Rat der
Europäischen Union

Brüssel, den 25. Januar 2021
(OR. en)

5534/21

Interinstitutionelles Dossier:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
Empfänger:	Delegationen
Nr. Vordok.:	14250/20
Betr.:	Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2019 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des **Datenschutzes** durch die **Slowakei** festgestellten Mängel

Die Delegationen erhalten in der Anlage den Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2019 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes durch die Slowakei festgestellten Mängel, der am 21. Januar 2021 im schriftlichen Verfahren angenommen wurde.

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 2019 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes durch die Slowakei 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 die Slowakische Republik gerichteten Beschlusses ist die Empfehlung von Abhilfemaßnahmen zur Beseitigung der Mängel, die während der 2019 im Bereich des Datenschutzes durchgeführten Schengen-Evaluierung festgestellt wurden. Nach Abschluss der Evaluierung nahm die Kommission mit dem Durchführungsbeschluss C(2020) 8160 einen Bericht an, in dem die Ergebnisse und Bewertungen sowie bewährte Vorgehensweisen und die während der Evaluierung festgestellten Mängel aufgeführt sind.

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

(2) Zu den bewährten Vorgehensweisen zählen unter anderem die Tatsache, dass die Datenschutzbehörde (DSB) seit der letzten Schengen-Evaluierung im Jahr 2012 entsprechend einer jährlichen Planung regelmäßig Aufsichtstätigkeiten in Bezug auf das SIS II durchgeführt hat und dass ein Konzept für die SIS-II-Inspektionen in den nächsten vier Jahren ausgearbeitet wurde, die Durchführung einer Vielzahl von VIS-Inspektionen in Konsulaten durch die DSB, die Bemühungen der DSB und des Innenministeriums, den betroffenen Personen Informationen in elektronischer und gedruckter Form zur Verfügung zu stellen, die mehrsprachigen Fassungen der Informationen zu Schengen-bezogenen Themen auf der Website und in den Faltblättern der DSB, die Bereitstellung von Vorlagen für Anträge für die von der Datenverarbeitung im SIS und VIS betroffenen Personen durch die DSB, die Tatsache, dass das SIRENE-Büro Anträge nicht nur in slowakischer Sprache, sondern auch auf Englisch beantwortet, die Unterrichtung der betroffenen Personen durch die slowakischen Behörden, wenn keine Daten über sie im SIS II gespeichert sind, die sehr aktive Kontrolle der VIS- und SIS-II-Protokolle durch die Inspektionsabteilung des Inspektionsdienstes des Innenministeriums, die sehr aktive Rolle der beiden Mitarbeiter in der Sicherheitsabteilung des Ministeriums für auswärtige und europäische Angelegenheiten (MAEA), die mit Datenschutzfragen befasst sind, die Tatsache, dass das MAEA seinen Mitarbeitern Datenschutzschulungen anbietet, insbesondere vor der befristeten Betrauung mit konsularischen Aufgaben, und dass die Sicherheitsabteilung in ihrer Funktion als Büro des Datenschutzbeauftragten diese Schulungen durchführt, das hohe Niveau der verfahrenstechnischen und physischen Sicherheit für den Schutz von SIS-II-Daten, die sehr aktive Rolle des Datenschutzbeauftragten und des stellvertretenden Datenschutzbeauftragten in der Datenschutzabteilung des Inspektionsreferats des Inspektionsdienstes des Innenministeriums, u. a. hinsichtlich Anleitungen und Protokollkontrolle in Bezug auf das SIS II und die Bereitstellung von Datenschutzschulungen für alle N.SIS-II-Endnutzer durch das Innenministerium.

(3) Angesichts der Bedeutung, die der ordnungsgemäßen Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes in Bezug auf das VIS zukommt, sollten die Empfehlungen 7 und 24 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 die Slowakische Republik 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:

Die Slowakische Republik sollte

Datenschutzbehörde

1. sicherstellen, dass der Haushalt und das Personal der DSB weiter aufgestockt werden, um die Leistung und Effizienz der DSB zu steigern;

2. dafür sorgen, dass der für die DSB vorgesehene Teil des gesamten Staatshaushalts klar erkennbar ist, damit gewährleistet ist, dass die DSB über ein separates öffentliches Jahresbudget verfügt;

