



Brüssel, den 8. März 2019
(OR. en)

7282/19

Interinstitutionelles Dossier:
2019/0032(NLE)

SCH-EVAL 51
DATAPROTECT 85
COMIX 149

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	7. März 2019
Empfänger:	Delegationen

Nr. Vordok.:	6393/19
--------------	---------

Betr.:	Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2018 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes durch Finnland festgestellten Mängel
--------	---

Die Delegationen erhalten anbei den Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2018 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes durch Finnland festgestellten Mängel, den der Rat auf seiner Tagung vom 7. März 2019 angenommen hat.

Im Einklang mit Artikel 15 Absatz 3 der Verordnung (EU) Nr. 1053/2013 des Rates vom 7. Oktober 2013 wird diese Empfehlung dem Europäischen Parlament und den nationalen Parlamenten übermittelt.

Durchführungsbeschluss des Rates zur Festlegung einer

EMPFEHLUNG

zur Beseitigung der 2018 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes durch Finnland festgestellten Mängel

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 1053/2013 des Rates vom 7. Oktober 2013 zur Einführung eines Evaluierungs- und Überwachungsmechanismus für die Überprüfung der Anwendung des Schengen-Besitzstands und zur Aufhebung des Beschlusses des Exekutivausschusses vom 16. September 1998 bezüglich der Errichtung des Ständigen Ausschusses Schengener Durchführungsübereinkommen¹, insbesondere auf Artikel 15,

auf Vorschlag der Europäischen Kommission,

in Erwägung nachstehender Gründe:

- (1) Gegenstand dieses an Finnland gerichteten Beschlusses ist die Empfehlung von Abhilfemaßnahmen zur Beseitigung der Mängel, die während der 2018 im Bereich des Datenschutzes durchgeführten Schengen-Evaluierung festgestellt worden sind. Nach Abschluss der Evaluierung nahm die Kommission mit dem Durchführungsbeschluss C(2019)290 einen Bericht an, in dem die Ergebnisse und Bewertungen sowie die während der Evaluierung festgestellten bewährten Vorgehensweisen und Mängel aufgeführt sind.

¹ ABl. L 295 vom 6.11.2013, S. 27.

- (2) Zu den bewährten Vorgehensweisen zählen unter anderem die sehr guten Sicherheits- und Notfallmaßnahmen im Datenzentrum in Rovaniemi, die mehrschichtigen Authentifizierungsvorschriften für Polizeibeamte, die spezielle Datenschutzbildung für Polizeibedienstete sowie die Tatsache, dass die Polizei alle Ersuchen betroffener Personen zu Datenschutzfragen unabhängig von der Sprache, in der sie gestellt werden, beantwortet.
- (3) Angesichts der Bedeutung, die der ordnungsgemäßen Anwendung des Schengen-Besitzstands auf dem Gebiet des Datenschutzes in Bezug auf das Schengener Informationssystem II (SIS II) zukommt, sollten die Empfehlungen 16 und 21 vorrangig umgesetzt werden.
- (4) Angesichts der Bedeutung, die der ordnungsgemäßen Anwendung des Schengen-Besitzstands auf dem Gebiet des Datenschutzes in Bezug auf das Visainformationssystem (VIS) zukommt, sollten die Empfehlungen 5 bis 10 vorrangig umgesetzt werden.
- (5) Um Rechtssicherheit zu gewährleisten, ist es ferner wichtig, dass zügig nationale Rechtsvorschriften zur Umsetzung der Datenschutz-Grundverordnung (EU) 2016/679 und der Datenschutzrichtlinie (EU) 2016/680 erlassen werden, u. a. der Gründungsrechtsakt für das Amt des Ombudsmanns für Datenschutz, mit dem dessen vollständige Unabhängigkeit gewährleistet und seine Aufsichtstätigkeit gestärkt wird.
- (6) Dieser Beschluss ist dem Europäischen Parlament und den Parlamenten der Mitgliedstaaten zu übermitteln. Innerhalb von drei Monaten nach dessen Annahme sollte Finnland gemäß Artikel 16 Absatz 1 der Verordnung (EU) Nr. 1053/2013 einen Aktionsplan erstellen, in dem alle Empfehlungen zur Behebung der im Evaluierungsbericht festgestellten Mängel aufgeführt sind, und diesen der Kommission und dem Rat vorlegen —

EMPFIEHLT:

Finnland sollte

Datenschutzaufsichtsbehörde

1. die vollständige Unabhängigkeit des Ombudsmanns für Datenschutz (Datenschutzbehörde – DSB) gewährleisten, indem sichergestellt wird, dass der Leiter/die Leiterin der Behörde vom Ombudsmann selbst und nicht vom Justizministerium ernannt wird;
2. sicherstellen, dass die Aufsichtstätigkeit der DSB in Bezug auf das SIS II regelmäßige Kontrollen von SIS-II-Ausschreibungen umfasst;
3. sicherstellen, dass die Aufsichtstätigkeit der DSB in Bezug auf das VIS regelmäßige Kontrollen von konsularischen Vertretungen umfasst;
4. sicherstellen, dass der mehrjährige Inspektionsplan der DSB neben den obligatorischen Prüfungen des SIS II und des VIS weitere Inspektionstätigkeiten umfasst;

