Rat der
Europäischen Union

Brüssel, den 24. September 2019
(OR. en)

12468/19

Interinstitutionelles Dossier:
2019/0168(NLE)

SCH-EVAL 157
DATAPROTECT 216
COMIX 427

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	20. September 2019
Empfänger:	Delegationen
Nr. Vordok.:	11904/19
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 **Litauen** festgestellten Mängel

Die Delegationen erhalten in der Anlage 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 Litauen festgestellten Mängel, den der Rat auf seiner Tagung vom 20. September 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 Litauen 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 Litauen 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) 5700 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 zählt unter anderem Folgendes: die Tatsache, dass die Datenschutzbehörde (DSB) Personen, die sich an sie wenden, berät und unterstützt, statt Anfragen einfach weiterzuleiten; die Bereitstellung von Musterschreiben für die Wahrnehmung der Rechte betroffener Personen in Bezug auf das Schengener Informationssystem II (SIS II) und das Visa-Informationssystem (VIS); die in den Räumlichkeiten der Abteilung für Informationstechnologie und Kommunikation des Innenministeriums (ITCD, wo das N.VIS und das N.SIS gehostet werden) getroffenen Sicherheitsmaßnahmen, die grundsätzlich hohen Standards entsprechen und eine sichere Umgebung für die Speicherung von Daten und die Verhinderung etwaiger Zwischenfälle gewährleisten; die guten Schulungen für VIS-Endnutzer, insbesondere für konsularische Mitarbeiter vor ihrer Entsendung in Botschaften/Konsulate; die Tatsache, dass dem Thema Schulung und Personalentwicklung ein hoher Stellenwert beigemessen wird und insbesondere gute Fortbildungen u. a. zum Datenschutz für N.SIS-Endnutzer und die Mitarbeiter des SIRENE-Büros angeboten werden; die ausführlichen, nützlichen und leicht verständlichen (in mehreren Sprachen abrufbaren) Informationen zum SIS II und VIS auf der Website der DSB; die Broschüren der DSB über den "Schutz personenbezogener Daten im Schengener Informationssystem" und den "Schutz personenbezogener Daten im Visa-Informationssystem", die sehr gute und einfach verständliche Informationen über die Verarbeitung von Daten in beiden Datenbanken und die damit verbundenen Rechte betroffener Personen bieten, sowie die intensive Mitwirkung der DSB an zahlreichen Sensibilisierungsmaßnahmen (Konferenzen, Schulungen und anderen Veranstaltungen), die sich unter anderem an das mit der Datenverarbeitung im SIS II und VIS befasste Personal richten.

(3) Angesichts der Bedeutung, die der ordnungsgemäßen Anwendung der Schengen-Vorschriften zum Datenschutz zukommt, insbesondere in Bezug auf die Gewährleistung der vollständigen Unabhängigkeit der DSB, sollte die Empfehlung 1 vorrangig umgesetzt werden.

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

Litauen sollte

Datenschutzaufsichtsbehörde

1. zur besseren Gewährleistung der vollständigen Unabhängigkeit der staatlichen Datenschutzbehörde (im Folgenden "DSB") die Vorgabe abschaffen, dass der Justizminister den strategischen Aktionsplan der DSB genehmigen muss und dass er zum jährlichen Aktionsplan konsultiert werden muss, bevor der Direktor der DSB diesen genehmigen kann; dies ist auch wichtig, damit sichergestellt ist, dass das Haushaltsverfahren in keinerlei Hinsicht die Unabhängigkeit der DSB gefährdet;

2. zur besseren Gewährleistung der vollständigen Unabhängigkeit der DSB die regelmäßigen bilateralen Treffen zwischen dem Justizminister und dem Direktor der DSB so gestalten, dass kein Risiko einer direkten oder indirekten Einflussnahme der Regierung auf die DSB besteht, die die Unabhängigkeit der DSB gefährden könnte;

3. alle Aspekte der Rechenschaftspflicht des Direktors der DSB gegenüber der Regierung und dem Justizminister beseitigen, die zu einer direkten oder indirekten Einflussnahme durch die Regierung und den Justizminister führen und die Unabhängigkeit der DSB beeinträchtigen könnten;

4. sicherstellen, dass die DSB die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten im SIS II häufiger kontrolliert;

5. sicherstellen, dass die DSB die Datenverarbeitungsvorgänge im N.SIS mindestens alle vier Jahre überprüft;

6. sicherstellen, dass die DSB die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten im VIS kontrolliert. Im Zuge der Inspektion der Botschaften sollte die DSB auch bei den externen Dienstleistern die Datenverarbeitungsvorgänge sowie die Gewährleistung der Datensicherheit überprüfen; diese Möglichkeit sollte im Vertrag zwischen dem Außenministerium und den jeweiligen externen Dienstleistern festgehalten werden;

7. sicherstellen, dass die DSB die Datenverarbeitungsvorgänge im N.VIS mindestens alle vier Jahre überprüft;

Rechte betroffener Personen

8. sicherstellen, dass die 60-Tage-Frist für die Beantwortung von Anträgen der von der Datenverarbeitung im SIS II betroffenen Personen gemäß Artikel 41 Absatz 6 der SIS-II-Verordnung und Artikel 58 Absatz 6 des SIS-II-Beschlusses eingehalten wird, bis die neuen SIS-Rechtsvorschriften[2] in vollem Umfang anwendbar werden (spätestens am 28. Dezember 2021), in denen auf die in der Datenschutz-Grundverordnung (DSGVO)[3] festgelegte Frist für die Beantwortung von Anträgen betroffener Personen (30 Tage mit der Möglichkeit einer Verlängerung um zwei weitere Monate, sofern dies erforderlich ist) verwiesen wird;

9. die internen Verfahren in Bezug auf die Zuständigkeit der beteiligten Behörden für die Rechte der von der Datenverarbeitung im SIS II betroffenen Personen klären, u. a. damit das Personal weiß, an wen die jeweiligen Anträge weiterzuleiten sind;

---

[2] Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56, siehe insbesondere Artikel 66 bis 71); Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006 (ABl. L 312 vom 7.12.2018, S. 14, siehe insbesondere Artikel 51-57).