3. sicherstellen, dass der Nationalrat im Rahmen des Haushaltsverfahrens über den Standpunkt der DSB zu ihrem Mittelbedarf sowie über die Haushaltsberatungen zwischen der DSB und dem Finanzministerium informiert wird;

4. Maßnahmen ergreifen, damit das Finanzministerium keine Korrelation zwischen dem Haushalt und der Höhe der von der DSB einzuziehenden Geldbußen herstellen kann, da dies Auswirkungen auf die Art und die Priorisierung der Arbeit der DSB haben und somit deren Unabhängigkeit beeinträchtigen könnte. Es sollte gewährleistet sein, dass die Haushaltsmittel der DSB während des Kalenderjahres nicht gekürzt werden können, wenn die veranschlagten Geldbußen nicht vollständig von der DSB eingezogen wurden.

5. sicherstellen, dass der DSB alle Aufgaben und Befugnisse gemäß den Artikeln 57 und 58 der Datenschutz-Grundverordnung (DSGVO) übertragen werden;

6. sicherstellen, dass die DSB zusätzlich zu den regelmäßigen Aufsichtsmaßnahmen in der N.SIS-Stelle und im SIRENE-Büro mehr Endnutzerbehörden kontrolliert, die Zugang zum SIS II haben;

7. dafür sorgen, dass die DSB im Rahmen ihrer Aufsicht in Bezug auf das VIS auch Inspektionen bei der zentralen Visumbehörde hinsichtlich der Datenverarbeitungsvorgänge im N.VIS durchführt. Da die Frist für die erste Revision des nationalen Visasystems im Oktober 2015 endete, sollte die DSB den noch ausstehenden Teil der Revision so bald wie möglich durchführen;

8. sicherstellen, dass die DSB auch die externen Dienstleister regelmäßig kontrolliert;

Rechte der betroffenen Personen

9. ermitteln, wie die DSB, das Innenministerium und das MAEA die betroffenen Personen angemessen über die potenziellen Risiken informieren können, die mit der Übermittlung von Kopien von Personalausweisen und sensiblen Informationen über das offene Internet verbunden sind. Das Innenministerium und das MAEA werden ersucht zu erwägen, den betroffenen Personen einen gesicherten elektronischen Übertragungsweg für die Übermittlung solcher Dokumente zur Verfügung zu stellen;

10. 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[1] (spätestens am 28. Dezember 2021) in vollem Umfang anwendbar werden, in denen auf die in der DSGVO festgelegte Frist für die Beantwortung von Anträgen betroffener Personen (30 Tage mit der Möglichkeit einer Verlängerung um weitere zwei Monate, sofern dies erforderlich ist) verwiesen wird;

11. erwägen, einige der gedruckten Informationen (Faltblätter/Informationstafeln usw.) für die betroffenen Personen in den Polizeidienststellen bereitzustellen, und zwar gut sichtbar und leicht zugänglich;

12. erwägen, beispielsweise eine informelle englische Fassung der Entscheidungen der DSB über Beschwerden im Zusammenhang mit Anträgen der von der Datenverarbeitung im SIS II betroffenen Personen bereitzustellen; dies würde dazu beitragen, dass die betroffenen Personen die Entscheidungen besser verstehen, und somit die Rechte dieser Personen stärken;

13. sicherstellen, dass die Informationen über die Rechte der von der Datenverarbeitung im VIS betroffenen Personen auf der Website des MAEA leichter zu finden sind; die Website sollte auch Vorlagen für die Ausübung der Rechte der von der Datenverarbeitung im VIS betroffenen Personen enthalten;

---

[1] 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 bis 57).

14. dafür sorgen, dass das Visumantragsformular klare Informationen über die verschiedenen Behörden enthält, die personenbezogene Daten im Rahmen des nationalen Visasystems verarbeiten; insbesondere sollte darauf hingewiesen werden, dass das MAEA als Verantwortlicher gilt;

15. physische Informationen (Faltblätter/Informationstafeln usw.) für die von der Datenverarbeitung im VIS betroffenen Personen an Flughäfen und sonstigen Grenzkontrollstellen bereitstellen, und zwar gut sichtbar und leicht zugänglich;

