



Brüssel, den 2. Dezember 2020
(OR. en)

13588/20

Interinstitutionelles Dossier:
2019/0267(NLE)

SCH-EVAL 190
DATAPROTECT 142
COMIX 556

BERATUNGSERGEBNISSE

Absender: Generalsekretariat des Rates

vom 1. Dezember 2020

Empfänger: Delegationen

Nr. Vordok.: 12856/20

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 **Slowenien** 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 Slowenien festgestellten Mängel, der am 1. Dezember 2020 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 Slowenien 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 Durchführungsübereinkommen¹, insbesondere auf Artikel 15,

auf Vorschlag der Europäischen Kommission,

in Erwägung nachstehender Gründe:

- (1) Gegenstand dieses an Slowenien gerichteten Beschlusses ist die Empfehlung von Abhilfemaßnahmen zur Beseitigung der Mängel, die während der 2019 im Bereich des Datenschutzes durchgeführten Schengen-Evaluierung festgestellt worden sind. Nach Abschluss der Evaluierung nahm die Kommission mit dem Durchführungsbeschluss C(2019) 8050 einen Bericht an, in dem die Ergebnisse und Bewertungen sowie die während der Evaluierung festgestellten bewährten Vorgehensweisen und Mängel aufgeführt sind.
- (2) Zu den bewährten Vorgehensweisen zählen unter anderem folgende: die Polizeibediensteten erhalten eine spezielle Datenschutzschulung; die Datenschutzbehörde hat eine erhebliche Zahl von Aufsichtsmaßnahmen in Bezug auf das SIS II und das VIS getroffen; die Struktur des VIZIS bietet ein hohes Datenschutzniveau und gewährleistet, dass geeignete Garantien bestehen und die für betroffene Personen online bereitgestellten Informationen zum SIS II und zum VIS sehr detailliert und leicht zugänglich sind.

¹ ABl. L 295 vom 6.11.2013, S. 27.

- (3) Angesichts der Bedeutung, die der ordnungsgemäßen Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes in Bezug auf das SIS II zukommt, sollten die Empfehlungen 8, 13 und 14 vorrangig umgesetzt werden. Was Empfehlung 13 anbelangt, so führt die Polizei derzeit bei sehr wenigen Nutzern lange Zeit zurückreichende Protokollprüfungen durch. Die kürzere Zeit zurückreichende Prüfung der Protokolle einer größeren Zahl von Nutzern würde die Darlegungslast in Bezug auf den einzelnen Nutzer verringern und gleichzeitig eine kohärentere Überwachung der Nutzeraktionen im SIS II gewährleisten.
- (4) Angesichts der Bedeutung, die der ordnungsgemäßen Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes in Bezug auf das VIS zukommt, sollten die Empfehlungen 5 und 6 vorrangig umgesetzt werden.
- (5) Um Rechtssicherheit zu gewährleisten, ist es ferner unerlässlich, dass zügig nationale Rechtsvorschriften zur Durchführung der Datenschutz-Grundverordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 zum Datenschutz bei der Strafverfolgung erlassen werden. Daher sollte Empfehlung 1 höchste Priorität erhalten.
- (6) Dieser Beschluss ist dem Europäischen Parlament und den Parlamenten der Mitgliedstaaten zu übermitteln. Innerhalb von drei Monaten nach seiner Annahme sollte Slowenien nach Artikel 16 Absatz 1 der Verordnung (EU) Nr. 1053/2013 einen Aktionsplan erstellen, in dem alle Empfehlungen zur Beseitigung der im Evaluierungsbericht festgestellten Mängel aufgeführt sind, und diesen der Kommission und dem Rat vorlegen —

EMPFIEHLT:

Slowenien sollte

Gesetzgebung

1. dringend seine nationalen Rechtsvorschriften an die Bestimmungen der Datenschutz-Grundverordnung (EU) 2016/679 anpassen und die Richtlinie (EU) 2016/680 zum Datenschutz bei der Strafverfolgung vollständig umsetzen;

