Rat der
Europäischen Union

Brüssel, den 26. November 2018
(OR. en)

14763/18

Interinstitutionelles Dossier:
2018/0338(NLE)

SCH-EVAL 228
DATAPROTECT 258
COMIX 648

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	26. November 2018
Empfänger:	Delegationen
Nr. Vordok.:	14114/18
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 **Norwegen** festgestellten Mängel

Die Delegationen erhalten anbei 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 Norwegen festgestellten Mängel, den der Rat auf seiner Tagung am 26. November 2018 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 Norwegen 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) Ziel dieses Beschlusses ist es, Norwegen Abhilfemaßnahmen zur Beseitigung der in der Evaluierung von 2017 auf dem Gebiet des Schengen-Besitzstands im Bereich des Datenschutzes festgestellten Mängel zu empfehlen. Nach Abschluss der Evaluierung nahm die Kommission mit dem Durchführungsbeschluss C(2018)4145 einen Bericht an, in dem die Ergebnisse und Beurteilungen sowie bewährte Vorgehensweisen und die während der Evaluierung festgestellten Mängel aufgeführt sind.

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

(2) Als bewährte Praxis gelten u. a. die gut entwickelte Ausbildung für NORVIS-Endnutzer; die Tatsache, dass das Ministerium für Auswärtige Angelegenheiten ("Ministry of Foreign Affairs"/MFA) über ein umfassendes Verfahrensinstrumentarium einschließlich etablierter Checklisten verfügt, um konsularische Vertretungen ("consular posts"/CP) zu beaufsichtigen und CP über Praktiken zur Überwachung externer Dienstleister zu informieren; die umfassenden Bemühungen des Nationalen Kriminalamts ("National Criminal Investigation Service"/NCIS) und der Polizeibezirke auf dem Gebiet der Ausbildung und der Sensibilisierung ihres Personals, einschließlich in Bezug auf Datenschutzfragen; die Tatsache, dass sechs Datenschutzbeauftragte ("Data Protection Officers"/DPO) beim NCIS für sämtliche legalen und praktischen Aspekte des Datenschutzes für das NCIS verantwortlich und in der Organisation sehr aktiv sind; die ähnliche Verpflichtung und proaktive Förderung eines Datenschutzes auf hohem Niveau durch die DPO der Polizeibezirke.

(3) Angesichts der Bedeutung, die der ordnungsgemäßen Anwendung des Schengen-Besitzstands auf dem Gebiet des Datenschutzes für das Schengener Informationssystem II (SIS II) zukommt, sollten die nachstehenden Empfehlungen 8, 22, 27, 28 und 29 vorrangig umgesetzt werden.

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

Norwegen sollte

Aufsichtsbehörde für den Datenschutz

1. zur besseren Gewährleistung der vollständigen Unabhängigkeit der norwegischen Aufsichtsbehörde für den Datenschutz ("Norwegian Data Protection Authority"/DPA) die Bedingungen der *'Instructions on Economy and Operations'* und des *'Grant Letter'* dergestalt abändern, dass sie nicht Gefahr laufen, die Regierung in Bezug auf die DPA direkt oder indirekt zu beeinflussen, was die Unabhängigkeit der DPA gefährden könnte;

2. zur besseren Gewährleistung der vollständigen Unabhängigkeit der DPA informelle Sitzungen des für die DPA Zuständigen mit dem "Ministry of Local Government and Modernisation" ("Ministerium") dergestalt anberaumen, dass sie nicht Gefahr laufen, die Regierung in Bezug auf die DPA direkt oder indirekt zu beeinflussen, was die Unabhängigkeit der DPA gefährden könnte;

3. all jene mit der untergeordneten Position der DPA gegenüber dem König und dem Ministerium verbundenen Bestimmungen aufheben, die zu einer direkten oder indirekten Einflussnahme der Regierung auf die DPA führen und folglich die Unabhängigkeit der DPA gefährden könnten;

4. zur besseren Gewährleistung der vollständigen Unabhängigkeit der DPA das Haushaltsverfahren dergestalt reformieren, dass die DPA einen wirklichen Einfluss auf den Vorschlag für ihren Haushalt hat, bevor der allgemeine Haushaltsvorschlag dem Parlament zur Erörterung und Annahme übermittelt und der Haushaltvorschlag der DPA dem Parlament unterbreitet wird;

