerhetskopierade N.SIS-band och N.SIS-hårddiskar.

23. Se till att användarprofilerna med långtgående tillgång till eller redigeringsrättigheter i N.SIS II (t.ex. medlemmar av Sirenekontoret) är säkrade med en obligatorisk metod för tvåfaktorsautentisering.

24. Se till att SEF förbättrar sin egenkontroll av behandlingen av personuppgifter i N.SIS och regelbundet utför sådana egenkontroller. Portugal uppmanas att anslå tillräckliga ekonomiska resurser och personalresurser till SEF för att säkerställa ändamålsenlig och kontinuerlig egenrevision och it-säkerhet, i synnerhet genom att se till att tjänsten för it-säkerhet i SEF:s informationstekniska avdelning tillsätts.

Information till allmänheten

25. Se till att SEF:s webbplats innehåller lämpliga länkar till dataskyddsmyndighetens webbplats.

Utfärdat i Bryssel den

På rådets vägnar
Ordförande