Conseil de
l'Union européenne

Bruxelles, le 25 janvier 2021
(OR. en)

5534/21

Dossier interinstitutionnel:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
Nº doc. préc.:	14250/20
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 **Slovaquie**, 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 Slovaquie, de l'acquis de Schengen dans le domaine de la protection des données, adoptée par voie de 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 Slovaquie, 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 Schengen[1], 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 République slovaque 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) 8160 de la Commission.

[1] JO L 295 du 6.11.2013, p. 27.

(2) Sont notamment considérés comme de bonnes pratiques le fait que, depuis la dernière évaluation de Schengen, effectuée en 2012, l'autorité chargée de la protection des données (ci-après dénommée "APD") ait exercé des activités de supervision du SIS II sur une base régulière conformément à un planning annuel et le fait que des principes aient été élaborés concernant les inspections du SIS II pour les quatre prochaines années; le fait que l'APD ait réalisé un nombre considérable d'inspections concernant le VIS dans des consulats; les efforts déployés par l'APD et le ministère de l'intérieur pour fournir des informations aux personnes concernées sur des supports électroniques et imprimés; l'existence d'informations sur des sujets relatifs à Schengen en différentes versions linguistiques sur le site web de l'APD et dans les brochures; le fait que l'APD ait fourni des modèles pour les demandes des personnes concernées dont les données sont stockées dans le SIS et dans le VIS; le fait que le bureau Sirene fournisse des réponses aux demandes non seulement en slovaque, mais aussi en anglais; le fait que les autorités slovaques informent les personnes concernées lorsque aucune donnée les concernant n'est stockée dans le SIS II; le contrôle très actif des fichiers journaux du VIS et du SIS II par l'unité "Inspections" du service du bureau des inspections du ministère de l'intérieur; le rôle très actif des deux agents du département de la sécurité au sein du ministère des affaires étrangères et européennes traitant des questions relatives à la protection des données; le fait que le ministère des affaires étrangères et européennes dispense à son personnel une formation à la protection des données, en particulier avant une affectation temporaire à des tâches consulaires, et que ce soit le département de la sécurité, en sa qualité de bureau du délégué à la protection des données (DPD) qui dispense cette formation; le fait que la sécurité physique et des procédures mise en place pour protéger les données du SIS II soit élevée; le rôle très actif du DPD et du DPD adjoint au sein du département de la protection des données relevant de l'unité "Inspections" du bureau du service des inspections du ministère de l'intérieur, notamment en matière d'orientations et de contrôle des fichiers journaux en ce qui concerne le SIS II; le fait que le ministère de l'intérieur dispense une formation à la protection des données à l'ensemble des utilisateurs finaux du N.SIS II.

(3) Eu égard à l'importance que revêt le respect de l'acquis de Schengen concernant la protection des données dans le contexte du VIS, priorité devrait être donnée à la mise en œuvre des recommandations 7 et 24.

(4) Il convient de transmettre la présente décision au Parlement européen et aux parlements des États membres. Conformément à l'article 16, paragraphe 1, du règlement (UE) n° 1053/2013, dans un délai de trois mois à compter de l'adoption de la présente décision, la République slovaque devrait élaborer un plan d'action énumérant toutes les recommandations, destiné à remédier à tout manquement constaté dans le rapport d'évaluation, et soumettre ce plan d'action à la Commission et au Conseil,

RECOMMANDE

que la République slovaque:

Autorité chargée de la protection des données

1. veille à ce que, pour renforcer les performances et l'efficacité de l'APD, le budget et le personnel de celle-ci soient encore augmentés;

2. veille à ce que la part du budget général de l'État prévue pour l'APD apparaisse clairement, afin de garantir que l'APD dispose d'un budget annuel public propre;

3. veille à ce que, dans la procédure budgétaire, le Conseil national soit informé de la position de l'APD sur ses besoins budgétaires et des discussions tenues entre l'APD et le ministère des finances concernant le budget;

4. prenne des mesures pour que le ministère des finances ne puisse pas établir de corrélation entre le budget et le montant des amendes à collecter par l'APD, car cela pourrait avoir une incidence sur la nature et l'organisation des priorités des travaux de l'APD, et donc affecter l'indépendance de celle-ci. Il conviendrait d'assurer que le budget de l'APD ne puisse pas diminuer au cours de l'année civile lorsque les amendes estimées n'ont pas été entièrement perçues par l'APD;

5. veille à ce que l'ensemble des missions et des pouvoirs attribués aux autorités chargées de la protection des données par les articles 57 et 58 du règlement général sur la protection des données (RGPD) soient conférés à l'APD;

6. veille à ce qu'en plus des activités de supervision classiques menées à l'office N.SIS et au bureau Sirene, l'APD supervise davantage d'autorités utilisatrices finales ayant un droit d'accès au SIS II;

7. veille à ce que les activités de supervision de l'APD en lien avec le VIS comprennent l'inspection de l'autorité centrale chargée des visas pour ce qui concerne les opérations de traitement des données dans le N-VIS. Le délai pour le premier audit du système national des visas (octobre 2015) n'ayant pas été respecté, l'APD devrait réaliser cette partie encore manquante de l'audit dans les plus brefs délais;

8. veille à ce que l'APD inspecte également les prestataires de services extérieurs sur une base régulière;

Droits des personnes concernées

9. trouve un moyen approprié pour que l'APD, le ministère de l'intérieur et le ministère des affaires étrangères et européennes informent les personnes concernées des risques potentiels inhérents à la communication de copies de cartes d'identité et d'informations sensibles sur l'internet ouvert. Le ministère de l'intérieur et le ministère des affaires étrangères et européennes sont invités à envisager d'offrir aux personnes concernées un canal de transmission électronique sécurisé pour la communication de ces documents;