5. die Befugnisse der DPA ausbauen, damit die DPA ihre Beschlüsse hinsichtlich der unrechtmäßigen Umsetzung der Verarbeitung personenbezogener Daten durch das Schengener Informationssystem II (SIS II) durchsetzen kann;

6. sicherstellen, dass die DPA die Rechtmäßigkeit der Verarbeitung personenbezogener SIS II-Daten überwacht, einschließlich der regelmäßigeren Analyse von Protokolldateien;

7. sicherstellen, dass die DPA die Rechtmäßigkeit der Verarbeitung personenbezogener Daten des Visa-Informationssystems ("VIS") überwacht, einschließlich der regelmäßigeren Analyse von Protokolldateien;

8. sicherstellen, dass die DPA zumindest alle vier Jahre Audits von Datenverarbeitungen im nationalen VIS-System vornimmt. Da die Frist des ersten Audit (Oktober 2015) nicht eingehalten wurde, sollten baldmöglichst Maßnahmen zur Erfüllung dieser Verpflichtung ergriffen werden;

Rechte Betroffener

9. auf den einschlägigen Websites (insbesondere der DPA und der norwegischen Polizei) klare Informationen über die beiden Möglichkeiten zur Ausübung der Rechte Betroffener von SIS-II-Daten bereitstellen: Ein Betroffener kann entweder einen Antrag beim NCIS stellen (mit der Möglichkeit der Einreichung einer Berufung beim Polizeidirektorat, das nach der Stellungnahme der DPA einen Beschluss fasst) oder der Betroffene kann einen Antrag bei der DPA stellen;

10. die Verpflichtung Betroffener abschaffen, stets eine beglaubigte Kopie ihrer Identitätsurkunde beibringen zu müssen, außer in Fällen, in denen Zweifel an der Identität des Betroffenen bestehen;

11. auf der Website der norwegischen Polizei Informationen über die Frist für die Anträge von von SIS-II-Daten Betroffenen sowie über die Möglichkeit einer Berufung beim Polizeidirektorat und der Adresse für eine solche Berufung bereitstellen;

12. Musterschreiben auf den Websites der DPA, der MFA und der CP bereitstellen, anhand derer vom VIS betroffene Personen ihre Rechte ausüben können;

13. auf der Website der DPA Informationen über die Möglichkeiten der direkten Kontaktaufnahme mit der DPA in Bezug auf VIS-Fragen bereitstellen, einschließlich der Möglichkeit zur Einreichung einer Beschwerde über die Rechte der von einer Bearbeitung von VIS-Daten Betroffenen;

Visa-Informationssystem

14. gewährleisten, dass der Vertrag zwischen der Norwegischen Direktion für Immigration ("UDI") und Sopra Steria (für den Betrieb und die Wartung der IT-Infrastruktur) spezifische Zielvorgaben für Sopra Steria betreffend Routinemaßnahmen zur Wartung des Systems enthält und UDI eine bessere Kontrolle über sämtliche Wartungsmaßnahmen von Sopra Steria sicherstellt;

15. die physische Sicherheit der NORVIS-Serverräume mit der Festlegung umfassender Kriterien verbessern, die gewährleisten, dass Sopra Steria das externe IT-Lieferungs- und Wartungsunternehmen hinreichend kontrolliert, vor allem, was die Sicherheit des Servergehäuses und den Zugang dazu betrifft;

16. die Einrichtung einer NORVIS-Notfallwiederherstellung an einem anderen Ort erwägen;

17. sicherstellen, dass UDI ein Verfahren für eine regelmäßige und aktive Kontrolle der NORVIS-Protokolldateien einführt, einschließlich der Verwaltungsprotokolle;

18. sicherstellen, dass unter Einhaltung der Anforderung nach Artikel 34 der VIS-Verordnung in Bezug auf die Löschung von Protokolldateien (ein Jahr nach Ablauf der Speicherfrist für in VIS eingegebene Daten) ein System (entweder automatisch oder manuell) zur regelmäßigen Löschung der Protokolle geschaffen wird;

19. gewährleisten, dass UDI den Standort für die Aufbewahrung der Backup-Dateien überprüft und sicherstellt, dass sich dieser Ort in einer angemessenen Entfernung von den Datenzentren befindet und regelmäßige Tests zur Wiederherstellung des Systems vorgenommen werden;

