

Bruxelles, le 25 janvier 2021
(OR. en)

5533/21

Dossier interinstitutionnel:
2020/0307(NLE)

SCH-EVAL 10
DATAPROTECT 13
COMIX 41

RÉSULTATS DES TRAVAUX

Origine: Secrétariat général du Conseil

Destinataire: délégations

N° doc. préc.: 14247/20

Objet: Décision d'exécution du Conseil arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2019 de l'application, par la **Hongrie**, de l'acquis de Schengen dans le domaine de la **protection des données**

Les délégations trouveront ci-joint la décision d'exécution du Conseil arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2019 de l'application, par la Hongrie, de l'acquis de Schengen dans le domaine de la protection des données, adoptée par procédure écrite le 21 janvier 2021.

Conformément à l'article 15, paragraphe 3, du règlement (UE) n° 1053/2013 du Conseil du 7 octobre 2013, cette recommandation sera transmise au Parlement européen et aux parlements nationaux.

Décision d'exécution du Conseil arrêtant une

RECOMMANDATION

pour remédier aux manquements constatés lors de l'évaluation de 2019 de l'application, par la Hongrie, de l'acquis de Schengen dans le domaine de la protection des données

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) n° 1053/2013 du Conseil du 7 octobre 2013 portant création d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen et abrogeant la décision du comité exécutif du 16 septembre 1998 concernant la création d'une commission permanente d'évaluation et d'application de Schengen¹, et notamment son article 15,

vu la proposition de la Commission européenne,

considérant ce qui suit:

- (1) La présente décision a pour objet de recommander à la Hongrie des mesures correctives pour remédier aux manquements constatés lors de l'évaluation de Schengen, effectuée en 2019, dans le domaine de la protection des données. À la suite de cette évaluation, un rapport faisant état des constatations et appréciations et dressant la liste des meilleures pratiques et manquements constatés lors de l'évaluation a été adopté par la décision d'exécution C(2020) 8170 de la Commission.

¹ JO L 295 du 6.11.2013, p. 27.

- (2) Parmi les bonnes pratiques figurent le fait que le budget de l'autorité nationale de la protection des données et de la liberté de l'information (ci-après dénommée "NAIH") n'ait cessé de croître, le fait que le bureau Sirene ait donné suite aux recommandations de la précédente évaluation de Schengen de 2012 sur la protection des données et prévoient à présent la possibilité pour les personnes concernées de déposer une plainte auprès de la NAIH; le fait que le ministère des affaires étrangères et du commerce extérieur fasse également référence au recours juridictionnel; le fait que les informations fournies sur le site web de la NAIH soient complètes, utiles et disponibles, facilement accessibles et exprimées en termes clairs; le fait que le ministère des affaires étrangères et du commerce extérieur ait pris des mesures pour gérer et formaliser les différents aspects de la sécurité de l'information; le fait que le ministère des affaires étrangères et du commerce extérieur dispose d'un plan de sécurité solide et global et que les modèles relatifs à l'exercice des droits des personnes concernées pour ce qui est de leurs données figurant dans le système d'information Schengen (SIS) II soient disponibles en plusieurs langues (hongrois, anglais, allemand, français et russe).
- (3) Il n'y a pas lieu de fournir une indication de priorité pour la mise en œuvre de cette recommandation.
- (4) Il convient de transmettre la présente décision au Parlement européen et aux parlements des États membres. Conformément à l'article 16, paragraphe 8, du règlement (UE) n° 1053/2013, la Hongrie devrait soumettre à la Commission, dans un délai de six mois à compter de l'adoption de la présente décision, une appréciation des (éventuelles) améliorations et une description des mesures nécessaires,

RECOMMANDE

que la Hongrie:

Autorité de protection des données (NAIH)

