Rat der
Europäischen Union

Brüssel, den 8. März 2019
(OR. en)

7278/19

Interinstitutionelles Dossier:
2019/0015(NLE)

SCH-EVAL 49
DATAPROTECT 82
COMIX 146

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
Empfänger:	Delegationen
Nr. Vordok.:	6391/19
Betr.:	Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2017 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des **Datenschutzes** durch **Spanien** festgestellten Mängel

Die Delegationen erhalten in der Anlage den Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2017 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes durch Spanien 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.

ANLAGE

Durchführungsbeschluss des Rates zur Festlegung einer

EMPFEHLUNG

zur Beseitigung der 2017 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes durch Spanien 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 Durchführungsübereinkommen[1], insbesondere auf Artikel 15,

auf Vorschlag der Europäischen Kommission,

in Erwägung nachstehender Gründe:

(1) Gegenstand dieses an Spanien gerichteten Beschlusses ist die Empfehlung von Abhilfemaßnahmen zur Beseitigung der Mängel, die während der 2017 im Bereich des Datenschutzes durchgeführten Schengen-Evaluierung festgestellt worden sind. Nach Abschluss der Evaluierung nahm die Kommission mit dem Durchführungsbeschluss C(2019)280 einen Bericht an, in dem die Ergebnisse und Bewertungen sowie die während der Evaluierung festgestellten Mängel und bewährten Vorgehensweisen aufgeführt sind.

(2) Als bewährte Vorgehensweisen gelten die umfangreichen Aufsichtstätigkeiten des Ministeriums für auswärtige Angelegenheiten und Zusammenarbeit (MAAZ) gegenüber den Konsulaten und dem externen Dienstleister, u. a. in den Bereichen Datensicherheit und Datenschutz, sowie die Eigenkontrolle des MAAZ.

[1] ABl. L 295 vom 6.11.2013, S. 27.

(3) Angesichts der Bedeutung, die der ordnungsgemäßen Anwendung des Schengen-Besitzstands im Bereich des Schutzes personenbezogener Daten im Zusammenhang mit dem SIS II und dem VIS zukommt, sollten die nachstehenden Empfehlungen 20 bis 22, 28, 29 und 34 vorrangig umgesetzt werden.

(4) Dieser Beschluss ist dem Europäischen Parlament und den Parlamenten der Mitgliedstaaten zu übermitteln. Innerhalb von drei Monaten nach dessen Annahme sollte Spanien 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:

Spanien sollte

Datenschutzaufsichtsbehörde

1. zur besseren Gewährleistung der vollständigen Unabhängigkeit der spanischen Datenschutzaufsichtsbehörde ("Agencia Española de Protección de Datos" – AEPD) sicherstellen, dass die AEPD in der Lage ist, ihren Vorschlag für den Haushaltsplan vor dem Parlament zu verteidigen, bevor dieser Vorschlag dem Parlament zur Erörterung und Annahme übermittelt wird;

2. dafür sorgen, dass die AEPD die Rechtmäßigkeit der Verarbeitung von personenbezogenen SIS-II- und VIS-Daten häufiger kontrolliert;

3. hinsichtlich der Überwachung des SIS II sicherstellen, dass der Umfang der Prüfung durch die zuständigen Datenschutzbehörden künftig auch eine Überprüfung der regionalen SIS-II-Nutzer umfasst, und gewährleisten, dass die laufende Prüfung so bald wie möglich abgeschlossen wird und die zuständigen Datenschutzbehörden mindestens alle vier Jahre solche umfassenden Prüfungen durchführen;

4. hinsichtlich der Überwachung des VIS sicherstellen, dass die AEPD die Datenverarbeitungsvorgänge im nationalen VIS mindestens alle vier Jahre überprüft;

5. sicherstellen, dass im Nachgang zu den von den zuständigen Datenschutzbehörden in Bezug auf das SIS II und das VIS durchgeführten Inspektionen verstärkt Folgemaßnahmen ergriffen werden, indem entweder eine konkrete Frist für die Umsetzung der Empfehlungen festgelegt wird oder der für die Verarbeitung Verantwortliche angehalten wird, die zuständigen Datenschutzbehörden binnen einer vorgeschriebenen Frist über die Umsetzung der Empfehlungen zu informieren;

6. dafür sorgen, dass die AEPD das Verfahren für die Annahme der Berichte im Nachgang zur Inspektion der Verarbeitung personenbezogener Daten im SIS II und im VIS unverzüglich abschließt;

