DÉCISION (UE, Euratom) 2018/559 DE LA COMMISSION

du 6 avril 2018

établissant les règles d'application de l'article 6 de la décision (UE, Euratom) 2017/46 sur la sécurité des systèmes d'information et de communication au sein de la Commission européenne

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 249,

vu le traité instituant la Communauté européenne de l'énergie atomique,

vu la décision (UE, Euratom) 2017/46 de la Commission du 10 janvier 2017 sur la sécurité des systèmes d'information et de communication au sein de la Commission européenne ([1]), et notamment son article 6,

considérant ce qui suit:

(1) L'adoption de la décision (UE, Euratom) 2017/46 rend nécessaires le réexamen, la mise à jour et la consolidation, par la Commission, des modalités d'exécution découlant de l'abrogation de la décision C(2006) 3602 de la Commission relative à la sécurité des systèmes d'information utilisés par les services de la Commission.

(2) Dans le strict respect des règles de procédure internes, le membre de la Commission chargé des questions de sécurité a été habilité à établir des règles d'application conformément à l'article 13 de la décision (UE, Euratom) 2017/46 ([2]).

(3) Il convient dès lors d'abroger les règles d'application de la décision C(2006) 3602,

A ADOPTÉ LA PRÉSENTE DÉCISION:

CHAPITRE 1

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. L'objet et le champ d'application de la présente décision sont indiqués à l'article 1er de la décision (UE, Euratom) 2017/46.

2. Les dispositions de la présente décision s'appliquent à tous les systèmes d'information et de communication (SIC). Cependant, les responsabilités définies dans la présente décision ne s'appliquent pas aux SIC traitant des informations classifiées de l'Union européenne. Les responsabilités correspondantes concernant ces systèmes sont définies par le propriétaire des systèmes et l'autorité de sécurité de la Commission, conformément à la décision (UE, Euratom) 2015/444 de la Commission ([3]).

3. Le chapitre 2 de la présente décision donne un aperçu de la mise en œuvre concrète de l'organisation et des responsabilités relatives à la sécurité informatique. Le chapitre 3 de la présente décision présente une synthèse des processus liés à l'article 6 de la décision (UE, Euratom) 2017/46.

Article 2

Définitions

Les définitions figurant à l'article 2 de la décision (UE, Euratom) 2017/46 s'appliquent à la présente décision. Aux fins de la présente décision, les définitions suivantes sont également applicables:

1. «Autorité d'agrément cryptographique» (AAC): fonction assurée par l'autorité de sécurité de la Commission qui relève de la compétence du directeur général des ressources humaines et de la sécurité.

([1]) JO L 6 du 11.1.2017, p. 40.
([2]) Décision C(2017) 7428 final de la Commission du 8 novembre 2017 octroyant une habilitation concernant l'adoption des règles d'application, des normes et des lignes directrices relatives à la sécurité des systèmes d'information et de communication au sein de la Commission européenne.
([3]) Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53).

2. «Connexion aux réseaux externes»: toute liaison de communication électronique entre le réseau interne de la Commission et tout autre réseau, y compris l'internet. Cette définition exclut les réseaux tiers fournis en vertu d'un contrat en vue d'être intégrés au réseau interne de la Commission.

3. «Clé sous seing privé»: procédure de stockage des copies de clés cryptographiques auprès d'un ou de plusieurs dépositaires, afin de garantir la séparation des fonctions et de permettre une récupération en cas de perte de la copie opérationnelle. Les clés peuvent être divisées en plusieurs parties, lesquelles sont remises à des dépositaires différents afin de garantir qu'aucun d'entre eux ne possède la clé dans son intégralité.

4. «RASCI»: acronyme correspondant à une répartition des responsabilités fondée sur les indicateurs d'attribution suivants:

   a) «*responsible*» (R): qui a l'obligation d'agir et de prendre des décisions pour atteindre les résultats souhaités;

   b) «*accountable*» (A): qui doit répondre d'actes, de décisions et de performances;

   c) «*supports*» (S): qui a l'obligation de travailler avec la personne chargée d'accomplir la tâche en question;

   d) «*consulted*» (C): qui est sollicité pour donner un conseil ou un avis;

   e) «*informed*» (I): qui est tenu au courant des informations pertinentes.

CHAPITRE 2

ORGANISATION ET RESPONSABILITÉS

Article 3

Rôles et responsabilités

Les rôles et responsabilités se rapportant aux articles 4 à 8 de la présente décision sont définis à l'annexe conformément au modèle RASCI.

Article 4

Alignement sur la politique de sécurité de l'information de la Commission

1. La direction générale des ressources humaines et de la sécurité examine la politique de sécurité informatique de la Commission ainsi que les normes et lignes directrices connexes afin de s'assurer de leur conformité aux politiques générales de la Commission en matière de sécurité, et notamment à la décision (UE, Euratom) 2015/443 de la Commission ([1]) et à la décision (UE, Euratom) 2015/444.