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

10. sicherstellen, dass das Innenministerium die Antworten an Personen, die ihre Rechte als betroffene Personen in Bezug auf das SIS II geltend machen möchten, kohärent gestaltet und die Betreffenden über ihr Recht auf Einlegung eines Rechtsbehelfs bei der DSB sowie bei Gericht unterrichtet;

11. die internen Verfahren in Bezug auf die Zuständigkeit der beteiligten Behörden für die Rechte der von der Datenverarbeitung im VIS betroffenen Personen klären, u. a. damit das Personal weiß, an wen die jeweiligen Anträge weiterzuleiten sind;

12. sicherstellen, dass das Innenministerium die Antworten an Personen, die ihre Rechte als betroffene Personen in Bezug auf das VIS geltend machen möchten, kohärent gestaltet und die Betreffenden über ihr Recht auf Einlegung eines Rechtsbehelfs bei der DSB sowie bei Gericht unterrichtet;

Visa-Informationssystem

13. sicherstellen, dass in den Verträgen zwischen dem Außenministerium und externen Dienstleistern festgelegt ist, in welcher Form die litauische DSB in die von den Botschaften/Konsulaten und dem Außenministerium durchgeführten Inspektionen einbezogen werden kann;

14. zur Gewährleistung einer besseren Eigenkontrolle die Protokolldateien regelmäßig proaktiv überprüfen, um die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten im VIS zu überwachen; sicherstellen, dass das Innenministerium das System SIEM für die automatische Protokollkontrolle weiterentwickelt;

15. sicherstellen, dass der Datenschutzbeauftragte des Außenministeriums stärker in die Konzeption und Veranstaltung von Datenschutzschulungen für Mitarbeiter des Außenministeriums (einschließlich der an Botschaften/Konsulate entsandten Mitarbeiter) einbezogen wird;

Schengener Informationssystem II

16. dafür sorgen, dass sich Endnutzer künftig nicht mehr mit mehreren Geräten gleichzeitig über den POLIS-Browser in das N.SIS einloggen können;

17. für den Zugang zu den Workstations der N.SIS-Nutzer bei der Polizei Smartcards einführen, um das Sicherheitsniveau und den Sicherheitsstandard zu erhöhen;

18. sicherstellen, dass die technischen Maßnahmen, mit denen die Nutzung von USB-Sticks an den Workstations der SIRENE-Büros verhindert werden soll, vollständig umgesetzt und in regelmäßigen Abständen kontrolliert werden;

19. zur Gewährleistung einer besseren Eigenkontrolle die Protokolldateien von SIS-II-Endnutzern aller betroffenen Behörden regelmäßig proaktiv überprüfen, um die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten im SIS II zu überwachen; sicherstellen, dass das Innenministerium das System SIEM für die automatische Protokollkontrolle weiterentwickelt;

20. gewährleisten, dass das Personal im Rahmen regelmäßiger Auffrischungskurse noch stärker für das Thema Datenschutz in Bezug auf die Verarbeitung von SIS-II- und VIS-Daten sensibilisiert wird;

21. sicherstellen, dass die Schulung und Sensibilisierung von Mitarbeitern mit Zugang zum N.SIS ein Bereich ist, für den die Gruppe der Datenschutzbeauftragten im Innenministerium federführend zuständig ist; damit könnte eine durchgängige Struktur und Planung im Rahmen der Personalentwicklung sichergestellt werden;

Sensibilisierung der Öffentlichkeit

22. gewährleisten, dass die Links auf der DSB-Website in Bezug auf das SIS II und VIS regelmäßig aktualisiert werden;

23. sicherstellen, dass die Websites von Organisationen, die Kontakte mit Staatsangehörigen anderer Länder haben – beispielsweise das Innenministerium, die Polizei, die staatliche Grenzschutzbehörde, das Außenministerium und Konsularstellen – einfach verständliche und klare Informationen zum SIS II und zum VIS sowie zu den damit verbundenen Rechten der betroffenen Personen auch in englischer Sprache bieten;

24. sicherstellen, dass englischsprachige Informationen zum SIS II und zum VIS sowie zu den Rechten der betroffenen Personen auf den betreffenden Websites leichter zu finden sind;

25. dafür sorgen, dass die Informationen zur Wahrnehmung der Rechte betroffener Personen in Bezug auf das N.SIS II und das VIS auf den Websites der Einrichtungen, die mit diesen Systemen arbeiten, kohärent sind;

26. auf dem EPM-Portal (Electronic Application Module), über das die betreffenden Personen Angaben zu Visumanträgen machen, Informationen zur Verarbeitung der Daten sowie zu den Rechten betroffener Personen in Bezug auf das VIS bereitstellen.

Geschehen zu Brüssel am […]

Im Namen des Rates
Der Präsident