Conseil de
l'Union européenne

Bruxelles, le 22 février 2022
(OR. en)

6426/22

Dossier interinstitutionnel:
2021/0392(NLE)

SCH-EVAL 21
DATAPROTECT 42
COMIX 87

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	21 février 2022
Destinataire:	délégations
Nº doc. préc.:	5893/22
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 **Pologne**, 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 Pologne, de l'acquis de Schengen dans le domaine de la protection des données, qui a été adoptée par le Conseil lors de sa session tenue le 21 février 2022.

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 Pologne, 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) Conformément au règlement (UE) n° 1053/2013, une évaluation destinée à vérifier l'application de l'acquis de Schengen dans le domaine de la protection des données à caractère personnel en Pologne a été effectuée en 2019. À la suite de cette évaluation, un rapport faisant état des constatations et évaluations et dressant la liste des meilleures pratiques et des manquements constatés lors de l'évaluation a été adopté par la décision d'exécution C(2021) 9100 de la Commission.

(2) Compte tenu des résultats de l'évaluation, il convient de recommander à la Pologne certaines mesures correctives pour remédier aux manquements constatés.

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

(3) Sont considérés comme de bonnes pratiques, entre autres: le cadre juridique national, qui permet au président de l'autorité polonaise chargée de la protection des données (APD) de nommer en toute indépendance ses adjoints ainsi que les membres du conseil consultatif; le fait que les candidats au poste de président de l'APD soient tenus de se soumettre à une audition publique au Parlement, qui est également diffusée sur l'internet par la chaîne officielle du Parlement; les activités de contrôle fréquent concernant les prestataires de services extérieurs, avec la participation du délégué à la protection des données, et les contrôles fréquents des consulats; la volonté de former le personnel et de développer ses compétences, y compris en matière de protection des données, pour les utilisateurs finaux du système national d'information Schengen (N.SIS) et le personnel du bureau SIRENE; les mesures de sécurité mises en œuvre dans les locaux des centres de données hébergeant le N.SIS et le système national d'information sur les visas (N.VIS).

(4) Compte tenu de l'importance que revêt le respect de l'acquis de Schengen en matière de protection des données à caractère personnel dans le cadre du système d'information sur les visas (VIS) et du système d'information Schengen (SIS), la priorité devrait être donnée à la mise en œuvre des recommandations 11, 12, 13, 20, 21 et 22 énoncées dans la présente décision.

(5) En application du règlement (UE) nº 1053/2013, la présente décision devrait être transmise au Parlement européen et aux parlements des États membres et la Pologne devrait, dans un délai de trois mois à compter de son adoption, élaborer un plan d'action énumérant toutes les recommandations visant 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 Pologne :

Législation

1. indique explicitement l'applicabilité du 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) au traitement des données à caractère personnel dans le N.VIS et le N.SIS, le cas échéant;

Autorité chargée de la protection des données

2. veille à ce que l'article 174 de la loi de 2018 sur la protection des données à caractère personnel et l'article 106 de la loi de 2018 relative à la protection des données dans le domaine répressif qui fixe le plafond des dépenses par année donnée ne limitent pas le budget de l'autorité polonaise chargée de la protection des données (APD) en dessous des sommes allouées dans le budget de l'État pour une année donnée;

3. veille à ce que l'APD planifie et organise mieux ses nombreuses inspections du N.SIS II afin de garantir que toutes les opérations de traitement du N.SIS II et toutes les entités concernées sont couvertes et que les inspections donnent lieu à un audit complet du N.SIS II comme prévu à l'article 44, paragraphe 2, du règlement (CE) n° 1987/2006;

4. veille à ce que l'APD effectue une inspection complète du N.VIS afin de s'acquitter pleinement de ses tâches conformément à l'article 41, paragraphe 2, du règlement (CE) n° 767/2008;

Droits des personnes concernées

5. veille à ce que les statistiques de l'APD relatives à l'exercice des droits des personnes concernées soient améliorées et différencient les plaintes des demandes, le système auquel elles se réfèrent (SIS ou VIS), l'objet et le type de demande (correction, suppression, accès);