2. La direction générale des ressources humaines et de la sécurité peut, si d'autres services de la Commission en font la demande, procéder à un examen des politiques ou de la documentation de ces services se rapportant à la sécurité informatique, afin de s'assurer qu'elles respectent la politique de sécurité de l'information de la Commission. Le chef du service de la Commission concerné veille à mettre fin à toute éventuelle non-conformité.

3. En sa qualité de responsable de la sécurité de l'information, la direction générale des ressources humaines et de la sécurité coopère avec la direction générale de l'informatique afin de s'assurer que les processus de sécurité informatique tiennent pleinement compte de la classification et des principes de sécurité tels que définis dans la décision (UE, Euratom) 2015/443, et notamment dans ses articles 3 et 9.

CHAPITRE 3

PROCESSUS DE SÉCURITÉ INFORMATIQUE

Article 5

Technologies de chiffrement

1. L'utilisation de technologies de chiffrement pour la protection des informations classifiées de l'Union européenne (ICUE) est conforme à la décision (UE, Euratom) 2015/444.

2. Les décisions relatives à l'utilisation de technologies de chiffrement pour la protection des données non classifiées de l'Union européenne sont prises par le propriétaire de chaque SIC en tenant compte à la fois des risques que le chiffrement est censé atténuer et de ceux que son utilisation entraîne.

3. Toute utilisation des technologies de chiffrement est soumise à l'accord préalable de l'AAC, à moins que le chiffrement ne soit exclusivement utilisé pour protéger la confidentialité des données non classifiées de l'Union européenne en transit et qu'il n'emploie des protocoles standard de communication par réseau.

([1]) Décision (UE, Euratom) 2015/443 de la Commission du 13 mars 2015 relative à la sécurité au sein de la Commission (JO L 72 du 17.3.2015, p. 41).

4. Sous réserve de l'exception notée au paragraphe 3 du présent article, les services de la Commission veillent à ce que les sauvegardes de toutes les clés de déchiffrement soient stockées selon la procédure de la «clé sous seing privé» à des fins de récupération des données stockées au cas où la clé de déchiffrement ne serait pas disponible. La récupération de données chiffrées à l'aide de sauvegardes de clés de déchiffrement n'est effectuée que lorsqu'elle est autorisée conformément à la norme définie par l'AAC.

5. Les demandes d'autorisation relatives à l'utilisation des technologies de chiffrement sont documentées en bonne et due forme et contiennent des informations concernant le SIC et les données à protéger, les technologies à utiliser et les procédures d'exploitation de sécurité correspondantes. Ces demandes d'autorisation sont signées par le propriétaire du système.

6. Les demandes d'autorisation relatives à l'utilisation des technologies de chiffrement sont évaluées par l'AAC conformément aux normes et exigences publiées.

Article 6

Inspections de sécurité informatique

1. La direction générale des ressources humaines et de la sécurité procède à des inspections de sécurité informatique afin de vérifier, d'une part, la conformité des mesures de sécurité informatique aux politiques de la Commission en matière de sécurité informatique et, d'autre part, l'intégrité de ces mesures de contrôle.

2. La direction générale des ressources humaines et de la sécurité peut effectuer une inspection de sécurité informatique:

a) de sa propre initiative;

b) à la demande du comité de pilotage de la sécurité informatique (CPSI);

c) à la demande d'un propriétaire de système;

d) à la suite d'un incident de sécurité; ou

e) après l'identification d'un risque élevé pour un système particulier.

3. Les propriétaires de données peuvent demander une inspection de sécurité informatique avant de stocker leurs informations dans un SIC.

4. Les résultats des inspections sont consignés dans un rapport officiel adressé au propriétaire du système, avec copie au responsable local de la sécurité informatique (*Local Informatics Security Officer*, LISO) et comportant des conclusions et des recommandations visant à améliorer la conformité du SIC à la politique de sécurité informatique. La direction générale des ressources humaines et de la sécurité signale au CPSI les principaux problèmes recensés et les recommandations formulées.

5. La direction générale des ressources humaines et de la sécurité surveille la mise en œuvre des recommandations.

6. Le cas échéant, les inspections de sécurité informatique comprennent l'inspection des services, locaux et équipements fournis au propriétaire du système, que ce soit par des prestataires de services internes ou externes.

Article 7

Accès depuis des réseaux externes

1. La direction générale des ressources humaines et de la sécurité fixe les règles dans une norme relative à l'autorisation des accès entre les SIC de la Commission et les réseaux externes.

