COM(2019) 28 final LIMITE

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2018/2019

Reçu à la Présidence de l'Assemblée nationale
le 07 février 2019

Enregistré à la Présidence du Sénat
le 07 février 2019

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

Proposition de décision d'exécution du Conseil arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2017 de l'application, par l'Espagne, de l'acquis de Schengen dans le domaine de la protection des données

E 13801

Conseil de
l'Union européenne

Bruxelles, le 5 février 2019
(OR. en)

6068/19

Dossier interinstitutionnel:
2019/0015 (NLE)

LIMITE

SCH-EVAL 18
DATAPROTECT 25
COMIX 64

PROPOSITION

Origine:	Pour le secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, directeur
Date de réception:	4 février 2019
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2019) 28 final
Objet:	Proposition de DÉCISION D'EXÉCUTION DU CONSEIL arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2017 de l'application, par **l'Espagne**, de l'acquis de Schengen dans le domaine de la **protection des données**

Les délégations trouveront ci-joint le document COM(2019) 28 final.

p.j.: COM(2019) 28 final

COMMISSION
EUROPÉENNE

Bruxelles, le 4.2.2019
COM(2019) 28 final

2019/0015 (NLE)

LIMITED

Proposition de

DÉCISION D'EXÉCUTION DU CONSEIL

arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2017 de l'application, par l'Espagne, de l'acquis de Schengen dans le domaine de la protection des données

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Le 7 octobre 2013, le Conseil a adopté le règlement (UE) nº 1053/2013 portant création d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen[1]. Conformément audit règlement, la Commission a mis en place un programme d'évaluation pluriannuel pour 2014-2019[2] et un programme d'évaluation annuel pour 2017[3], comprenant des plans détaillés pour les inspections sur place dans les États membres devant faire l'objet d'une évaluation, les domaines à évaluer et les sites à inspecter.

Les domaines à évaluer couvrent tous les aspects de l'acquis de Schengen: la gestion des frontières extérieures, la politique de visas, le système d'information Schengen, la protection des données, la coopération policière, la coopération judiciaire en matière pénale et l'absence de contrôle aux frontières intérieures. En outre, il est tenu compte, dans toutes les évaluations, des questions relatives aux droits fondamentaux et du fonctionnement des autorités qui appliquent les parties concernées de l'acquis de Schengen.

Sur la base des programmes pluriannuel et annuel, une équipe composée d'experts des États membres et de la Commission a, entre le 1er et le 6 octobre 2017, évalué la mise en œuvre, par l'Espagne, des règles en matière de protection des données. Son rapport d'évaluation[4] présente ses constatations et appréciations, y compris les meilleures pratiques et les éventuels manquements constatés au cours de l'évaluation.

En parallèle, l'équipe d'experts a formulé des recommandations relatives aux mesures correctives visant à remédier à ces manquements.

La présente proposition tient compte de ces recommandations.

Dans ce contexte, la présente proposition de décision d'exécution du Conseil arrêtant une recommandation vise à garantir que l'Espagne applique de manière correcte et effective toutes les règles de Schengen relatives à la protection des données.

• Cohérence avec les dispositions existantes dans le domaine d'action

La présente recommandation vise à mettre en œuvre les dispositions existantes dans le domaine d'action.

• Cohérence avec les autres politiques de l'Union

La présente recommandation n'a pas de lien avec les autres politiques clés de l'Union.

---

1 JO L 295 du 6.11.2013, p. 27.

2 Décision d'exécution C(2014) 3683 de la Commission du 18 juin 2014 établissant le programme d'évaluation pluriannuel pour 2014-2019 conformément à l'article 5 du 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.

3 Décision d'exécution C(2016) 7387 de la Commission du 21 novembre 2016 établissant la première section du programme d'évaluation annuel pour 2017 conformément à l'article 6 du 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.

4 COM(2019) 280.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

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.