16. sicherstellen, dass in den Antworten an betroffene Personen, in denen es um personenbezogene VIS-Daten geht, darauf hingewiesen wird, dass bei der DSB und dem zuständigen Gericht ein Rechtsbehelf gegen eine Antwort eingelegt werden kann;

17. die erforderlichen Maßnahmen ergreifen, um die Zuständigkeiten des MAEA und der zentralen Visumbehörde (Innenministerium) für die Bearbeitung von Anträgen der von der Datenverarbeitung im VIS betroffenen Personen zu präzisieren und für beide Stellen interne oder methodische Leitlinien zu erstellen; diese Informationen sollten den betroffenen Personen zur Verfügung stehen;

Visa-Informationssystem

18. die erforderlichen Maßnahmen ergreifen, um das Sicherheitsniveau für den Zugang zur Verwaltungsumgebung und insbesondere zu den im MAEA und bei der zentralen Visumbehörde (Innenministerium) erfassten Anträgen auf nationale Visa zu erhöhen, insbesondere durch Zugang zu den nationalen Visa-Datenbanken über die Multi-Faktor-Technologie;

19. die erforderlichen Maßnahmen ergreifen, um die physische und organisatorische Sicherheit im N.VIS-Rechenzentrum des MAEA insbesondere in Bezug auf folgende Aspekte zu erhöhen:

    – Bereitstellung eines Besucherlogbuchs am Eingang des Rechenzentrums zur Erfassung von IKT-Mitarbeitern, Besuchern oder Lieferanten, deren Zugang beschränkt sein sollte,

    – Installation einer Feuerlöschanlage mit Gas (Argonite),

    – Installation eines Wasserleck-Meldesystems,

    – Gewährleistung eines staubfreien und aufgeräumten Bodens,

    – Verriegelung des Schutzzauns für die EU-Server;

20. das Verfahren zur Einrichtung eines neuen N.VIS-Rechenzentrums an einem anderen Ort und den Umzug des Rechenzentrums beschleunigen;

21. erwägen, die lokale Aufbewahrungsfrist für die N.VIS-Protokolldateien in den diplomatischen Missionen und konsularischen Vertretungen zu ändern, indem anstelle der MB-Menge ein Zeitraum festgelegt wird;

22. erwägen, im MAEA Systeme für die automatische Protokollkontrolle zu verwenden;

23. die erforderlichen Maßnahmen ergreifen, damit die diplomatischen Missionen oder das MAEA die externen Dienstleister regelmäßig kontrollieren;

24. die erforderlichen Maßnahmen ergreifen, um die örtlichen Konsularbediensteten systematischer und einheitlich in Datenschutzfragen zu schulen;

25. sicherstellen, dass mit dem elektronischen Visumantrag dieselben Daten erhoben werden wie mit dem Antragsformular in Papierform (siehe Anhang I des EU-Visakodexes[1]);

Schengener Informationssystem II

26. die erforderlichen Maßnahmen ergreifen, um das Sicherheitsniveau für den Zugang zum N.SIS II zu erhöhen, insbesondere durch die Multi-Faktor-Authentifizierung und die ausschließliche Verwendung von HTTPS-Verbindungen für den Zugang zum N.SIS II;

27. sicherstellen, dass das Innenministerium die DSB über jede Datenschutzverletzung unterrichtet, die voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Darüber hinaus sollte das Innenministerium ein Register der Verletzungen des Schutzes personenbezogener Daten einrichten;

---

1 Verordnung (EG) Nr. 810/2009 des Europäischen Parlaments und des Rates vom 13. Juli 2009 über einen Visakodex der Gemeinschaft (Visakodex). ABl. L 243 vom 15.9.2009, S. 1.

Sensibilisierung der Öffentlichkeit

28. erwägen, die DSB-Faltblätter den betroffenen Personen auch an besser zugänglichen Orten wie Polizeidienststellen, Grenzkontrollbereichen und konsularischen Räumlichkeiten zur Verfügung zu stellen;

29. erwägen, DSB-Präsentationen, -Seminare und -Veranstaltungen im Rahmen von Tagen der offenen Tür auch der breiten Öffentlichkeit zugänglich zu machen, insbesondere betroffenen Personen, da für sie die Informationen über das SIS II und das VIS von Belang sind.

Geschehen zu Brüssel am […]

Im Namen des Rates
Der Präsident