



Brüssel, den 13. Oktober 2016
(OR. en)

13128/16

Interinstitutionelles Dossier:
2016/0199 (NLE)

SCH-EVAL 169
COMIX 656

BERATUNGSERGEBNISSE

Absender: Generalsekretariat des Rates

vom 13. Oktober 2016

Empfänger: Delegationen

Nr. Vordok.: 12608/16

Betr.: Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2015 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich Datenschutz durch die Niederlande festgestellten Mängel

Die Delegationen erhalten in der Anlage den Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2015 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich Datenschutz durch die Niederlande festgestellten Mängel, den der Rat auf seiner 3490. Tagung vom 13. Oktober 2016 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 2015 bei der Evaluierung der Anwendung des Schengen-Besitzstands im
Bereich Datenschutz durch die Niederlande festgestellten Mängel**

DER RAT 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 die Niederlande gerichteten Beschlusses ist die Festlegung einer Empfehlung für Maßnahmen zur Beseitigung der Mängel, die während der 2015 im Bereich des Datenschutzes durchgeführten Schengen-Evaluierung festgestellt worden sind. Nach Abschluss der Evaluierung nahm die Kommission mit Durchführungsbeschluss [C(2016)3890] einen Bericht an, in dem die Ergebnisse und Bewertungen sowie bewährte Vorgehensweisen und die während der Evaluierung festgestellten Mängel aufgeführt sind.
- (2) Die Bemühungen des Ministeriums für auswärtige Angelegenheiten (im Folgenden "Außenministerium"), klare und einheitliche Vorschriften für den Schutz personenbezogener Daten externer Dienstleister festzulegen, indem diese Vorschriften in die Rahmenvereinbarung zwischen dem Außenministerium und den externen Dienstleistern aufgenommen werden, wird als gute Praxis betrachtet.

¹ ABl. L 295 vom 6.11.2013, S. 27.

(3) Es ist wichtig, dass jeder festgestellte Mangel so rasch wie möglich behoben wird.

(4) Dieser Beschluss zur Festlegung einer Empfehlung ist dem Europäischen Parlament und den Parlamenten der Mitgliedstaaten zu übermitteln. Innerhalb von sechs Monaten nach Annahme der Empfehlung übermittelt der evaluierte Mitgliedstaat der Kommission gemäß Artikel 16 Absatz 8 der Verordnung (EU) Nr. 1053/2013 seine Bewertung einer möglichen Umsetzung der Empfehlungen, einschließlich Angaben zu etwaigen weiteren Verbesserungen –

EMPFIEHLT:

Die Niederlande sollten

Datenschutzaufsichtsbehörde

1. zur Gewährleistung der vollständigen Unabhängigkeit der niederländischen Datenschutzaufsichtsbehörde ("Data Protection Authority", im Folgenden "DPA") die nationalen Vorschriften abschaffen, nach denen der Minister für Sicherheit und Justiz befugt ist, über die Einstufung von Mitarbeitern des DPA-Sekretariats in höheren Besoldungsgruppen/ auf Führungsebene (ab Stufe 14) zu entscheiden,
2. zur Gewährleistung der vollständigen Unabhängigkeit der DPA die nationalen Vorschriften abschaffen, nach denen der Minister für Sicherheit und Justiz befugt ist, über die wirksame und effiziente Nutzung der DPA-Mittel zu entscheiden,
3. zur Gewährleistung der vollständigen Unabhängigkeit der DPA die nationalen Vorschriften über den DPA-Haushalt dergestalt reformieren, dass das Ministerium für Sicherheit und Justiz keinen Einfluss auf den Vorschlag des jährlichen Haushaltsplans hat, bevor dieser in den allgemeinen Haushaltsvorschlag des Ministeriums für Sicherheit und Justiz eingeflossen ist und dem Parlament zur Annahme übermittelt wurde,
4. sicherstellen, dass die DPA die Rechtmäßigkeit der Verarbeitung personenbezogener Daten im Schengener Informationssystem II (im Folgenden "SIS II"), einschließlich der Kontrolle von Protokolldateien in regelmäßigeren Abständen, überwacht,

5. sicherstellen, dass die DPA die Rechtmäßigkeit der Verarbeitung personenbezogener Daten im Visa-Informationssystem (im Folgenden "VIS"), einschließlich der Kontrolle von Protokolldateien in regelmäßigeren Abständen, überwacht,
6. sicherstellen, dass die DPA die Verantwortung für das Ergebnis des VIS-Audits, das auch im Namen des Außenministeriums vom Ministerium für Sicherheit und Justiz beim ministeriellen Audit-Dienst ("Auditdienst Rijk") angeordnet wurde, übernimmt und die erforderlichen Folgemaßnahmen ergreift. Dazu sollte insbesondere ein zusätzliches Audit sämtlicher Aspekte, die bislang nicht Gegenstand des Audits waren, durch die DPA selbst zählen,
7. sicherstellen, dass jedes künftige VIS-Audit entweder von der DPA selbst durchgeführt oder von der DPA direkt bei einem unabhängigen Datenschutz-Prüfer angefordert wird. Der Prüfer muss unter der Kontrolle und der Verantwortung der DPA bleiben, die deshalb Zweck, Tragweite und Methode des Audits klar definieren, Leitlinien festlegen sowie das Audit und seine endgültigen Ergebnisse überwachen muss;