• Subsidiarité (en cas de compétence non exclusive)

L'article 15, paragraphe 2, du règlement (UE) nº 1053/2013 du Conseil prévoit expressément que la Commission présente une proposition au Conseil afin qu'il adopte des recommandations quant aux mesures correctives destinées à remédier à tout manquement constaté lors de l'évaluation. Une action à l'échelle de l'Union est nécessaire afin de renforcer la confiance mutuelle entre les États membres et d'assurer une meilleure coordination entre eux au niveau de l'Union en vue de garantir que les États membres appliquent effectivement l'ensemble des règles Schengen.

• Proportionnalité

L'article 15, paragraphe 2, du règlement (UE) nº 1053/2013 du Conseil traduit les compétences particulières attribuées au Conseil dans le domaine de l'évaluation mutuelle de la mise en œuvre des politiques de l'Union au sein de l'espace de liberté, de sécurité et de justice.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

• Évaluations ex post/bilans de qualité de la législation existante

s.o.

• Consultation des parties intéressées

Consultés conformément à l'article 14, paragraphe 5, et à l'article 21, paragraphe 2, du règlement (UE) n° 1053/2013 du Conseil, les États membres ont émis un avis positif sur le rapport d'évaluation lors de la réunion du comité Schengen du 29 novembre 2018.

• Obtention et utilisation d'expertise

s.o.

• Analyse d'impact

s.o.

• Réglementation affûtée et simplification

s.o.

• Droits fondamentaux

La protection des droits fondamentaux lors de l'application de l'acquis de Schengen a été prise en compte au cours du processus d'évaluation.

4. INCIDENCE BUDGÉTAIRE

s.o.

5. AUTRES ÉLÉMENTS

s.o.

2019/0015 (NLE)

Proposition de

DÉCISION D'EXÉCUTION DU CONSEIL

arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2017 de l'application, par l'Espagne, 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[5], 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 l'Espagne 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 manquements constatés lors de l'évaluation a été adopté par la décision d'exécution C(2019) 280 de la Commission.

(2) Sont considérées comme de bonnes pratiques les nombreuses activités du ministère des affaires étrangères et de la coopération («MAEC») liées à la supervision des consulats et du prestataire de services extérieur, notamment en matière de sécurité des données et de protection des données, ainsi que les activités d'autocontrôle du MAEC.

(3) Eu égard à l'importance que revêt le respect de l'acquis de Schengen sur la protection des données à caractère personnel en ce qui concerne le SIS II et le VIS, la priorité devrait être donnée à la mise en œuvre des recommandations 20 à 22, 28, 29 et 34 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, l'Espagne 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,

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

RECOMMANDE CE QUI SUIT:

l'Espagne devrait

Autorité de contrôle de la protection des données

1. afin de mieux garantir l'indépendance totale de l'Agencia Española de Protección de Datos (ci-après l'«AEPD»), veiller à ce que cette dernière soit en mesure de défendre sa proposition de budget devant le Parlement ou avant la transmission de cette proposition au Parlement pour examen et adoption;

2. veiller à ce que l'AEPD contrôle fréquemment la licéité du traitement des données à caractère personnel du SIS II et du VIS;

3. en ce qui concerne la supervision du SIS II, veiller à ce que la portée de l'audit effectué par les autorités compétentes en matière de protection des données soit élargie pour y inclure également les utilisateurs régionaux du SIS II, terminer l'audit en cours dans les meilleurs délais et faire en sorte que ces audits complets soient effectués par les autorités compétentes en matière de protection des données au moins tous les quatre ans;

4. en ce qui concerne la supervision du VIS, veiller à ce que l'AEPD effectue un audit des opérations de traitement des données dans le système national du VIS tous les quatre ans au moins;

5. veiller à ce que le suivi des inspections effectuées par les autorités compétentes en matière de protection des données en ce qui concerne tant le SIS II que le VIS soit renforcé en fixant un délai spécifique pour la mise en œuvre des recommandations ou en demandant au responsable du traitement d'informer les autorités compétentes en matière de protection des données de la mise en œuvre des recommandations dans un certain délai;

