Procedure file

Informations de base

COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	2023/0108(COD)	En attente de la position du Conseil en 1ère lecture
Services de sécurité gérés Modification Règlement 2019/881 2017/0225(COD) Sujet 3.30.06 Technologies de l'information et de la communication, technologies numériques 3.30.07 Cybersécurité, politique cyberespace 3.30.25 Réseaux mondiaux et société de l'information, internet		

Acteurs principaux

Parlement européen	Commission au fond	Rapporteur(e)	Date de nomination
	ITRE Industrie, recherche et énergie		02/05/2023
		S&D CUTAJAR Josianne	
		Rapporteur(e) fictif/fictive	
		epp NIEBLER Angelika	
		renew europe. GROOTHUIS Bart	
		NIINISTÖ Ville	
		ECR TOŠENOVSKÝ Evžen	
	Commission pour avis	Rapporteur(e) pour avis	Date de nomination
	IMCO Marché intérieur et protection des consommateurs	Président au nom de la commission	23/05/2023
		CAVAZZINI Anna	
	LIBE Libertés civiles, justice et affaires intérieures	La commission a décidé de ne pas donner d'avis.	
Conseil de l'Union européenne			
Commission européenne	DG de la Commission	Commissaire	
	Réseaux de communication, contenu et technologies	BRETON Thierry	
Comité économique et social européen			

Evénements clés

18/04/2023	Publication de la proposition législative	COM(2023)0208	Résumé
01/06/2023	Annonce en plénière de la saisine de la commission, 1ère lecture		
25/10/2023	Vote en commission,1ère lecture		
25/10/2023	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d?un rapport adopté en commission		
26/10/2023	Dépôt du rapport de la commission, 1ère lecture	A9-0307/2023	Résumé
08/11/2023	Décision de la commission parlementaire d?engager des négociations interinstitutionnelles annoncée en plénière (Article 71)		
09/11/2023	Décision de la commission parlementaire d?engager des négociations interinstitutionnelles confirmée par la plénière (Article 71)		
20/03/2024	Approbation en commission du texte adopté en négociations interinstitutionnelles de la 1ère lecture	PE760.887 GEDA/A/(2024)001687	
24/04/2024	Résultat du vote au parlement		
24/04/2024	Décision du Parlement, 1ère lecture	T9-0354/2024	Résumé

Informations techniques

Référence de procédure	2023/0108(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Législation
Instrument législatif	Règlement
	Modification Règlement 2019/881 2017/0225(COD)
Base juridique	Traité sur le fonctionnement de l'UE TFEU 114
Autre base juridique	Règlement du Parlement EP 165
Consultation obligatoire d'autres institutions	Comité économique et social européen
Etape de la procédure	En attente de la position du Conseil en 1ère lecture
Dossier de la commission parlementaire	ITRE/9/11804

Portail de documentation

Document de base législatif		COM(2023)0208	18/04/2023	EC	Résumé
Comité économique et social: avis, rapport		CES2408/2023	13/07/2023	ESC	
Projet de rapport de la commission		PE752.802	07/09/2023	EP	
Amendements déposés en commission		PE753.562	21/09/2023	EP	
Avis spécifique	IMCO	PE749.983	21/09/2023	EP	

Rapport déposé de la commission, 1ère lecture/lecture unique		A9-0307/2023	26/10/2023	EP	Résumé
Lettre de Coreper confirmant l'accord interinstitutionnel		GEDA/A/(2024)001687	21/03/2024	CSL	
Texte adopté du Parlement, 1ère lecture/lecture unique		T9-0354/2024	24/04/2024	EP	Résumé

Informations complémentaires		
Document de recherche	Briefing	19/10/2023

Services de sécurité gérés

OBJECTIF : proposer une modification ciblée du règlement sur la cybersécurité, afin de permettre ladoption future de schémas de certification européens pour les «services de sécurité gérés».