10. veille à ce que le délai de 60 jours pour répondre aux demandes des personnes concernées à propos du SIS II, prévu à l'article 41, paragraphe 6, du règlement SIS II et à l'article 58, paragraphe 6, de la décision SIS II, soit respecté jusqu'à ce que le nouvel acquis SIS[1] devienne pleinement applicable (au plus tard le 28 décembre 2021), celui-ci contenant des références croisées au délai prévu dans le RGPD pour les réponses à donner aux demandes de personnes concernées (30 jours, avec une possibilité d'extension de deux mois supplémentaires si nécessaire);

11. envisage de fournir certaines des informations imprimées (brochures/posters, etc.) destinées aux personnes concernées dans les locaux des commissariats de police, ainsi que de les rendre visibles et facilement accessibles;

12. envisage de fournir, par exemple, une version non officielle en langue anglaise des décisions de l'APD sur des plaintes relatives à des demandes de personnes concernées à propos du SIS II; cela aiderait les personnes concernées à mieux comprendre les décisions et, de ce fait, renforcerait leurs droits;

13. veille à ce que les informations sur les droits des personnes concernées dont les données sont stockées dans le VIS soient plus faciles à trouver sur le site web du ministère des affaires étrangères et européennes; ce site web devrait également contenir des formulaires permettant auxdites personnes concernées d'exercer leurs droits;

---

[1] Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56; voir notamment les articles 66 à 71); règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006 (JO L 312 du 7.12.2018, p. 14; voir notamment les articles 51 à 57).

14. veille à ce que le formulaire de demande de visa contienne des informations claires sur les différentes autorités qui traitent les données à caractère personnel dans le cadre du système national des visas. En particulier, il devrait être indiqué que c'est le ministère des affaires étrangères et européennes qui est le responsable du traitement;

15. fournisse aux personnes concernées dont les données sont stockées dans le VIS des informations sous forme physique (brochures/posters, etc.) dans les locaux des aéroports et d'autres points de contrôle des frontières et les rendre visibles et facilement accessibles;

16. veille à ce que les réponses adressées aux personnes concernées en rapport avec les données à caractère personnel stockées dans le VIS fournissent des informations sur les possibilités de former un recours contre la réponse devant l'APD et la juridiction compétente;

17. prenne les mesures nécessaires pour clarifier les responsabilités du ministère des affaires étrangères et européennes et de l'autorité centrale chargée des visas (ministère de l'intérieur) à l'égard du traitement des demandes émanant de personnes concernées dont les données sont stockées dans le VIS et pour élaborer des orientations internes ou méthodologiques destinées à ces deux entités; ces informations devraient être mises à la disposition des personnes concernées;

Système d'information sur les visas

18. prenne les mesures nécessaires pour augmenter le niveau de sécurité de l'accès aux administrations de l'État, et en particulier aux demandes de visas nationaux déposées auprès du ministère des affaires étrangères et européennes et du ministère de l'intérieur (autorité centrale chargée des visas), notamment par un accès aux bases de données nationales concernant les visas au moyen de technologies plurifactorielles;

19. prenne les mesures nécessaires pour améliorer la sécurité physique et organisationnelle au centre de données du N-VIS du ministère des affaires étrangères et européennes, en particulier sur les points suivants:

    – mise en place d'un registre des visiteurs à l'entrée du centre de données pour le personnel informatique, les visiteurs ou les fournisseurs dont l'accès devrait être limité;

    – installation d'un système d'extinction d'incendie au gaz (argonite);

    – installation d'un système de détection des fuites d'eau;

    – maintien d'un sol propre et sans poussière;

    – verrouillage de la barrière de protection des serveurs de l'UE;

20. accélère la procédure de mise en place d'un nouveau centre de données pour le N-VIS en un autre lieu et le déménagement du centre de données;

21. envisage de modifier la période de conservation locale des fichiers journaux du N-VIS dans les missions consulaires et diplomatiques, en fixant une durée plutôt qu'un volume de Mb;

22. envisage l'utilisation de systèmes de contrôle automatique des enregistrements au ministère des affaires étrangères et européennes;

23. prenne les mesures nécessaires pour que les missions diplomatiques ou le ministère des affaires étrangères et européennes inspectent les prestataires de services extérieurs sur une base régulière;

24. prenne les mesures nécessaires pour dispenser une formation à la protection des données au personnel consulaire local de manière plus systématique et uniforme;

25. veille à ce que la demande de visa électronique repose sur les mêmes informations que celles requises dans le formulaire de demande de visa sur papier (voir annexe I du code des visas de l'UE[1]);

Système d'information Schengen II

26. prenne les mesures nécessaires pour améliorer le niveau de sécurité de l'accès au N.SIS II, en particulier en utilisant une authentification plurifactorielle et en recourant uniquement à des connexions https;

27. veille à ce que le ministère de l'intérieur informe l'APD de toute violation de données qui est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. En outre, le ministère de l'intérieur devrait mettre en place un registre des violations de données à caractère personnel;

[1] Règlement (CE) n° 810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code communautaire des visas (code des visas) (JO L 243 du 15.9.2009, p. 1).

Sensibilisation du public

28. envisage de mettre les brochures de l'APD à la disposition des personnes concernées également en des lieux plus accessibles, comme les commissariats de police, les zones de contrôle aux frontières et les locaux des consulats;

29. envisage d'ouvrir les présentations, séminaires et journées portes ouvertes de l'APD au grand public, en particulier aux intéressés concernés par les informations sur le SIS II et le VIS.

Fait à Bruxelles, le

Par le Conseil
Le président