

Bruxelles, le 17 juin 2022
(OR. en)

10396/22

Dossier interinstitutionnel:
2021/0224(NLE)

SCH-EVAL 83
DATAPROTECT 197
COMIX 324

RÉSULTATS DES TRAVAUX

Origine: Secrétariat général du Conseil

en date du: 17 juin 2022

Destinataire: délégations

N° doc. préc.: 7788/22

Objet: Décision d'exécution du Conseil arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2020 de l'application, par l'**Autriche**, 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 2020 de l'application, par l'Autriche, de l'acquis de Schengen dans le domaine de la protection des données, adoptée par le Conseil lors de sa session tenue le 17 juin 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 2020 de l'application, par l'Autriche, 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) En novembre 2020, l'Autriche a fait l'objet d'une évaluation de Schengen 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(2021) 9200 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, le personnel de l'autorité autrichienne chargée de la protection des données (APD) a été renforcé et continue de l'être et que le budget a été revu à la hausse; le fait que les accords entre le responsable du traitement et le sous-traitant concernant les données du système d'information sur les visas (VIS) prévoient un niveau élevé de protection des données et garantissent la mise en place de garanties pertinentes en matière de protection des données par l'ensemble des parties concernées par le traitement de ces données; la formation du personnel aux questions liées à la protection des données du VIS par le ministère de l'intérieur et le ministère des affaires européennes et internationales; l'approche pluridimensionnelle du ministère des affaires européennes et internationales à l'égard du contrôle de la procédure de délivrance des visas; le caractère très circonstancié et facilement accessible des informations fournies par l'APD en ce qui concerne le SIS II et le VIS; les informations sur le SIS et le VIS fournies sur le site web du ministère de l'intérieur, ainsi que le fait que ce dernier répond rapidement aux demandes d'accès relatives au SIS II ou au VIS.
- (3) Il convient de formuler des recommandations relatives aux mesures correctives que l'Autriche doit prendre pour remédier aux manquements constatés dans le cadre de l'évaluation. Eu égard à l'importance que revêt le respect de l'acquis de Schengen en matière de protection des données à caractère personnel, il y a lieu de donner la priorité à la mise en œuvre des recommandations n° 1, 6, 7 et 13 énoncées dans la présente décision.
- (4) Il convient de transmettre la présente décision au Parlement européen et aux parlements nationaux 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, l'Autriche devrait élaborer un plan d'action, énumérant toutes les recommandations, destiné à remédier aux manquements constatés dans le rapport d'évaluation et soumettre ce plan d'action à la Commission et au Conseil,

RECOMMANDE:

que l'Autriche:

Législation

1. mette en œuvre l'article 79 du règlement général sur la protection des données (RGPD)¹ et transpose en droit national autrichien l'article 54 de la directive (UE) 2016/680² en matière de protection des données dans le domaine répressif afin de prévoir un droit de recours juridictionnel effectif contre la décision d'un responsable du traitement ou d'un sous-traitant qui est une autorité publique;

Autorité chargée de la protection des données

2. précise, dans sa législation nationale, les motifs de licenciement du directeur et du directeur adjoint de l'APD autrichienne autres qu'une faute grave ou que le fait de ne plus remplir les conditions requises pour exercer leurs fonctions, de façon à prévenir tout risque de révocation anticipée de leurs mandats;
3. veille à ce que l'expert en technologies de l'information engagé récemment par l'APD et tout autre expert supplémentaire en la matière possèdent ou acquièrent une connaissance approfondie du système d'information Schengen de deuxième génération (SIS II) et du système d'information sur les visas (VIS), ainsi que de la gestion de la sécurité de l'information pour pouvoir aussi participer activement aux activités de supervision du SIS et du VIS. En outre, l'APD devrait continuer à associer à ses inspections des experts en technologies de l'information externes jusqu'à ce qu'elle puisse couvrir toutes les tâches d'inspection liées aux technologies de l'information grâce à son propre personnel;

¹ 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).

² Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

4. veille à ce que l'APD effectue des visites d'inspection auprès du bureau Sirene, des inspections auprès de certaines autorités utilisatrices finales du système, telles que la police, ainsi que des vérifications et des analyses régulières des fichiers journaux, de façon à s'acquitter de sa mission consistant à assurer une supervision globale du traitement des données à caractère personnel du SIS II;
5. veille à ce que les activités de supervision de l'APD concernant le VIS couvrent également tous les aspects liés à la sécurité, y compris les journaux, au moyen de contrôles réguliers effectués sur la base de l'analyse des fichiers journaux et à ce que l'APD procède à des inspections approfondies des salles de serveurs et réalise aussi des inspections auprès d'autres utilisateurs finaux du système VIS, tels que la police;
6. veille à ce que l'APD finalise le deuxième audit du système national d'information sur les visas (N-VIS) dès que la situation concernant la COVID-19 le permettra;
7. veille à ce que l'APD réalise un audit des opérations de traitement des données dans le N-VIS au moins une fois tous les quatre ans;

Système d'information Schengen

8. veille à ce que tous les dispositifs permettant l'accès aux données du SIS II utilisent une authentification en deux facteurs;
9. veille à ce que tous les documents des systèmes de gestion de la sécurité de l'information mis en place pour les deux centres de données fassent l'objet d'un réexamen plus fréquent et à ce que les normes utilisées correspondent toujours à l'état de la technique;
10. veille à ce que le plan de sécurité relatif au SIS II fasse l'objet d'un réexamen régulier et, le cas échéant, d'une mise à jour, et à ce que des mesures de sécurité soient prises pour garantir durablement la solidité du système en plus de sa confidentialité, de son intégrité et de son accessibilité, en veillant notamment à ce que le responsable du traitement tienne compte de l'évolution technique pour que les mesures de sécurité adoptées continuent d'atteindre ces objectifs;

11. précise si l'autorité centrale de compensation fait partie intégrante du ministère de l'intérieur ou s'il s'agit d'un sous-traitant de données externe;
12. veille à ce que, pour le traitement des cas d'usurpation d'identité, des améliorations soient apportées quant aux informations communiquées à la personne concernée et dans les formulaires de consentement utilisés, et à ce que ces formulaires contiennent des informations sur les droits de la personne concernée, les coordonnées du délégué à la protection des données, la base juridique du traitement, ainsi que la durée de conservation des données à caractère personnel;

Système d'information sur les visas

13. veille à ce que les relevés de toutes les opérations de traitement de données effectuées dans le VIS soient conservés au niveau national, conformément à l'article 34 du règlement (CE) n° 767/2008 (règlement VIS) (pendant une période d'un an après la durée de conservation visée à l'article 23, paragraphe 1, du règlement VIS);

Sensibilisation du public et droits des personnes concernées

14. veille à ce que le ministère de l'intérieur mette à disposition son site web dans d'autres versions linguistiques (que l'allemand), en anglais par exemple, pour ce qui est du traitement des données du SIS II et du VIS et des droits des personnes concernées en la matière, et à ce qu'il facilite l'accès aux informations figurant sur ce site web relatives aux droits des personnes concernées pour ce qui est des données du SIS II et du VIS;
15. veille à ce que le ministère de l'intérieur fournisse sur son site web des formulaires, rédigés en allemand et dans d'autres langues, comme l'anglais, en vue de l'exercice des droits d'accès, de rectification et d'effacement;
16. mette à disposition des versions papier des brochures d'information sur le SIS et permette de les obtenir auprès des autorités publiques;

17. veille, afin de renforcer les droits des personnes concernées, à ce que le ministère de l'intérieur fournisse une traduction non officielle, en anglais par exemple, des réponses données aux personnes concernées;
18. veille à ce que les sites web des directions de police provinciales fournissent des informations sur le SIS II et le VIS, y compris sur le traitement des données à caractère personnel y afférent, et comportent des liens renvoyant au site web de l'APD;
19. veille à ce que les informations relatives au traitement des données à caractère personnel du VIS soient aisément accessibles sur les sites web du ministère des affaires européennes et internationales ainsi que des consulats et des ambassades, et à ce que ces sites contiennent des liens renvoyant au site web de l'APD;
20. veille à ce que l'APD fournisse les mêmes informations sur l'obligation de la personne concernée de démontrer son identité sur son site web (en allemand et en anglais) et dans les formulaires de demande d'accès destinés à la personne concernée;
21. veille à ce que l'APD fournisse sur son site web (en allemand et en anglais) des formulaires types spécifiques de demande de rectification et d'effacement des données du SIS et du VIS;
22. veille à ce que l'APD fournisse dans la version anglaise de son site web des informations sur le délai de réclamation, visé à l'article 24, paragraphe 4, de la loi sur la protection des données à caractère personnel.

Fait à Bruxelles, le

Par le Conseil

Le président / La présidente