Conseil de
l'Union européenne

Bruxelles, le 24 septembre 2019
(OR. en)

12468/19

Dossier interinstitutionnel:
2019/0168(NLE)

SCH-EVAL 157
DATAPROTECT 216
COMIX 427

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	20 septembre 2019
Destinataire:	délégations
Nº doc. préc.:	11904/19
Objet:	Décision d'exécution du Conseil arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2018 de l'application, par la **Lituanie**, de l'acquis de Schengen dans le domaine de la **protection des données**

Les délégations trouveront en annexe la décision d'exécution du Conseil arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2018 de l'application, par la Lituanie, de l'acquis de Schengen dans le domaine de la protection des données, adoptée par le Conseil lors de sa session tenue le 20 septembre 2019.

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 2018 de l'application, par la Lituanie, 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) nº 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 Lituanie des mesures correctives pour remédier aux manquements constatés lors de l'évaluation de Schengen, effectuée en 2018, dans le domaine de la protection des données. À la suite de cette évaluation, un rapport faisant état des constatations et des appréciations et dressant la liste des meilleures pratiques et des manquements constatés lors de l'évaluation a été adopté par la décision d'exécution C(2019) 5700 de la Commission.

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

(2) Sont notamment considérés comme de bonnes pratiques le fait que l'autorité de protection des données (APD) fournisse des conseils et des orientations aux personnes qui font appel à elle plutôt que de se borner à faire suivre les demandes; la fourniture de lettres-types pour l'exercice des droits des personnes concernées dans le cadre du système d'information Schengen de deuxième génération (SIS II) et du système d'information sur les visas (VIS); le fait que les mesures de sécurité mises en œuvre dans les locaux du service des technologies de l'information et des communications auprès du ministère de l'intérieur (qui héberge le N.VIS et le N.SIS) soient généralement d'un niveau élevé et permettent de sécuriser l'environnement de stockage des données et de prévenir tout incident; le fait que la formation prodiguée aux utilisateurs finals du VIS, notamment au personnel consulaire avant une affectation dans une ambassade ou un consulat, soit bien développée; l'importance attachée à la formation et au perfectionnement du personnel, en particulier une formation bien développée, notamment en matière de protection des données, pour les utilisateurs finals du N.SIS et pour le personnel du bureau SIRENE; le fait que l'information que fournit l'APD sur son site web au sujet du SIS II et du VIS soit très complète, utile et rédigée de manière aisément compréhensible (dans plusieurs langues); le fait que les brochures de l'APD intitulées "Personal Data Protection in the Schengen Information System" [La protection des données à caractère personnel dans le système d'information Schengen] et "Personal Data Protection in the Visa Information System" [La protection des données à caractère personnel dans le système d'information sur les visas] fournissent des informations accessibles et de grande qualité sur le traitement des données dans ces deux bases de données et sur les droits des personnes concernées qui s'y rattachent, ainsi que la participation active de l'APD à de nombreuses conférences, formations et autres actions de sensibilisation, notamment destinées au personnel chargé du traitement des données dans le cadre du SIS II et du VIS.

(3) Eu égard à l'importance que revêt le respect de l'acquis de Schengen dans le domaine de la protection des données, notamment pour garantir l'indépendance totale de l'APD, la priorité devrait être donnée à la mise en œuvre de la recommandation 1.

(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 Lituanie devrait élaborer un plan d'action énumérant toutes les recommandations visant à remédier aux manquements constatés dans le rapport d'évaluation et le soumettre à la Commission et au Conseil,

RECOMMANDE:

que la Lituanie:

Autorité de contrôle de la protection des données

1. abolisse, afin de mieux garantir l'indépendance totale de l'Inspection nationale de la protection des données (ci-après dénommée l'"APD"), l'obligation de faire approuver le plan d'action stratégique de l'APD par le ministre de la justice et de consulter ce dernier sur le plan d'action annuel avant que le directeur de l'APD puisse l'approuver; cette mesure est également importante pour veiller à ce que la procédure budgétaire ne comporte pas d'éléments susceptibles de violer l'indépendance de l'APD;

2. organise, afin de garantir l'indépendance totale de l'APD, les rencontres bilatérales régulières entre le ministre de la justice et le directeur de l'APD de telle façon qu'il ne puisse en résulter un risque d'influence directe ou indirecte du gouvernement sur l'APD susceptible de compromettre l'indépendance de cette dernière;

3. supprime tous les éléments de responsabilité du directeur de l'APD devant le gouvernement et le ministre de la justice qui pourraient créer un risque d'influence directe ou indirecte du gouvernement et du ministre de la justice susceptible de compromettre l'indépendance de l'APD;

4. veille à ce que l'APD contrôle plus fréquemment la licéité du traitement des données à caractère personnel du SIS II;

5. veille à ce que des audits des opérations de traitement des données dans le N.SIS soient effectués par l'APD au moins tous les quatre ans;