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Parlement européen décide conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE : le règlement (UE) 2019/881 du Parlement européen et du Conseil relatif à l'ENISA (l'Agence de l'Union européenne pour la cybersécurité) et à la certification en matière de cybersécurité des technologies de l'information et des communications établit un cadre pour la mise en place de systèmes européens de certification en matière de cybersécurité dans le but d'assurer un niveau adéquat de cybersécurité pour les produits dinformation et de technologie TIC, les services TIC et les processus TIC dans l'Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur en ce qui concerne les systèmes de certification en matière de cybersécurité dans l'Union.

Les services de sécurité gérés, qui sont des services consistant à mener des activités liées à la gestion des risques de cybersécurité de leurs clients, ou à fournir une assistance à cet égard, ont pris une importance croissante dans la prévention et l'atténuation des incidents de cybersécurité. En conséquence, les prestataires de ces services sont considérés comme des entités essentielles ou importantes appartenant à un secteur de haute criticité conformément à la directive (UE) 2022/2555 du Parlement européen et du Conseil relative à des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union.

Les fournisseurs de services de sécurité gérés dans des domaines tels que la réponse aux incidents, les tests de pénétration, les audits de sécurité et le conseil, jouent un rôle particulièrement important pour aider les entreprises et autres organisations à prévenir, détecter, réagir ou se remettre des cyberincidents. Cependant, ils ont également été la cible de cyberattaques et présentent un risque particulier en raison de leur intégration étroite dans les opérations de leurs clients.

Certains États membres ont déjà commencé à adopter des systèmes de certification pour les services de sécurité gérés. Il existe donc un risque concret de fragmentation du marché intérieur de ces services, auquel la présente proposition vise à remédier.

CONTENU : la modification ciblée proposée vise à permettre, au moyen dactes dexécution de la Commission, ladoption de schémas européens de certification de cybersécurité pour les «services de sécurité gérés», en plus des produits dinformation et de technologie (TIC), des services TIC et des processus TIC, qui sont déjà couverts par le règlement sur la cybersécurité.

La proposition introduit une définition de ces services, qui est très étroitement alignée sur la définition des «fournisseurs de services de sécurité gérés» au sens de la directive NIS 2 (article 2 du règlement sur la cybersécurité). Elle ajoute également une nouvelle disposition sur les objectifs de sécurité de la certification européenne de cybersécurité adaptée aux «services de sécurité gérés». Enfin, un certain nombre de modifications techniques sont apportées afin de garantir que les articles pertinents s'appliquent également aux «services de sécurité gérés».

Services de sécurité gérés

La commission de l'industrie, de la recherche et de l'énergie a adopté le rapport de Josianne CUTAJAR (S&D, MT) sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés.

La commission compétente a recommandé que la position du Parlement européen arrêtée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Modifications de la définition des services de sécurité gérés

Le rapport indique que les services de sécurité gérés - qui sont des services consistant à effectuer ou à fournir une assistance pour les activités liées à la gestion des risques de cybersécurité de leurs clients, y compris la détection, la réponse apportée aux incidents et le rétablissement à la suite de ceux-ci- ont gagné en importance dans la prévention et l'atténuation des incidents de cybersécurité.

Les activités des fournisseurs de services de sécurité gérés consistent en des services de prévention, d'identification, de protection, de détection, d'analyse, de confinement, de réponse et de récupération, y compris, mais sans s'y limiter, la fourniture de renseignements sur les cybermenaces, la surveillance des menaces en temps réel grâce à des techniques proactives, y compris la sécurité par conception, l'évaluation des risques, la détection étendue, la remédiation et la réponse.

Programme de travail glissant de l'Union pour la certification européenne en matière de cybersécurité

Selon les députés, le programme de travail glissant de l'Union devrait inclure une liste de produits TIC, de services TIC et de processus TIC

ou de catégories de ceux-ci, ainsi que de services de sécurité gérés, susceptibles de bénéficier d'une inclusion dans le champ d'application d'un système européen de certification en matière de cybersécurité. Dans ce contexte, la Commission devrait inclure une évaluation approfondie des parcours de formation existants pour combler les déficits de compétences identifiés, ainsi qu'une liste de propositions pour répondre aux besoins en employés qualifiés et en types de compétences.