20. sicherstellen, dass das IT-Personal der UDI weiterhin spezifisch ausgebildet wird, um besser über die Überwachung des Systems und Maßnahmen externer Unternehmen unterrichtet zu sein;

21. gewährleisten, dass UDI ein strukturierteres und umfassenderes Verfahren für die Überwachung des Verwaltungszugangs zu den NORVIS-Servern, regelmäßige aktive Protokolldateiüberprüfungen, Inspektionen der Datenzentren und allgemein eine aktivere Kontrolle der Tätigkeiten der IT-Verwaltungsunternehmen vornimmt;

22. sicherstellen, dass UDI ihre Maßnahmen in Anbetracht von Artikel 32 der VIS-Verordnung überprüft und wirksame Verfahren für Protokollierungen im Zusammenhang mit dem Zugang zum NORVIS-System einführt; gewährleisten, dass UDI ein wirksames System zur Protokollierung von Datenbankenverwalter-/Verwaltungsmaßnahmen einführt, um so der UDI die Kontrolle und Überwachung von derlei Tätigkeiten zu ermöglichen;

Schengener Informationssystem

23. sicherstellen, dass das NCIS technische Maßnahmen ergreift, um die Verwendung persönlicher USB-Sticks an SIRENE-Computerarbeitsplätzen zu unterbinden;

24. sicherstellen, dass das NCIS technische Maßnahmen ergreift, um den Ausdruck von Dokumenten an SIRENE-Computerarbeitsplätzen zu erfassen;

25. gewährleisten, dass die norwegische Polizei Nutzerprofile schafft, die die Aufgaben und Zuständigkeiten von Personen beschreiben, die für den Zugang, das Einloggen, die Aktualisierung und Löschung sowie die Suche nach SIS-II-Daten (gemäß Artikel 10 Absatz 1 Buchstabe g der SIS-II-Verordnung und Artikel 10 Absatz 1 Buchstabe g des SIS-II-Ratsbeschlusses) zuständig sind. Insbesondere muss gewährleistet werden, dass über das SIRENE-Personal hinaus nur die Polizeimitarbeiter Zugang zu SIS II erhalten, die für ihre Arbeit polizeiliche Überprüfungen durchführen müssen;

26. sicherstellen, dass das SIS-II-Datenzentrum besser gesichert wird und das Verfahren zur Errichtung eines neuen und sicheren Datenzentrums im vierten Quartal 2019 beschleunigt wird;

27. gewährleisten, dass ausländische Dateien im Sinne von Artikel 38 Absatz 2 der SIS-II-Verordnung, in denen keine Angaben gefunden wurden, ein Jahr nach der Löschung der betreffenden Anfrage in SIS II gelöscht werden sollten;

28. sicherstellen, dass gemäß Artikel 12 Absatz 4 der SIS-II-Verordnung und Artikel 12 Absatz 4 des SIS-Ratsbeschlusses SIS-II-Aufzeichnungen frühestens ein Jahr und spätestens drei Jahre nach ihrer Anlage gelöscht werden;

29. gewährleisten, dass die Protokollierungen aller über das "Schengen-formidling" gesandten und übermittelten Mitteilungen (Schaffung, Aktualisierung oder Löschung norwegischer Angaben) gemäß den Anforderungen nach Artikel 12 Absatz 4 der SIS-II-Verordnung und Artikel 12 Absatz 4 des SIS-Ratsbeschlusses in SIS II gelöscht werden;

Sensibilisierung der Öffentlichkeit

30. sicherstellen, dass die Informationen auf der Website der norwegischen Polizei über SIS II, über die Rechte Betroffener und die Zuständigkeit der DPA leichter zu finden sind;

31. erwägen, ob die DPA und die norwegische Polizei nicht gedruckte Informationen über SIS II und über die Rechte Betroffener für die Öffentlichkeit herausgeben sollten;

32. sicherstellen, dass umfassende Informationen für die Öffentlichkeit in Bezug auf die Verarbeitung personenbezogener Daten im VIS und über die Rechte Betroffener auf den Websites der DPA, MFA und konsularischen Vertretungen bereitgestellt werden;

33. erwägen, ob die DPA und die CPs nicht gedruckte Informationen über VIS und über die Rechte Betroffener für die Öffentlichkeit herausgeben sollten.

Geschehen zu Brüssel am […]

Für den Rat
Der Präsident