Rechte betroffener Personen

8. die nationalen Vorschriften über die Frist für die Beantwortung von Zugangsanträgen an die im SIS-II-Rechtsrahmen festgelegte Frist anpassen,
9. weitere Informationen über die Rechte betroffener Personen in Bezug auf SIS II – einschließlich Vorlagen für Schreiben zur Ausübung dieser Rechte – auch auf der englischsprachigen Website der DPA zur Verfügung stellen,
10. Informationen über die Rechte betroffener Personen in Bezug auf SIS II auf der Website der nationalen Polizei zur Verfügung stellen,
11. betroffene Personen über die Risiken der Übermittlung personenbezogener Daten über das offene Internet informieren; die Niederlande sollten die Einrichtung eines sicheren Kanals für die Übermittlung von Ersuchen betroffener Personen um Zugang, Berichtigung und Löschung von Daten über das SIS II in Betracht ziehen und darüber auf den Websites der nationalen Polizei und der DPA informieren,

12. in den den betroffenen Personen zur Verfügung stehenden Informationen (insbesondere im "Schengen-Visum-Antragsformular" und der Broschüre der Einwanderungs- und Einbürgerungsbehörde über "Visa für einen kurzfristigen Aufenthalt in den Niederlanden") klarstellen, an welche Behörde die betroffenen Personen ihre Anträge auf Zugang, Berichtigung und Löschung von Daten im VIS richten sollten und welche Behörde diese Anträge prüfen wird,
13. Informationen über die Rechte betroffener Personen in Bezug auf das VIS, auch auf der englischsprachigen Website der DPA, zur Verfügung stellen;

Visa-Informationssystem

14. die Aufteilung von Aufgaben und Zuständigkeiten zwischen sämtlichen verschiedenen Akteuren im Rahmen der Verfahren für die Visa-Beantragung und -Ausstellung klar definieren und dokumentieren (Außenministerium, Einwanderungs- und Einbürgerungsbehörde, konsularische Vertretungen, regionale Unterstützungsbüros und externe Dienstleister), wenn es um die Verarbeitung personenbezogener Daten über das VIS geht. In der Dokumentation sollte detailliert dargelegt werden, wie das Außenministerium seinen Zuständigkeiten als Kontrollstelle der VIS-Datenverarbeitung nachkommt. Das Außenministerium sollte – in seiner Eigenschaft als Datenverarbeitungs-Kontrollstelle – überlegen, wie nachgeprüft werden kann, dass alle Akteure ihre jeweiligen Zuständigkeiten für die VIS-Datenverarbeitung wahrnehmen,
15. sicherstellen, dass das Außenministerium eine regelmäßige Überprüfung der Rechtmäßigkeit der Datenverarbeitung im VIS auf der Grundlage von Protokollen durchführt;

Schengener Informationssystem

16. sicherstellen, dass die nationale Polizei die Rechtmäßigkeit des Zugangs der Nutzer zu SIS-II-Daten aktiv bewertet und regelmäßig kontrolliert. Die nationale Polizei sollte die Nutzung technischer Hilfsmittel für die Suche und Analyse der NSIS-Protokolle in Erwägung ziehen,
17. in den nationalen Vorschriften klarstellen, dass die NSIS-II-Datensätze spätestens drei Jahre nach ihrer Eintragung gelöscht werden und nur für den Fall, dass sie ein bereits laufendes Kontrollverfahren betreffen, für einen längeren Zeitraum gespeichert werden dürfen. Damit sollte klargestellt werden, dass die nationale Regelung, die eine Speicherfrist von fünf Jahren für Protokolle der nationalen Systeme der nationalen Polizei vorsieht, nicht für NSIS-Datensätze gilt;

Sensibilisierungsmaßnahmen

18. allgemeine Informationen über SIS II und VIS auf der englischsprachigen Website der DPA zur Verfügung stellen,
19. Informationen über SIS II auf der englischsprachigen Website der nationalen Polizei zur Verfügung stellen,
20. leichter zugängliche Informationen über das VIS, die Verarbeitung personenbezogener Daten bei der Visa-Beantragung und -Ausstellung sowie zu den Rechten betroffener Personen auf den Websites des Außenministeriums, der konsularischen Vertretungen, der externen Dienstleister und der Einwanderungs- und Einbürgerungsbehörde zur Verfügung stellen,
21. Links zur Website der DPA auf den Websites der nationalen Polizei, des Außenministeriums, der konsularischen Vertretungen, der externen Dienstleister und der Einwanderungs- und Einbürgerungsbehörde vorsehen.

Geschehen zu Brüssel am

*Im Namen des Rates
Der Präsident*