1. veille à ce que la NAIH, lorsqu'elle surveille le respect de la législation relative au SIS II, procède également à des contrôles réguliers des signalements introduits dans le SIS II;
2. veille à ce que la NAIH assure le suivi des conclusions et des recommandations résultant des contrôles du SIS II et des audits des mesures de surveillance précédentes et à ce qu'elles soient également prises en considération dans les plans d'inspection de 2019;
3. veille à ce que la NAIH assure un suivi complet de la mise en œuvre effective des recommandations découlant des activités de surveillance du système d'information sur les visas (VIS);

4. veille à ce que les activités de surveillance du VIS menées par la NAIH couvrent tous les aspects du système national d'information sur les visas relatifs à la protection des données, y compris le traitement par des prestataires de services extérieurs;

Droits des personnes concernées

5. élargisse le champ d'application de l'annexe 9 du décret gouvernemental 15/2013 (qui établit un modèle spécifique pour l'exercice des droits d'accès des personnes concernées) afin d'établir également des modèles pour l'exercice d'autres droits des personnes concernées, tels que la correction ou la suppression de données;
6. veille à ce que les autorités hongroises (direction générale nationale chargée de la police des étrangers - OIF) clarifient leurs procédures relatives à l'évaluation des demandes des personnes concernées, en particulier lorsqu'elles limitent les droits de rectification ou de suppression, et les alignent sur le droit de l'Union et le droit national applicables;

Système d'information sur les visas

7. veille à ce que les utilisateurs privilégiés du VIS fassent l'objet d'une surveillance suffisante; dans cette perspective, des mesures organisationnelles et techniques peuvent être nécessaires pour surveiller les utilisateurs privilégiés;
8. augmente la fréquence des tests relatifs à la gestion de la continuité des activités/au plan de reprise des activités, en particulier pour le ministère des affaires étrangères et du commerce extérieur;
9. veille à ce que, jusqu'à la mise en œuvre du site TI secondaire, à court terme, toutes les copies de sauvegarde ne soient pas stockées dans le même local que la salle des serveurs, mais dans un lieu extérieur;
10. accroisse la sécurité de l'accès aux rayonnages ("racks");
11. effectue régulièrement un examen de la sécurité du système de cryptage mis au point en interne (ministère des affaires étrangères et du commerce extérieur);

Système d'information Schengen

12. améliore la sécurité physique du bâtiment abritant le centre de données en dotant également la deuxième sortie/entrée de caméras de surveillance, ainsi que celle des rayonnages dans la salle des serveurs;
13. effectue régulièrement des contrôles de sécurité du système de gestion de l'accès des utilisateurs du SIS II;

14. veille à l'utilisation d'un ensemble uniforme de directives/lignes directrices relatives à la sécurité de l'information pour le N.SIS (politique en matière de mots de passe, etc.);
15. veille à ce que le bureau Sirene, en coopération avec les archives nationales, examine les possibilités de recourir à une procédure de sélection plus fréquente en ce qui concerne la conservation des données;
16. augmente la fréquence des tests relatifs à la gestion de la continuité des activités/au plan de reprise des activités;
17. veille à ce que l'administration centrale de la police nationale hongroise (ORFK), et notamment l'office N.SIS et le bureau Sirene, mette en place une solution pour la surveillance des utilisateurs privilégiés;
18. veille à ce que le bureau Sirene joue un rôle plus actif dans la coordination de la vérification de la qualité des informations introduites dans le SIS II, tel que décrit à la section 1.15 du manuel Sirene;

Sensibilisation du public

19. veille à ce que le ministère des affaires étrangères et du commerce extérieur définisse clairement le(s) responsable(s) du traitement aux fins du VIS. Afin d'assurer la transparence et de permettre aux personnes d'exercer leurs droits, il est important que les personnes concernées soient dûment informées des responsabilités incombant à chaque responsable du traitement des données;
20. veille à ce que l'administration centrale de la police nationale hongroise fournisse régulièrement des mises à jour de la version anglaise contenant la section consacrée au SIS.

Fait à Bruxelles, le

*Par le Conseil
Le président*