COM(2019) 29 final LIMITE

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2018/2019

Reçu à la Présidence de l'Assemblée nationale
le 12 février 2019

Enregistré à la Présidence du Sénat
le 12 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 2018 de l'application, par la Finlande, de l'acquis de Schengen dans le domaine de la protection des données

E 13813

Conseil de
l'Union européenne

Bruxelles, le 7 février 2019
(OR. en)

6240/19

LIMITE

SCH-EVAL 21
DATAPROTECT 35
COMIX 72

Dossier interinstitutionnel:
2019/0032 (NLE)

PROPOSITION

Origine:	Pour le secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, directeur
Date de réception:	6 février 2019
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2019) 29 final
Objet:	Proposition de DÉCISION D'EXÉCUTION DU CONSEIL arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2018 de l'application, par la **Finlande**, de l'acquis de Schengen dans le domaine de la **protection des données**

Les délégations trouveront ci-joint le document COM(2019) 29 final.

p.j.: COM(2019) 29 final

COMMISSION
EUROPÉENNE

Bruxelles, le 6.2.2019
COM(2019) 29 final

2019/0032 (NLE)

LIMITED

Proposition de

DÉCISION D'EXÉCUTION DU CONSEIL

arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2018 de l'application, par la Finlande, 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[1] portant création d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen. 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 2018[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 les 10 et 15 juin 2018, évalué la mise en œuvre, par la Finlande, des règles en matière de protection des données. Son rapport d'évaluation[4] présente ses constatations et appréciations, y compris les bonnes 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 uniquement de ces recommandations.

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

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

Les présentes recommandations visent à mettre en œuvre les dispositions existantes dans le domaine d'action.

• Cohérence avec les autres politiques de l'Union

Les présentes recommandations n'ont 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(2017) 7000 de la Commission du 7 novembre 2017 établissant la première section du programme d'évaluation annuel pour 2018 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 C(2019) 290.

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

Conformément à l'article 14, paragraphe 5, et à l'article 21, paragraphe 2, du règlement (UE) nº 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.

2019/0032 (NLE)

Proposition de

DÉCISION D'EXÉCUTION DU CONSEIL

arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2018 de l'application, par la Finlande, 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 la Finlande des mesures correctives pour remédier aux manquements constatés lors de l'évaluation de Schengen réalisée 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 bonnes pratiques et des manquements constatés lors de l'évaluation a été adopté par la décision d'exécution de la Commission C(2019) 290.

(2) Sont considérées comme de bonnes pratiques, entre autres, les mesures exceptionnelles de sécurité et d'intervention d'urgence au centre informatique de Rovaniemi, les exigences d'authentification multiniveaux imposées aux fonctionnaires de police, la formation spécifique à la protection des données dispensée au personnel de police et le fait que la police réponde à toutes les demandes des personnes concernées, indépendamment de la langue dans laquelle elles ont été formulées.

(3) Eu égard à l'importance que revêt le respect de l'acquis de Schengen concernant la protection des données dans le contexte du système d'information Schengen de deuxième génération (SIS II), il convient d'accorder la priorité aux recommandations 16 et 21.

(4) Eu égard à l'importance que revêt le respect de l'acquis de Schengen concernant la protection des données dans le contexte du système d'information sur les visas (VIS), il convient d'accorder la priorité aux recommandations 5 à 10.

(5) En outre, afin de garantir la sécurité juridique, il est essentiel d'adopter rapidement des lois nationales mettant en œuvre le règlement général sur la protection des données (UE) 2016/679 et transposant la directive sur la protection des données (UE) 2016/680, y compris l'acte fondateur concernant le médiateur chargé de la protection

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

des données qui garantit son indépendance absolue et renforce ses activités de surveillance.

(6) 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, la Finlande 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:

La Finlande devrait:

Autorité de contrôle de la protection des données

(1) garantir l'indépendance absolue du médiateur chargé de la protection des données en prévoyant que son chef de bureau soit désigné par le médiateur lui-même, et non par le ministère de la justice;

(2) veiller à ce que les activités de surveillance du médiateur chargé de la protection des données concernant le SIS II prévoient des contrôles réguliers des signalements introduits dans le SIS II;

(3) veiller à ce que les activités de surveillance du médiateur chargé de la protection des données concernant le VIS prévoient des contrôles réguliers des postes consulaires;

(4) veiller à ce que le plan d'inspection pluriannuel du médiateur chargé de la protection des données comporte d'autres activités d'inspection que les audits obligatoires du SIS II et du VIS;

Système d'information sur les visas

(5) veiller à ce que le prestataire de services extérieur ne puisse envoyer des données concernant les demandeurs de visa que par VPN sécurisé et sous forme cryptée;