PME

Les députés ont estimé que la Commission devrait garantir un soutien financier approprié dans le cadre réglementaire des programmes existants de l'Union, en particulier afin d'alléger la charge financière pesant sur les microentreprises et les PME, y compris les jeunes pousses agissant dans le domaine des services de sécurité gérés.

Évaluation et révision

D'ici le 28 juin 2024, et tous les trois ans par la suite, la Commission devrait évaluer l'impact, l'efficacité et l'efficience de l'ENISA et de ses pratiques de travail, la nécessité éventuelle de modifier le mandat de l'ENISA et les implications financières d'une telle modification. L'évaluation devrait porter sur : i) l'efficience et l'efficacité des procédures conduisant à la consultation, à la préparation et à l'adoption des systèmes européens de certification en matière de cybersécurité, ainsi que sur les moyens d'améliorer et d'accélérer ces procédures ; ii) la question de savoir si des exigences essentielles de cybersécurité pour l'accès au marché intérieur sont nécessaires afin d'empêcher les produits TIC, les services TIC, les processus TIC et les services de sécurité gérés qui ne satisfont pas aux exigences fondamentales de cybersécurité d'entrer sur le marché de l'Union.

Services de sécurité gérés

Le Parlement européen a adopté par 530 voix pour, 5 contre et 33 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés.

La position du Parlement européen arrêtée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Objectif

Le règlement proposé vise à permettre ladoption de schémas européens de certification de cybersécurité pour les services de sécurité gérés. Un service de sécurité géré est défini comme un service fourni à un tiers consistant à effectuer des activités liées à la gestion des risques en matière de cybersécurité, ou à fournir une assistance dans le cadre de ces activités, telles que le traitement des incidents, les tests dintrusion, les audits de sécurité et le conseil en matière de sécurité, y compris les conseils dexperts, liés à lassistance technique.

Les schémas de certification faciliteront lentrée sur le marché et loffre de services de sécurité gérés, en simplifiant la charge réglementaire, administrative et financière potentielle que les fournisseurs, en particulier les microentreprises ou les petites et moyennes entreprises (PME), pourraient rencontrer lorsquils proposent des services de sécurité gérés.

En outre, afin dencourager ladoption de services de sécurité gérés et den stimuler la demande, les schémas de certification contribueront à leur accessibilité, en particulier pour les petits acteurs, tels que les microentreprises et les PME, ainsi que pour les collectivités locales et régionales qui disposent de capacités et de ressources limitées, mais qui sont plus exposées aux atteintes à la cybersécurité ayant des implications financières, juridiques, de réputation et opérationnelles.

Le schéma de certification de lUnion pour les services de sécurité gérés devrait contribuer à la disponibilité de services sûrs et de haute qualité qui garantissent une transition numérique sûre et à la réalisation des objectifs fixés dans le programme daction pour la décennie numérique, en particulier en ce qui concerne lobjectif consistant à ce que 75% des entreprises de lUnion commencent à utiliser linformatique en nuage, lIA ou les mégadonnées, à ce que plus de 90% des microentreprises et des PME atteignent au moins un niveau élémentaire dintensité numérique et à ce que les services publics essentiels soient proposés en ligne.

Préparation, adoption et réexamen dun schéma européen de certification de cybersécurité

À la suite dune demande formulée par la Commission, lENISA préparera un schéma candidat qui satisfait aux exigences applicables énoncées au règlement. À la suite dune demande formulée par le groupe européen de certification de cybersécurité (GECC) pourra préparer un schéma candidat qui satisfait aux exigences applicables. Si lENISA rejette une telle demande, elle devra motiver son refus. Toute décision de rejeter une telle demande sera prise par le conseil dadministration.