2. Les règles distinguent différents types de connexion depuis des réseaux externes et définissent des règles de sécurité appropriées pour chaque type de connexion, en précisant s'il est nécessaire d'obtenir une autorisation préalable de l'autorité compétente, comme indiqué au paragraphe 4 du présent article.

3. Si nécessaire, l'autorisation est accordée dans le cadre d'une procédure officielle de demande et d'approbation. L'approbation est valable pendant une durée déterminée et doit être obtenue avant l'activation de la connexion.

4. La direction générale des ressources humaines et de la sécurité est responsable au premier chef de l'autorisation des demandes, mais peut, à son entière discrétion, déléguer la responsabilité d'autoriser certains types de connexion, conformément à l'article 17, paragraphe 3, de la décision (UE, Euratom) 2015/443 et aux conditions fixées au paragraphe 8.

5. L'entité délivrant l'autorisation peut imposer, à titre de condition préalable à l'approbation, des exigences de sécurité supplémentaires afin de protéger les SIC et les réseaux de la Commission contre les risques d'accès non autorisé ou d'autres atteintes à la sécurité.

6. La direction générale de l'informatique est le fournisseur standard de services de réseaux à la Commission. Tout autre service de la Commission exploitant un réseau qui n'est pas fourni par la direction générale de l'informatique doit obtenir l'accord préalable du CPSI. Le service de la Commission documente la justification opérationnelle de la demande et démontre que les mesures de contrôle des réseaux sont suffisantes pour répondre aux exigences en matière de contrôle des flux d'information entrants et sortants.

7. Le propriétaire d'un SIC définit les exigences de sécurité auxquelles est soumis l'accès externe à ce SIC et veille, avec l'aide du LISO, à la mise en œuvre de mesures appropriées pour protéger sa sécurité.

8. Les mesures de sécurité mises en œuvre pour les connexions depuis des réseaux externes reposent sur les principes du besoin d'en connaître et du moindre privilège, lesquels garantissent que chaque personne ne reçoit que les informations et les droits d'accès nécessaires à l'accomplissement de ses fonctions officielles pour la Commission.

9. Toutes les connexions depuis des réseaux externes sont filtrées et surveillées afin de déceler toute atteinte éventuelle à la sécurité.

10. Lorsque des connexions sont établies pour permettre l'externalisation d'un SIC, l'autorisation est subordonnée à l'aboutissement de la procédure décrite à l'article 8.

Article 8

Externalisation de SIC

1. Aux fins de la présente décision, un SIC est réputé être externalisé dès lors qu'il est fourni sur la base d'un contrat conclu avec un prestataire tiers et en vertu duquel le SIC est hébergé en dehors des locaux de la Commission. Cela comprend l'externalisation d'un ou de plusieurs SIC ou autres services informatiques, les centres de données situés en dehors des locaux de la Commission, ainsi que le traitement d'ensembles de données de la Commission par des services externes.

2. L'externalisation d'un SIC tient compte du niveau de sensibilité ou de la classification des informations traitées, comme suit:

a) Le SIC traitant des ICUE est homologué conformément à la décision (UE, Euratom) 2015/444 et l'autorité d'homologation de sécurité de la Commission (AHS) est consultée au préalable. Les systèmes assurant le traitement d'ICUE ne sont pas externalisés.

b) Le propriétaire d'un SIC traitant des données non classifiées de l'Union européenne met en œuvre des mesures proportionnées afin de répondre aux besoins de sécurité conformément aux obligations légales applicables ou selon le niveau de sensibilité des informations, en tenant compte des risques engendrés par l'externalisation. La direction générale des ressources humaines et de la sécurité peut imposer des exigences supplémentaires.

c) Les projets de développement externalisés tiennent compte du niveau de sensibilité du code développé ainsi que des données d'essai éventuellement utilisées pendant le développement.

3. Les principes suivants s'appliquent au SIC externalisés, en plus de ceux énoncés à l'article 3 de la décision (UE, Euratom) 2017/46:

a) les accords d'externalisation sont conçus de façon à éviter toute dépendance envers certains fournisseurs;

b) les accords portant sur la sécurité de l'externalisation réduisent autant que possible les possibilités, pour le personnel des prestataires tiers, d'accéder à des informations de la Commission ou de les modifier;

c) le personnel des prestataires tiers ayant accès à un SIC externalisé signe des accords de confidentialité;

d) l'externalisation d'un SIC est indiquée dans l'inventaire des SIC.

4. Le propriétaire du système doit, avec la participation du propriétaire des données:

a) évaluer et recenser les risques liés à l'externalisation;

b) établir des exigences de sécurité pertinentes;

c) consulter les propriétaires de tous les autres SIC connectés afin de veiller à l'inclusion de leurs exigences en matière de sécurité;

d) s'assurer que des exigences et des droits appropriés au regard de la sécurité figurent dans le contrat d'externalisation;

e) satisfaire à toute autre exigence définie dans la procédure détaillée, telle que mentionnée au paragraphe 8 du présent article.