(6) veiller à ce que les données concernant les demandeurs de visa ne soient pas conservées sur les serveurs du prestataire de services extérieur;

(7) veiller à ce que le prestataire de services extérieur crée d'autres moyens pour la transmission de données depuis la Chine et la Russie vers le Royaume-Uni;

(8) signer l'accord de protection des données avec le prestataire de services extérieur et clarifier les responsabilités respectives du ministère des affaires étrangères (MAE), en tant que responsable du traitement des données en ce qui concerne le VIS, et le prestataire de services extérieur, en tant que sous-traitant des données;

(9) veiller à ce que les fichiers-journaux soient conservés par le MAE et analysés de manière régulière, en vue de l'autocontrôle en matière de protection des données, et mettre en place des procédures d'autocontrôle du traitement des données à caractère personnel dans SUVI sur une base régulière;

(10) veiller à ce que le MAE exerce un contrôle effectif sur le système national d'information sur les visas;

(11) créer un site de récupération pour SUVI à un endroit différent de celui où est situé le serveur principal de SUVI;

(12) veiller à ce que le MAE tienne le répertoire des utilisateurs d'ELVIS;

(13) veiller à ce que l'accord de protection des données entre le MEA et Tieto réponde aux exigences sur les accords entre responsable du traitement et sous-traitant prévues par le règlement général sur la protection des données (UE) 2016/679;

(14) veiller à ce que le MAE élabore une formation à l'intention de son personnel et des employés des consulats ou ambassades, axée spécifiquement sur la protection des données à caractère personnel liées au VIS;

(15) veiller à ce que le délégué à la protection des données du MAE participe au traitement des données à caractère personnel, au traitement des dossiers et à la formation du personnel;

Système d'information Schengen

(16) veiller à ce que la police effectue un autocontrôle sur une base régulière, en particulier l'autocontrôle des fichiers-journaux;

(17) définir clairement le rôle du délégué à la protection des données et garantir la participation de ce dernier aux travaux sur la protection des données, tout en veillant à l'amélioration de la relation entre les différentes entités de la police chargées de la protection des données (délégué à la protection des données, groupe de protection des données, coordinateurs de la protection des données et groupe de coopération en matière de protection des données);

(18) garantir un système intégré qui présente les signalements nationaux et internationaux simultanément à l'utilisateur final sur demande;

(19) veiller à ce que les photographies, les empreintes digitales, et d'autres données obligatoires du SIS II soient intégrées dans les signalements SIS II de manière sécurisée;

(20) clarifier la répartition des tâches en matière de sécurité informatique au sein de la police;

(21) générer des fichiers-journaux nationaux du SIS II au niveau central et faire en sorte que la justification de la demande puisse être établie à partir du fichier-journal;

Droits des personnes concernées et actions de sensibilisation

(22) garantir des options alternatives pour l'exercice effectif des droits de la personne concernée en matière d'accès, de rectification et d'effacement de données du SIS II et du VIS;

(23) réduire le montant de la taxe, à partir de la deuxième demande d'accès, pour toute demande effectuée dans un délai de 12 mois, afin de permettre aux personnes concernées d'avoir un droit d'accès effectif à leurs données SIS II;

(24) apporter une réponse aux personnes concernées lorsqu'elles exercent leur droit d'accès indirect dans un délai qui est conforme à l'acquis de Schengen;

(25) garantir la disponibilité d'un modèle de lettre relative à l'exercice du droit de rectification et d'effacement des données du SIS II et du VIS;

(26) garantir la participation des délégués respectifs à la protection des données dans le cadre du traitement des demandes des personnes relatives à l'exercice de leurs droits par rapport aux données du SIS II et du VIS;

(27) garantir l'existence d'un fichier central concernant les demandes des personnes concernées au sujet des données du SIS II;

(28) fournir au médiateur chargé de la protection des données les statistiques relatives à l'exercice des droits de la personne concernée ayant trait au SIS II, sur une base annuelle;

(29) fournir des informations claires aux personnes concernées au sujet de l'exercice de leurs droits, lorsque ce droit est limité en vertu de la législation;

(30) fournir des informations sur les droits des personnes concernées en ce qui concerne le SIS II et le VIS et d'autres informations générales sur la protection des données, sur le site internet du médiateur chargé de la protection des données, des informations sur les droits des personnes concernées en ce qui concerne le VIS sur le site internet du MEA et des informations générales sur la protection des données facilement accessibles sur le site web du MEA ainsi que sur les sites internet des ambassades et des postes consulaires.

Fait à Bruxelles, le

Par le Conseil
Le président