Lors de la préparation dun schéma candidat, lENISA consultera en temps utile toutes les parties prenantes concernées au moyen dun processus de consultation formel, ouvert, transparent et inclusif. Pour chaque schéma candidat, lENISA créera un groupe de travail ad hoc afin quil lui fournisse des conseils et des compétences spécifiques. Les groupes de travail ad hoc créés à cette fin comprendront, le cas échéant des experts des administrations publiques des États membres, des institutions, organes et organismes de lUnion et du secteur privé.

Information et consultation sur les schémas européens de certification de cybersécurité

La Commission rendra publiques les informations relatives à sa demande à lENISA de préparer un schéma candidat. Au cours de la préparation dun schéma candidat par lENISA, le Parlement européen et le Conseil pourront demander à la Commission, en sa qualité de président du GECC, et à lENISA, de présenter tous les trimestres des informations pertinentes sur un projet de schéma candidat.

À la demande du Parlement européen ou du Conseil, lENISA, en accord avec la Commission, pourra mettre à la disposition du Parlement européen et du Conseil des parties pertinentes dun projet de schéma candidat dune manière adaptée au niveau de confidentialité requis et, le cas échéant, de manière restreinte.

Afin de renforcer le dialogue entre les institutions de lUnion et de contribuer à un processus de consultation formel, ouvert, transparent et inclusif, le Parlement européen et le Conseil pourront inviter la Commission et lENISA à examiner des questions concernant le fonctionnement des schémas européens de certification de cybersécurité pour les produits TIC, services TIC, processus TIC ou services de sécurité gérés. La Commission devra tenir compte, le cas échéant, des éléments découlant des avis exprimés par le Parlement européen et le Conseil.

Une nouvelle annexe contient les exigences auxquelles doivent satisfaire les organismes dévaluation de la conformité qui souhaitent être

accrédités.

Dans une déclaration, la Commission rappelle quil est reconnu quun réexamen approfondi du règlement sur la cybersécurité est de la plus haute importance, y compris lévaluation des procédures conduisant à lélaboration, à ladoption et au réexamen des schémas européens de certification de cybersécurité.

Ce réexamen devrait se fonder sur une analyse approfondie et une vaste consultation sur lincidence, lefficacité et lefficience du fonctionnement du cadre européen de certification de cybersécurité. Lanalyse effectuée dans le cadre de lévaluation établie à larticle 67 du règlement sur la cybersécurité devrait inclure des activités délaboration de schémas en cours, telles que celles concernant le schéma européen de certification de cybersécurité pour les services en nuage, ainsi que des activités concernant des schémas adoptés, telles que celles concernant le schéma européen de certification de cybersécurité fondé sur des critères communs.

La Commission, qui est responsable du réexamen du règlement sur la cybersécurité, veillera à ce que ce réexamen tienne compte, le cas échéant, des éléments nécessaires mentionnés à la lumière de larticle 67 lorsquelle présente le réexamen aux colégislateurs.

Transparence

CUTAJAR Josianne	Rapporteur(e)	ITRE	14/11/2023	ISC2
GROOTHUIS Bart	Rapporteur(e) fictif/fictive	ITRE	24/10/2023	DIGITALEUROPE
CUTAJAR Josianne	Rapporteur(e)	ITRE	10/10/2023	Lenovo Group Limited
CUTAJAR Josianne	Rapporteur(e)	ITRE	15/09/2023	European Commission, DG CNECT
CUTAJAR Josianne	Rapporteur(e)	ITRE	14/09/2023	TIC Council
CUTAJAR Josianne	Rapporteur(e)	ITRE	29/08/2023	ENISA
CUTAJAR Josianne	Rapporteur(e)	ITRE	27/07/2023	FERMA - Federation of European Risk Management Associations
CUTAJAR Josianne	Rapporteur(e)	ITRE	18/07/2023	Board of Cyber
CUTAJAR Josianne	Rapporteur(e)	ITRE	06/07/2023	ESET Slovak
CUTAJAR Josianne	Rapporteur(e)	ITRE	06/07/2023	Red Alert Labs IoT Security
DANTI Nicola	Membre	12/10/2023	Leonardo S.p.A.	