Conseil de
l'Union européenne

Bruxelles, le 14 mai 2018
(OR. en)

8792/18

Dossier interinstitutionnel:
2018/0051 (NLE)

SCH-EVAL 102
COMIX 244

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	14 mai 2018
Destinataire:	délégations
Nº doc. préc.:	8285/18
Objet:	Décision d'exécution du Conseil arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2017 de l'application, par le **Portugal**, 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 2017 de l'application, par le Portugal, 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 14 mai 2018.

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.

ANNEXE

Décision d'exécution du Conseil arrêtant une

RECOMMANDATION

pour remédier aux manquements constatés lors de l'évaluation de 2017 de l'application, par le Portugal, 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 au Portugal des mesures correctives pour remédier aux manquements constatés lors de l'évaluation de Schengen effectuée en 2017 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 des manquements constatés lors de l'évaluation a été adopté par la décision d'exécution C(2018) 1190 de la Commission .

(2) En ce qui concerne les bonnes pratiques, l'équipe sur place s'est félicitée de l'investissement soutenu de l'autorité chargée de la protection des données dans la formation de son personnel technique.

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

(3) Eu égard à l'importance que revêt le respect de l'acquis de Schengen, notamment en ce qui concerne l'obligation de garantir et de réaliser une surveillance effective et de veiller à la mise en œuvre des mesures de sécurité nécessaires, priorité devrait être donnée à la mise en œuvre des recommandations 1, 4, 14, 17 et 22 formulées ci-dessous.

(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) nº 1053/2013, dans un délai de trois mois à compter de l'adoption de la présente décision, le Portugal élabore un plan d'action destiné à remédier aux manquements constatés dans le rapport d'évaluation et le soumet à la Commission et au Conseil,

RECOMMANDE ce qui suit:

le Portugal devrait:

Autorité de contrôle de la protection des données

1. allouer des ressources financières et humaines suffisantes à l'Autorité chargée de la protection des données (APD), afin qu'elle soit en mesure de s'acquitter de toutes les tâches qui lui sont confiées dans le cadre de l'acquis relatif au système d'information Schengen de deuxième génération (SIS II) et au système d'information sur les visas (VIS), en tenant compte également de l'accroissement futur des responsabilités;

2. afin de mieux garantir l'indépendance complète de l'APD, accorder à celle-ci l'autonomie financière dont elle a besoin pour exécuter son budget annuel ainsi que l'autonomie en matière de recrutement de son personnel en alignant au minimum les règles en la matière sur celles applicables à d'autres autorités indépendantes au Portugal;

3. veiller à ce que l'APD mène à bien sans retard la procédure relative à l'adoption des rapports à l'issue de l'inspection portant sur le traitement des données à caractère personnel dans le cadre du SIS II;

4. veiller à ce que l'APD achève sans retard l'audit du VIS;

Droits des personnes concernées

5. veiller à ce que les personnes concernées soient informées de leurs droits dans le cadre du SIS II sur le site web du Serviço de Estrangeiros e Fronteiras (service des étrangers et des frontières, SEF);

6. veiller à ce que les personnes concernées, qui ont demandé l'accès à leurs données à caractère personnel, soient informées des catégories de données réellement traitées dans le SIS II;

7. veiller à ce que les personnes concernées reçoivent des informations claires sur l'identité du responsable du traitement des données lors du traitement de leurs données à caractère personnel dans le cadre de la délivrance de visas Schengen;

Système d'information sur les visas

8. clarifier la situation concernant la fonction de responsable du traitement des données à caractère personnel dans le cadre du N.VIS [englobant les applications utilisées à la fois par le ministère des affaires étrangères (MAE), le SEF et les centres de données y afférents], en clarifiant notamment le rôle du MAE et en précisant la répartition des responsabilités en matière de traitement des données à caractère personnel entre le SEF et le MAE;

9. veiller à ce que le MAE réalise des activités de surveillance systématiques prévoyant l'évaluation constructive des aspects liés au traitement des données à caractère personnel par le prestataire de services extérieur (PSE). À cet égard, le Portugal est encouragé à étoffer le questionnaire que le MAE envoie au PSE afin de couvrir de façon plus détaillée les aspects relatifs à la protection des données et à renforcer les activités de surveillance du MAE à l'égard de la protection des données réalisées par le PSE et le sous-traitant, selon le cas;

10. prévoir une procédure qui permet de vérifier les réponses fournies par le SIS II au cours de la procédure de demande de visa;

11. veiller à ce que les mots de passe de tous les utilisateurs du N.VIS soient cryptés;

12. veiller à ce que le SEF et le MAE analysent régulièrement les fichiers journaux afin de garantir le contrôle de la protection des données;

13. veiller à ce que le MAE réalise régulièrement un autocontrôle du traitement des données à caractère personnel dans le système informatique (RPV) et le centre de données y afférent;

14. veiller à ce que le MAE adopte sans retard un plan de sécurité pour le RPV et le centre de données y afférent;

15. mettre entièrement en œuvre la décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, et veiller à ce que l'accès aux données du N.VIS soit conforme aux conditions et à la procédure qui y sont établies;

16. veiller à ce que le PSE supprime les données à caractère personnel des demandeurs qu'il conserve dans ses systèmes en respectant les délais mentionnés à l'annexe X, partie A, point d), du code des visas, qui requiert que ces données soient effacées immédiatement après leur transmission au consulat;

Système d'information Schengen II

17. prévoir pour le N.SIS II un site de secours complet possédant toutes les fonctionnalités, notamment la connexion aux infrastructures de communication de s-Testa;

18. préciser les responsabilités entre les parties intervenant dans le traitement des données du N.SIS II, à savoir le responsable du traitement des données et les autorités ayant accès au SIS.II (autorités utilisatrices) en ce qui concerne la sécurité informatique, ainsi que le contrôle et l'autocontrôle de celle-ci, par exemple en concluant des accords entre le responsable du traitement des données et les autorités ayant accès au SIS II;

19. appliquer une gestion de l'utilisateur qui prévoit un autocontrôle efficace grâce aux journaux centraux du responsable du traitement des données du N.SIS II sans qu'il soit nécessaire de consulter les journaux des autorités utilisatrices;

20. veiller à ce que le SEF analyse régulièrement les fichiers journaux afin de garantir le contrôle de la protection des données;

21. veiller à ce que les environnements informatiques utilisés par les utilisateurs ayant un accès très étendu au N.SIS ou des droits éditoriaux dans celui-ci (tels que les membres du bureau Sirene) soient logiquement ou physiquement séparés de l'accès à l'internet;

22. veiller à ce que le responsable du traitement des données crypte les bandes de sauvegarde et les disques durs du N.SIS;

23. veiller à ce que les profils d'utilisateur ayant un accès très étendu aux données du N.SIS ou des droits éditoriaux dans celui-ci (tels que les membres du bureau Sirene) soient sécurisés par un mécanisme obligatoire d'authentification à deux facteurs;

24. veiller à ce que le SEF renforce ses activités en matière d'autocontrôle du traitement des données à caractère personnel dans le N.SIS et réalise régulièrement cet autocontrôle; le Portugal est encouragé à octroyer des ressources humaines et financières suffisantes au SEF afin d'assurer un autocontrôle et une sécurité informatique efficaces et continus en particulier en veillant à pourvoir le poste d'agent à la sécurité informatique au sein de la division des technologies de l'information du SEF;

Sensibilisation du public

25. veiller à ce que le site web du SEF comporte des liens appropriés vers le site web de l'APD.

Fait à Bruxelles, le

Par le Conseil
Le président