Visa-Informationssystem

5. gewährleisten, dass der externe Dienstleister Daten von Visumantragstellern nur verschlüsselt über ein sicheres VPN übermitteln kann;
6. sicherstellen, dass Daten von Visumantragstellern nicht auf den Servern des externen Dienstleisters gespeichert werden;
7. sicherstellen, dass der externe Dienstleister für die Übermittlung der Daten von Antragstellern aus China und Russland in das Vereinigte Königreich alternative Lösungen bereitstellt;
8. die Datenschutzvereinbarung mit dem externen Dienstleister unterzeichnen und die jeweiligen Zuständigkeiten in Bezug auf das VIS präzisieren, d. h. die Rolle des Außenministeriums als für die Verarbeitung verantwortliche Stelle und die Funktion des externen Dienstleisters als Auftragsverarbeiter;

9. gewährleisten, dass das Außenministerium Logdateien speichert und im Rahmen der Eigenüberwachung (Einhaltung von Datenschutzvorschriften) regelmäßig analysiert, und Verfahren für die regelmäßige Eigenkontrolle/Eigenüberwachung der Verarbeitung personenbezogener Daten in SUVI einführen;
10. gewährleisten, dass das Außenministerium seine Kontrollfunktion in Bezug auf das nationale Visa-Informationssystem wirksam wahrnimmt;
11. außerhalb des Standortes des SUVI-Hauptservers einen Standort für die SUVI-Notfallwiederherstellung einrichten;
12. sicherstellen, dass das Außenministerium ein Verzeichnis der ELVIS-Nutzer führt;
13. sicherstellen, dass die Datenschutzvereinbarung zwischen dem Außenministerium und Tieto den Vorgaben entspricht, die für Vereinbarungen zwischen Verantwortlichen und Auftragsverarbeitern gemäß der Datenschutz-Grundverordnung (EU) 2016/679 gelten;
14. sicherstellen, dass das Außenministerium für seine Mitarbeiter und das Personal von Konsulaten und Botschaften in Bezug auf das VIS spezielle Schulungen zum Thema "Schutz personenbezogener Daten" entwickelt;
15. sicherstellen, dass der Datenschutzbeauftragte des Außenministeriums bei der Verarbeitung personenbezogener Daten und der Fallbearbeitung sowie beim Thema Mitarbeiterschulungen einbezogen wird;

Schengener Informationssystem

16. sicherstellen, dass die Polizei sich einer regelmäßigen Eigenkontrolle unterzieht und insbesondere Logdateien überprüft;
17. die Rolle des Datenschutzbeauftragten klar definieren und sicherstellen, dass er in die Arbeiten zum Thema Datenschutz einbezogen wird, sowie gewährleisten, dass die verschiedenen Datenschutzstellen der Polizei (Datenschutzbeauftragter, Datenschutzgruppe, Datenschutzkoordinatoren und Datenschutz-Kooperationsgruppe) besser zusammenarbeiten;

18. ein integriertes System gewährleisten, das dem Endnutzer bei einer Suchanfrage gleichzeitig nationale und internationale Ausschreibungen anzeigt;
19. sicherstellen, dass Lichtbilder, Fingerabdrücke und andere obligatorische SIS-II-Daten auf sichere Weise in die SIS-II-Ausschreibungen integriert werden;
20. klarstellen, wer innerhalb der Polizei für welche IT-Sicherheitsaufgaben zuständig ist;
21. auf zentraler Ebene nationale SIS-II-Logdateien generieren und sicherstellen, dass der Logdatei der Grund für die Abfrage zu entnehmen ist;

Rechte betroffener Personen und Sensibilisierung

22. alternative Lösungen sicherstellen, damit betroffene Personen ihr Recht auf Zugang, Berichtigung und Löschung von SIS-II-Daten und VIS-Daten wirksam wahrnehmen können;
23. die Gebühr für alle zweiten und nachfolgenden Zugangersuchen, die innerhalb von 12 Monaten gestellt werden, senken, damit die betroffenen Personen ihr Recht auf Zugang zu ihren SIS-II-Daten wirksam wahrnehmen können;
24. betroffenen Personen, die ihre indirekten Zugriffsrechte wahrnehmen wollen, binnen einer Frist antworten, die mit den Schengen-Vorschriften in Einklang steht;
25. sicherstellen, dass ein Musterschreiben zur Verfügung steht, mit dem das Recht auf Berichtigung und Löschung von SIS-II- und VIS-Daten geltend gemacht werden kann;
26. sicherstellen, dass bei der Bearbeitung von Ersuchen betroffener Personen, die ihre Rechte in Bezug auf SIS-II- und VIS-Daten geltend machen, die jeweils zuständigen Datenschutzbeauftragten hinzugezogen werden;
27. sicherstellen, dass Ersuchen betroffener Personen in Bezug auf SIS-II-Daten zentral erfasst werden;
28. der Datenschutzbehörde jährlich Statistiken über die Wahrnehmung der Rechte betroffener Personen in Bezug auf das SIS II übermitteln;

29. betroffene Personen klar darüber informieren, wie sie ihre Rechte gegenüber der Datenschutzbehörde indirekt geltend machen können, wenn ihr Recht aufgrund der bestehenden Rechtsvorschriften eingeschränkt ist;
30. auf der Website der Datenschutzbehörde Informationen zu den Rechten betroffener Personen in Bezug auf das SIS II und das VIS sowie allgemein zum Thema Datenschutz zur Verfügung stellen, auf der Website des Außenministeriums Informationen zu den Rechten betroffener Personen in Bezug auf das VIS bereitstellen, und auf der Website des Außenministeriums und den Websites der Botschaften und konsularischen Vertretungen allgemeine Informationen zum Thema Datenschutz leichter zugänglich machen.

Geschehen zu Brüssel am [...]

Im Namen des Rates

Der Präsident