Ces actions sont effectuées avant la signature du contrat ou de tout autre accord portant sur l'externalisation d'un ou de plusieurs SIC.

5. Les propriétaires de systèmes gèrent les risques liés à l'externalisation pendant la durée de vie du SIC afin de satisfaire aux exigences de sécurité définies.

6. Les propriétaires de systèmes veillent à ce que les prestataires tiers soient tenus de signaler immédiatement à la Commission tout incident de sécurité informatique affectant un SIC de la Commission qui est externalisé.

7. Le propriétaire du système doit veiller à la conformité du SIC, du contrat d'externalisation et des dispositifs de sécurité aux règles de la Commission en matière de sécurité de l'information et de sécurité informatique.

8. La direction générale des ressources humaines et de la sécurité fixe, dans une norme détaillée, les règles relatives aux responsabilités et aux activités visées aux paragraphes 1 à 7 conformément à l'article 10 ci-dessous.

CHAPITRE 4

DISPOSITIONS DIVERSES ET DISPOSITIONS FINALES

Article 9

Transparence

La présente décision est portée à la connaissance du personnel de la Commission et de toutes les personnes auxquelles elle s'applique, et elle est publiée au *Journal officiel de l'Union européenne*.

Article 10

Normes

1. Les dispositions de la présente décision sont, le cas échéant, décrites plus en détail dans des normes et/ou des lignes directrices devant être adoptées conformément à la décision (UE, Euratom) 2017/46 et à la décision C(2017) 7428. Les normes et les lignes directrices relatives à la sécurité informatique fournissent de plus amples détails sur les présentes règles d'application et la décision (UE, Euratom) 2017/46 pour certains domaines liés à la sécurité conformément à la norme ISO 27001:2013, annexe A. Ces normes et lignes directrices sont fondées sur les meilleures pratiques du secteur et choisies en fonction de l'environnement informatique de la Commission.

2. Si nécessaire, des normes sont élaborées conformément à la norme ISO 27001:2013, annexe A, dans les domaines suivants:

(1) organisation de la sécurité de l'information;

(2) sécurité des ressources humaines;

(3) gestion des actifs;

(4) contrôle des accès;

(5) cryptographie;

(6) sécurité physique et environnementale;

(7) sécurité opérationnelle;

(8) sécurité des communications;

(9) acquisition, développement et maintenance des systèmes;

(10) relations avec les fournisseurs;

(11) gestion des incidents de sécurité de l'information;

(12) aspects de la gestion de la continuité des activités relevant de la sécurité de l'information;

(13) conformité.

3. Le CPSI approuve les normes mentionnées aux paragraphes 1 et 2 du présent article avant leur adoption.

4. Les règles d'application de la décision C(2006) 3602 relatives au champ d'application de la présente décision sont abrogées.

5. Les normes et lignes directrices adoptées en vertu de la décision C(2006) 3602 du 16 août 2006 restent en vigueur, pour autant qu'elles ne soient pas en contradiction avec les présentes règles d'application, jusqu'à ce qu'elles soient abrogées ou remplacées par des normes ou lignes directrices adoptées en vertu de l'article 13 de la décision (UE, Euratom) 2017/46.

Article 11

Entrée en vigueur

La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 6 avril 2018.

Par la Commission,
au nom du président,
Günther OETTINGER
Membre de la Commission

ANNEXE

RÔLES ET RESPONSABILITÉS (RASCI)

Le modèle RASCI attribue des rôles à des entités sur la base des abréviations suivantes:

a) R — *Responsible* (qui a l'obligation d'agir)

b) A — *Accountable* (qui doit rendre des comptes)

c) S — *Supports* (qui doit soutenir)

d) C — *Consulted* (qui est sollicité pour donner un avis)

e) I — *Informed* (qui est tenu informé)

Rôle / Processus	CPSI	HR (DS)	Services de la Commission	Propriétaire du système	Propriétaire des données	LISO	DIGIT	Prestataires
Alignement sur la politique de la Commission en matière de sécurité de l'information		**R/A**	**S**				**S**	
Technologies de chiffrement		**C**	**A**	**R**	**I**	**C**		
Inspections de sécurité informatique	**I**	**A/R**		**S**	**I**	**I**	**S**	
Accès depuis des réseaux externes	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Externalisation de SIC		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Le CPSI est consulté en ce qui concerne l'exploitation de réseaux internes par tout service de la Commission autre que la direction générale de l'informatique.

[2] Le propriétaire d'un SIC externalisé est responsable et le propriétaire de tout autre SIC auquel est relié un SIC externalisé est consulté.