6. veille à ce que l'APD contrôle la licéité du traitement des données à caractère personnel du VIS. Lorsqu'elle inspecte les ambassades, l'APD devrait également vérifier les opérations de traitement de données et la sécurité des données auprès des prestataires de services externes; cette possibilité devrait être précisée dans le contrat conclu entre le ministère des affaires étrangères et les prestataires de services externes;

7. veille à ce que des audits des opérations de traitement des données dans le N.SIS soient effectués par l'APD au moins tous les quatre ans;

Droits des personnes concernées

8. veille à ce que le délai de 60 jours pour répondre à une demande SIS II d'une personne concernée, 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[2] devienne pleinement applicable (au plus tard le 28 décembre 2021), celui-ci contenant des références croisées au délai prévu dans le règlement général sur la protection des données (RGPD)[3] pour les réponses à donner aux demandes de personnes concernées (30 jours, avec une possibilité d'extension de deux mois supplémentaires si nécessaire);

9. clarifie les procédures internes relatives à la responsabilité des autorités concernées en matière de traitement des droits des personnes concernées dans le SIS II, afin que le personnel sache à qui adresser les demandes;

---

[2] 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).

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

10. veille à la cohérence des réponses définitives données par le ministère de l'intérieur aux personnes souhaitant exercer leurs droits en tant que personnes concernées dans le SIS II, de façon que les intéressés soient informés de leur droit de recours devant l'APD et de leurs droits de recours juridictionnels;

11. clarifie les procédures internes relatives à la responsabilité des autorités concernées en matière de traitement des droits des personnes concernées dans le VIS, afin que le personnel sache à qui adresser les demandes;

12. veille à la cohérence des réponses définitives données par le ministère de l'intérieur aux personnes souhaitant exercer leurs droits en tant que personnes concernées dans le VIS, de façon que les intéressés soient informés de leur droit de recours devant l'APD et de leurs droits de recours juridictionnels;

Système d'information sur les visas

13. prenne les mesures requises pour que les contrats conclus entre le ministère des affaires étrangères et les prestataires de services externes prévoient les modalités de la participation de l'APD lituanienne aux inspections effectuées par les ambassades/les consulats et ledit ministère;

14. améliore l'autocontrôle en procédant de manière proactive à une vérification régulière des fichiers-journaux afin de contrôler la licéité du traitement des données à caractère personnel dans le VIS. Le ministère de l'intérieur devrait continuer à développer le système SIEM pour le contrôle automatique des fichiers-journaux;

15. veille à ce que le DPD du ministère des affaires étrangères participe plus activement à la conception et à l'organisation concrète des formations en matière de protection des données dispensées au personnel dudit ministère, notamment le personnel en poste dans les ambassades et consulats;

Système d'information Schengen II

16. supprime la possibilité pour un utilisateur final de se connecter au N.SIS via le navigateur POLIS sur plusieurs appareils en même temps;

17. veille à l'introduction de cartes à puce pour l'accès aux stations de travail d'utilisateurs du N.SIS au sein de la police, afin de relever le niveau et les normes de sécurité;

18. veille à ce que les mesures techniques prises pour empêcher l'utilisation de clés USB sur des stations de travail du bureau SIRENE soient pleinement appliquées et fassent l'objet de contrôles périodiques;

19. améliore l'autocontrôle en procédant de manière proactive à une vérification régulière des fichiers-journaux des utilisateurs finals du SIS II de toutes les autorités concernées afin de contrôler la licéité du traitement des données à caractère personnel dans le SIS II; le ministère de l'intérieur devrait continuer à développer le système SIEM pour le contrôle automatique des fichiers-journaux;

20. veille à améliorer la sensibilisation du personnel à la protection des données lors du traitement de données dans le SIS II et le VIS, grâce à l'organisation régulière de cours de remise à niveau;

21. veille à ce que le groupe des DPD du ministère de l'intérieur dirige la formation et la sensibilisation du personnel ayant accès au N.SIS, ce qui lui permettra d'assurer la continuité dans la structure et la planification du perfectionnement du personnel;

Sensibilisation du public

22. veille à ce que les liens relatifs au SIS II et au VIS figurant sur le site web de l'APD soient régulièrement mis à jour;

23. veille à ce que les sites web d'organismes ayant des contacts avec des ressortissants d'autres pays, tels que le ministère de l'intérieur, la police, le service national des gardes-frontières, le ministère des affaires étrangères et les services consulaires, fournissent en anglais également des informations accessibles et claires sur le SIS II et le VIS et sur les droits connexes des personnes concernées;

24. veille à ce que les informations sur le SIS II et le VIS, ainsi que sur les droits connexes des personnes concernées, figurant en anglais sur des sites web soient plus aisées à trouver;

25. veille à la cohérence des informations sur l'exercice des droits des personnes concernées en rapport avec le N.SIS II et le VIS fournies sur les sites web des organismes qui travaillent avec ces systèmes;

26. ajoute, sur le portail EPM par l'intermédiaire duquel les personnes peuvent communiquer leurs coordonnées pour les demandes de visa, des informations sur le traitement des données et les droits des personnes concernées dans le cadre du VIS.

Fait à Bruxelles, le

Par le Conseil
Le président