Rechte betroffener Personen – SIS II

7. sicherstellen, dass der für die Verarbeitung im SIS II Verantwortliche auf seiner Website einfach zugängliche Informationen über das Verfahren, nach dem betroffene Personen ihre Rechte geltend machen können, sowie die diesbezüglichen Standardformulare bereitstellt. Auf der Website des für die Verarbeitung Verantwortlichen sollte daher ein direkter Link zur AEPD-Website angeboten werden;

8. sicherstellen, dass das SIRENE-Büro bei der Beantwortung von Ersuchen betroffener Personen Informationen über Beschwerdemechanismen bereitstellt;

9. dafür sorgen, dass betroffene Personen ihre Ersuchen und Nachweise auf sichere Weise elektronisch übermitteln können (insbesondere Kopien von Dokumenten, die zu ihrer Identifizierung dienen);

10. schriftlich ein internes Verfahren festlegen, nach welchem Ersuchen betroffener Personen, die ihre Rechte in Bezug auf das SIS II geltend machen, zu bearbeiten sind, um diesbezüglich unterbrechungsfreie Abläufe zu gewährleisten;

11. die AEPD ersuchen, das Standardformular, das betroffene Personen zur Wahrnehmung ihrer Rechte in Bezug auf das SIS II verwenden können, in weiteren Sprachen – wie Englisch und Französisch – leicht zugänglich zu veröffentlichen, und auf der AEPD-Website einen Link zur Website des für die Verarbeitung im SIS II Verantwortlichen einbauen;

Rechte betroffener Personen – VIS

12. die AEPD ersuchen, das Standardformular, das betroffene Personen zur Wahrnehmung ihrer Rechte in Bezug auf das VIS verwenden können, in weiteren Sprachen – wie Englisch und Französisch – leicht zugänglich zu veröffentlichen;

13. gewährleisten, dass das MAAZ auf seiner Website ein Standardformular, das betroffene Personen zur Wahrnehmung ihrer Rechte verwenden können, leicht zugänglich macht und in weiteren Sprachen – wie Englisch und Französisch – bereitstellt. Auf der Website des für die Verarbeitung Verantwortlichen sollte daher ein direkter Link zur AEPD-Website angeboten werden;

14. sicherstellen, dass das MAAZ bei der Beantwortung von Ersuchen betroffener Personen Informationen über Beschwerdemechanismen bereitstellt;

15. für Visa, die von der nationalen Polizei an den Grenzen ausgestellt werden, gewährleisten, dass die nationale Polizei auf ihrer Website einfach zugängliche Informationen über das Verfahren, nach dem betroffene Personen ihre Rechte geltend machen können, sowie die diesbezüglichen Standardformulare bereitstellt. Auf der Website der nationalen Polizei sollte daher ein direkter Link zur AEPD-Website angeboten werden;

16. für Visa, die von der nationalen Polizei an den Grenzen ausgestellt werden, schriftlich ein internes Verfahren festlegen, nach welchem Ersuchen betroffener Personen, die ihre Rechte in Bezug auf das VIS geltend machen, zu bearbeiten sind, um diesbezüglich unterbrechungsfreie Abläufe zu gewährleisten;

17. sicherstellen, dass die betroffenen Personen klare Informationen darüber erhalten, wer im Rahmen der Erteilung von Schengen-Visa für die Verarbeitung ihrer personenbezogenen Daten verantwortlich ist;

Visa-Informationssystem

18. klarstellen, wer für die Verarbeitung von personenbezogenen Daten im N.VIS (u. a. in den Anwendungen, die sowohl vom MAAZ als auch von der nationalen Polizei für an den Grenzen ausgestellte Visa genutzt werden) verantwortlich ist, insbesondere welche Aufgaben die nationale Polizei hat und wie die Aufgabenverteilung für die Verarbeitung personenbezogener Daten zwischen der nationalen Polizei und dem MAAZ geregelt ist;

19. ein formales Verfahren einführen, das im Rahmen des Visumverfahrens die Überprüfung von SIS-II-Treffern ermöglicht;

20. sicherstellen, dass alle N.VIS-Nutzerpasswörter verschlüsselt werden;

21. sicherstellen, dass die Daten auf dem N.VIS-Server und die Datenträger mit den Sicherungskopien verschlüsselt werden;

22. für den VIS-Serverraum jederzeit ein hohes Maß an physischer Sicherheit gewährleisten, insbesondere durch eine ordnungsgemäße Wartung und Reparatur der Sicherheitsvorrichtungen für den Zugang zum Serverraum;

23. den Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten vollständig umsetzen und sicherstellen, dass der Zugang zu den N.VIS-Daten den darin festgelegten Anforderungen und Verfahren entspricht, v. a. indem sichergestellt wird, dass in den Zugangsprotokollen der jeweilige Nutzer, der den Zugang zu VIS-Daten beantragt hat, der genaue Grund für den Zugang und das nationale Aktenzeichen aufgeführt werden;