Datenschutzaufsichtsbehörde

2. dafür sorgen, dass die obligatorischen Prüfungen durch die Datenschutzaufsichtsbehörde rechtzeitig abgeschlossen werden, sobald eine ausreichende Grundlage für die Beschlussfassung vorhanden ist;
3. dafür sorgen, dass mindestens alle vier Jahre eine allgemeine VIS-Überprüfung der Datenverarbeitung im nationalen System vorgenommen wird;

Visa-Informationssystem

4. eine Risikobewertung für den Serverraum durchführen und dokumentieren und die Risiken für die physische Sicherheit mindern;
5. prüfen, ob außerhalb des Standorts des Hauptservers ein Standort für die Notfallwiederherstellung von SI.VIS- und VIZIS-Datensätzen eingerichtet werden sollte;
6. eine regelmäßige Eigenkontrolle des gesamten SI.VIS vornehmen, um den ordnungsgemäßen Betrieb und die ordnungsgemäße Nutzung des Systems zu gewährleisten;
7. dafür sorgen, dass der Datenschutzbeauftragte des Außenministeriums aktiv an Projekten zur Verarbeitung personenbezogener Daten mitwirkt;

Schengener Informationssystem

8. dafür sorgen, dass das Löschungsverfahren für die Zusatzinformationen in der SIRENE-Anwendung häufiger und in regelmäßigen Abständen durchgeführt wird;
9. dafür sorgen, dass die Löschungsverfahren für die Zusatzinformationen in der SIRENE-Anwendung schriftlich dokumentiert werden und für den Datenschutzbeauftragten und die Datenschutzaufsichtsbehörde zugänglich sind;
10. dafür sorgen, dass die Löschungsverfahren automatisch durchgeführt werden, um sicherzustellen, dass die Löschung nach Ablauf der Speicherfristen erfolgt;
11. eine Risikobewertung für das Datenzentrum der Polizei und die Serverräume der Polizei durchführen und dokumentieren und die größten Risiken für die physische Datensicherheit mindern;

12. prüfen, ob es notwendig ist, so vielen Bediensteten Zugang zu den Serverräumen im Datenzentrum der Polizei zu gewähren, und dafür sorgen, dass Zugangsrechte auf die Bediensteten beschränkt werden, die im Rahmen ihrer Aufgaben einen physischen Zugang zu den Server-Racks benötigen;
13. häufiger die Protokolle über den Zugriff auf SIS-II-Daten und deren Verarbeitung prüfen;
14. dafür sorgen, dass die Speicherfristen für Protokolle beachtet werden und dass Protokolle, die älter als drei Jahre sind, nach Artikel 12 Absatz 4 des SIS-II-Beschlusses und der SIS-II-Verordnung gelöscht werden;
15. nach Artikel 13 des SIS-II-Beschlusses und der SIS-II-Verordnung eine regelmäßige Eigenkontrolle der Einhaltung der Datenschutzvorschriften für das SIS II vornehmen;

Rechte betroffener Personen und Sensibilisierung

16. dafür sorgen, dass Inspektionen, die die Datenschutzbehörde auf Antrag betroffener Personen veranlasst, so rechtzeitig abgeschlossen werden, dass die betroffenen Personen ihr Recht auf einen behördlichen Rechtsbehelf wirksam ausüben können;
17. betroffenen Personen die Ausübung ihrer Rechte dadurch erleichtern, dass allgemeine Anträge ohne Angabe des bzw. der Systeme, für die der Zugang zu personenbezogenen Daten beantragt wird, so ausgelegt werden, dass sie auch die im SIS II verarbeiteten personenbezogenen Daten umfassen;
18. die Standardantwort, mit der Anträge auf Zugang zu Informationen im Falle von Zugangsbeschränkungen beschieden werden, verbessern;
19. in seinem nationalen Recht für eine geeignete Rechtsgrundlage für die Beschränkung der sich aus dem SIS-II-Beschluss ergebenden Rechte betroffener Personen sorgen.

Geschehen zu Brüssel am [...]

*Im Namen des Rates
Der Präsident*