6. veiller à ce que l'AEPD mène à bien sans tarder la procédure relative à l'adoption des rapports à l'issue des inspections portant sur le traitement des données à caractère personnel dans le cadre du SIS II et du VIS;

Droits des personnes concernées — SIS II

7. veiller à ce que le responsable du traitement du SIS II fournisse, sur son site internet, des informations facilement accessibles sur la procédure à suivre pour l'exercice des droits des personnes concernées ainsi que des formulaires types à cette même fin. Le site internet du responsable du traitement devrait donc contenir un hyperlien renvoyant directement au site internet de l'AEPD;

8. veiller à ce qu'en réponse aux demandes des personnes concernées, le bureau SIRENE fournisse des informations sur les mécanismes de plainte;

9. fournir aux personnes concernées des moyens sécurisés pour la transmission électronique de leurs demandes et des pièces justificatives (et en particulier des moyens sécurisés pour la fourniture de copies de documents d'identité);

10. mettre en place une procédure écrite interne concernant la manière de traiter les demandes portant sur l'exercice des droits des personnes concernées dans le cadre du SIS II afin de garantir la continuité des opérations pour le traitement de ces demandes;

11. encourager l'AEPD à publier le formulaire type pour l'exercice des droits des personnes concernées dans le cadre du SIS II dans d'autres langues, telles que l'anglais et le français, de manière à ce que les personnes concernées puissent y accéder facilement, et ajouter un hyperlien sur le site internet de l'AEPD vers le site internet du responsable du traitement du SIS II;

Droits des personnes concernées - VIS

12. encourager l'AEPD à publier le formulaire type pour l'exercice des droits des personnes concernées dans le cadre du VIS, y compris dans d'autres langues telles que l'anglais et le français, de manière à ce qu'il soit facilement accessible par les personnes concernées;

13. veiller à ce que le ministère des affaires étrangères et de la coopération («MAEC») publie sur son site internet un formulaire type facilement accessible pour l'exercice des droits des personnes concernées, y compris dans d'autres langues (telles que l'anglais et le français). Le site internet du responsable du traitement devrait donc contenir un hyperlien renvoyant directement au site internet de l'AEPD;

14. veiller à ce que le MAEC fournisse des informations sur les mécanismes de plainte en réponse aux demandes des personnes concernées;

15. en ce qui concerne les visas délivrés par la police nationale aux frontières, veiller à ce que cette dernière fournisse, sur son site internet, des informations facilement accessibles sur la procédure à suivre pour l'exercice des droits des personnes concernées ainsi que des formulaires types à cette même fin. Le site internet de la police nationale devrait donc contenir un hyperlien renvoyant directement au site internet de l'AEPD;

16. en ce qui concerne les visas délivrés par la police nationale aux frontières, mettre en place une procédure écrite interne sur la manière de traiter les demandes portant sur l'exercice des droits de la personne concernée dans le cadre du SIS II afin de garantir la continuité des opérations pour le traitement de ces demandes;

17. veiller à ce que des informations claires sur l'identité du responsable du traitement soient fournies aux personnes concernées pour ce qui est du traitement de leurs données à caractère personnel dans le cadre de la délivrance de visas Schengen;

Système d'information sur les visas

18. clarifier la situation concernant la fonction de responsable du traitement des données à caractère personnel dans le N.VIS (englobant les applications utilisées à la fois par le MAEC et par la police nationale pour les visas délivrés aux frontières), en précisant notamment le rôle de la police nationale et la répartition des responsabilités en matière de traitement des données à caractère personnel entre la police nationale et le MAEC;

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

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

21. veiller à ce que les données qui se trouvent sur le serveur N.VIS et sur les bandes de sauvegarde soient cryptées;

22. garantir à tout moment un niveau élevé de sécurité physique de la salle des serveurs VIS, notamment par la maintenance et la réparation adéquates des dispositifs de sécurité concernant l'accès à la salle des serveurs;

23. mettre pleinement 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 Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves et veiller à ce que les registres répertoriant l'accès aux données du N.VIS respectent les exigences qui sont établies dans cette décision, en veillant notamment à ce que ces registres indiquent l'identité

des utilisateurs demandant un accès aux données du VIS, le motif précis de cet accès et la référence du fichier national.