24. sicherstellen, dass im Einklang mit Artikel 23 der Verordnung (EG) Nr. 767/2008 vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) Daten im N.VIS nicht länger als fünf Jahre gespeichert werden;

25. im Einklang mit den Fristen gemäß Artikel 34 Absatz 2 der VIS-Verordnung und Artikel 16 des VIS-Ratsbeschlusses sicherstellen, dass die Protokolle über die Vorgänge im Zusammenhang mit VIS-Daten in allen für die Verarbeitung von VIS-Daten relevanten Anwendungen (insbesondere SIVICO, AVANCE und ADEXTTRA) nach Ablauf der in Artikel 23 Absatz 1 der VIS-Verordnung genannten Aufbewahrungsfrist höchstens ein Jahr gespeichert werden, und in Bezug auf VIS-Zugangsprotokolle sicherstellen, dass diese nach Ablauf der Aufbewahrungsfrist gemäß Artikel 23 Absatz 1 der VIS-Verordnung ein Jahr lang gespeichert werden;

26. sicherstellen, dass der externe Dienstleister die in seinen Systemen gespeicherten personenbezogenen Daten von Antragstellern im Einklang mit den in Anhang X Teil A Buchstabe d des Visakodexes festgelegten Fristen unmittelbar nach ihrer Übermittlung an das Konsulat löscht;

27. gewährleisten, dass das MAAZ und die nationale Polizei die Protokolle aller Anwendungen, bei denen VIS-Daten vom MAAZ und in ADEXTTRA verarbeitet werden, regelmäßig überprüft, um die datenschutzrechtliche Kontrolle zu gewährleisten;

Schengener Informationssystem II

28. dringend einen vollständigen Backup-Standort einrichten und unverzüglich sicherstellen, dass die Datenträger mit den Sicherungskopien separat aufbewahrt werden;

29. für den Zugang zu Nutzerprofilen mit weitreichenden Zugangs- oder Schreibrechten für N.SIS-II-Daten (SIRENE-Nutzer und Administratoren) zusätzliche Schutzmaßnahmen (Zwei-Faktor-Authentifizierung) vorsehen;

30. die Kontrolle des Zugangs zum SIRENE-Büro verschärfen und sicherstellen, dass nur befugte Polizeibeamte Zugang zu den Gebäuden haben;

31. die Endnutzer regelmäßig und fortlaufend zum Thema "Datenschutz im SIS II" schulen;

32. eine Benutzerverwaltung einrichten, die dem für die Verarbeitung im N.SIS II Verantwortlichen eine wirksame Eigenkontrolle anhand von zentralen Protokollen ermöglicht, ohne dass bei den nutzenden Behörden Protokolle eingesehen werden müssen;

33. gewährleisten, dass der für die Verarbeitung im N.SIS Verantwortliche eine umfassende Sicherheitsstrategie in Bezug auf die SIS-II-Daten sicherstellt, die auch IT-Sicherheitsmaßnahmen für den Zugang zu N.SIS-II-Daten umfasst, einschließlich Kontroll- und Eigenkontrollmaßnahmen oder der Schulung von Behörden, die auf das SIS II zugreifen (nutzende Behörden). Ferner sollte präzisiert werden, wie die Zuständigkeiten der an der Verarbeitung der N.SIS-II-Daten beteiligten Parteien verteilt sind, d. h. welche Aufgaben der für die Verarbeitung Verantwortliche und die nutzenden Behörden im Hinblick auf IT-Sicherheit, Kontrolle und Eigenkontrolle wahrnehmen, beispielsweise indem entsprechende Vereinbarungen zwischen dem für die Verarbeitung Verantwortlichen und den Behörden mit Zugang zum SIS II geschlossen werden;

34. sicherstellen, dass der für die Verarbeitung im SIS II Verantwortliche unverzüglich einen Sicherheitsplan beschließt;

35. sicherstellen, dass der für die Verarbeitung im SIS II Verantwortliche sich regelmäßig einer Eigenkontrolle in Bezug auf die Verarbeitung personenbezogener Daten im N.SIS unterzieht;

36. sicherstellen, dass der für die Verarbeitung im SIS II Verantwortliche die Protokolldateien regelmäßig analysiert, um die datenschutzrechtliche Kontrolle zu gewährleisten;

37. gewährleisten, dass die Protokolle zu Abfragen von N.SIS-Daten gemäß Artikel 12 Absatz 4 der SIS-II-Verordnung und des SIS-II-Ratsbeschlusses nach ihrer Erstellung nicht länger als drei Jahre gespeichert werden.

Geschehen zu Brüssel am […]

Im Namen des Rates
Der Präsident