6. veille à ce que le responsable du traitement adopte une approche plus proactive quant à la fourniture d'informations sur les droits des personnes concernées relatifs aux données du VIS;

7. veille à ce que le responsable du traitement des données du SIS et du VIS (police nationale polonaise - organe technique central pour le système informatique national) publie des formulaires types pour les demandes relatives à l'exercice des droits des personnes concernées;

Système d'information sur les visas

8. veille à ce que les relevés d'accès au VIS contiennent également des informations sur la justification de cet accès;

9. réévalue la liste des autorités ayant accès au VIS et les droits d'accès de ces dernières aux données du VIS, compte tenu de leurs compétences et de l'utilisation de ces données dans la pratique;

10. au vu de la multitude de responsables du traitement des données du VIS établis par les législations nationales et les dispositions contractuelles, et des nombreux acteurs concernés, clarifie la relation entre les autorités participant au processus de délivrance des visas et les autorités traitant les données du VIS, ainsi que les responsabilités de ces autorités en matière de traitement des données;

11. veille à ce que, pour exploiter pleinement les fichiers journaux conservés, les fichiers-journaux du VIS soient analysés de manière régulière afin de contrôler la protection des données;

12. adopte un plan de sécurité du VIS portant sur la sécurité physique du deuxième site de données ainsi que sur d'autres aspects liés à la sécurité informatique du système informatique national, y compris du système N.VIS;

13. aligne la durée de conservation des registres relatifs aux applications liées au VIS (en particulier les applications "Pobyt" et "ZSE 6") sur les délais fixés à l'article 34, paragraphe 2, du règlement (CE) n° 767/2008 et à l'article 16 de la décision 2008/633/JAI du Conseil;

Système d'information Schengen II

14. veille à ce que le responsable du traitement du N.SIS II mette en place un système central de gestion des utilisateurs permettant un autocontrôle efficace sans qu'il soit nécessaire de consulter les registres dans les institutions qui sont les utilisateurs finaux du N.SIS II;

15. veille à ce que, pour exploiter pleinement les fichiers-journaux conservés, les fichiers-journaux du SIS soient analysés de manière régulière afin de contrôler la protection des données;

16. garantit une notification automatisée des événements liés à la sécurité informatique et des activités d'autocontrôle du responsable du traitement afin d'améliorer encore la sécurité;

17. veille à ce que, parmi les mesures techniques adoptées, un terme soit mis à l'utilisation des dispositifs ou clés USB, en bloquant tous les ports USB sur les postes de travail du SIS;

18. envisage d'associer de manière proactive et régulière le délégué à la protection des données (DPD) du ministère de l'intérieur au suivi du traitement des données du SIS et du VIS au moyen du suivi des journaux d'audit;

19. veille à ce que le responsable du traitement des données du SIS fournisse à l'APD les profils des membres du personnel de toutes les autorités ayant accès au SIS;

20. aligne la durée de conservation des registres relatifs aux applications ayant accès aux données du SIS sur ce qui est prévu à l'article 12, paragraphe 4, du règlement (CE) n° 1987/2006 et à l'article 12, paragraphe 4, de la décision 2007/533/JAI du Conseil;

21. veille à ce que, conformément à l'article 10 du règlement (CE) n° 1987/2006 et à l'article 10 de la décision 2007/533/JAI du Conseil, le responsable du traitement des données du SIS adopte un plan de sécurité du SIS;

22. veille à ce que le large éventail d'institutions ayant accès aux données du SIS II soit réexaminé, afin de garantir que seules les institutions qui en ont besoin, compte tenu de leurs compétences et de leurs besoins pratiques, peuvent accéder aux données;

Sensibilisation du public

23. veille à ce que les sites web de l'APD et de la police fournissent des informations sur les droits des personnes concernées relatifs aux données du VIS.

Fait à Bruxelles, le

Par le Conseil
Le président