24. veiller à ce que les données stockées dans le N.VIS ne soient pas conservées plus de cinq ans, conformément à l'article 23 du règlement (CE) n° 767/2008 du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS);

25. veiller à ce que les registres des opérations liées aux données du VIS effectuées dans toutes les applications pertinentes pour le traitement de ces données (et notamment les applications SIVICO, AVANCE et ADEXTTRA) ne soient pas conservés plus d'un an après l'expiration de la période de conservation visée à l'article 23, paragraphe 1, du règlement VIS, conformément aux délais prévus à l'article 34, paragraphe 2, du règlement VIS et à l'article 16 de la décision du Conseil concernant le VIS. En ce qui concerne les registres liés au VIS, veiller à ce qu'ils soient conservés pendant une période d'un an après l'expiration de la période de conservation visée à l'article 23, paragraphe 1, du règlement VIS;

25. veiller à ce que le prestataire de services extérieur supprime les données à caractère personnel des demandeurs qu'il conserve dans ses systèmes dans les délais visés à l'annexe X, partie A, point d), du code des visas, qui requiert que ces données soient supprimées immédiatement après leur transmission au consulat;

27. veiller à ce que le MAEC et la police nationale vérifient régulièrement les registres de toutes les applications associées au traitement des données du VIS par le MAEC et d'Adexttra afin de garantir le contrôle de la protection des données;

Système d'information Schengen II

28. mettre sur pied de façon prioritaire un site de secours complet et veiller à ce que les bandes de sauvegarde soient stockées séparément de toute urgence;

29. prévoir des mesures de protection supplémentaires (c'est-à-dire une authentification à deux facteurs) pour les profils d'utilisateur disposant de droits d'accès ou de modification très étendus en ce qui concerne les données du N.SIS II (utilisateurs et administrateurs SIRENE);

30. renforcer le contrôle de l'accès au bureau SIRENE en veillant à ce que ses locaux soient accessibles uniquement aux fonctionnaires de police autorisés;

31. veiller à ce que les utilisateurs finaux bénéficient de formations régulières et continues axées sur la protection des données dans le cadre du SIS II;

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

33. veiller à ce que le responsable du traitement du N.SIS prévoie une politique globale de sécurité en matière de données du SIS II, qui couvre également les mesures de sécurité informatique pour l'accès aux données du N.SIS II, y compris les mesures de contrôle et d'autocontrôle et les mesures de formation des autorités ayant accès au SIS II (autorités utilisatrices). L'Espagne est encouragée à préciser les responsabilités entre les parties intervenant dans le traitement des données du N.SIS II, à savoir le responsable du traitement et les 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 et les autorités ayant accès au SIS II;

34. veiller à ce que le responsable du traitement du SIS II adopte sans attendre un plan de sécurité;

35. veiller à ce que le responsable du traitement du SIS II s'acquitte régulièrement des activités liées à l'autocontrôle du traitement des données à caractère personnel dans le N.SIS;

36. veiller à ce que le responsable du traitement du SIS II analyse régulièrement les registres afin de garantir le contrôle de la protection des données;

37. veiller à ce que les registres répertoriant les demandes concernant des données du N.SIS ne soient pas conservés pendant plus de 3 ans après leur création, conformément à l'article 12, paragraphe 4, du règlement relatif au SIS II et à la décision du Conseil relative au SIS II.

Fait à Bruxelles, le

Par le Conseil
Le président