

Informations de base	
2023/0108(COD)	Procédure terminée
COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	
Services de sécurité gérés	
Modification Règlement 2019/881 2017/0225(COD)	
Subject	
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	CUTAJAR Josianne (S&D)	02/05/2023
		Rapporteur(e) fictif/fictive NIEBLER Angelika (EPP) GROOTHUIS Bart (Renew) NIINISTÖ Ville (Greens/EFA) TOŠENOVSKÝ Evžen (ECR)	
Commission pour avis	Commission pour avis	Rapporteur(e) pour avis	Date de nomination
	IMCO Marché intérieur et protection des consommateurs	Président au nom de la commission CAVAZZINI Anna (Greens/EFA)	23/05/2023
	LIBE Libertés civiles, justice et affaires intérieures	La commission a décidé de ne pas donner d'avis.	
Conseil de l'Union européenne	Formation du Conseil	Réunions	Date
	Emploi, politique sociale, santé et consommateurs	4064	2024-12-02
Commission européenne	DG de la Commission	Commissaire	
	Réseaux de communication, contenu et technologies	BRETON Thierry	

Comité économique et social européen

Evénements clés			
Date	Événement	Référence	Résumé
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	GEDA/A/(2024)001687 PE760.887	
24/04/2024	Décision du Parlement, 1ère lecture	T9-0354/2024	Résumé
24/04/2024	Résultat du vote au parlement		
02/12/2024	Adoption de l'acte par le Conseil après la 1ère lecture du Parlement		
19/12/2024	Signature de l'acte final		
15/01/2025	Publication de l'acte final au Journal officiel		

Informations techniques	
Référence de la procédure	2023/0108(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Note thématique
Instrument législatif	Règlement
Modifications et abrogations	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
État de la procédure	Procédure terminée
Dossier de la commission	ITRE/9/11804

Portail de documentation
Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE752.802	07/09/2023	
Avis spécifique	IMCO	PE749.983	21/09/2023	
Amendements déposés en commission		PE753.562	21/09/2023	
Rapport déposé de la commission, 1ère lecture/lecture unique		A9-0307/2023	26/10/2023	Résumé
Texte convenu lors de négociations interinstitutionnelles		PE760.887	20/03/2024	
Texte adopté du Parlement, 1ère lecture/lecture unique		T9-0354/2024	24/04/2024	Résumé

Conseil de l'Union

Type de document	Référence	Date	Résumé
Lettre de la Coreper confirmant l'accord interinstitutionnel	GEDA/A/(2024)001687	21/03/2024	
Projet d'acte final	00093/2024/LEX	19/12/2024	

Commission Européenne

Type de document	Référence	Date	Résumé
Document de base législatif	COM(2023)0208 	18/04/2023	Résumé
Réaction de la Commission sur le texte adopté en plénière	SP(2024)394	08/08/2024	

Parlements nationaux

Type de document	Parlement /Chambre	Référence	Date	Résumé
Contribution	CZ_CHAMBER	COM(2023)0208	29/06/2023	
Contribution	PT_PARLIAMENT	COM(2023)0208	20/07/2023	
Contribution	CZ_SENATE	COM(2023)0208	01/08/2023	

Autres Institutions et organes

Institution/organe	Type de document	Référence	Date	Résumé
EESC	Comité économique et social: avis, rapport	CES2408/2023	13/07/2023	

Informations complémentaires			
Source	Document	Date	
Service de recherche du PE	Briefing	19/10/2023	

Réunions avec des représentant(e)s d'intérêts, publiées conformément au règlement intérieur

Rapporteur(e)s, rapporteur(e)s fictifs/fictives et président(e)s des commissions

Transparence				
Nom	Rôle	Commission	Date	Représentant(e)s d'intérêts
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	Leonardo Cyber and Security Solutions
CUTAJAR Josianne	Rapporteur(e)	ITRE	06/07/2023	Red Alert Labs IoT Security
CUTAJAR Josianne	Rapporteur(e)	ITRE	06/07/2023	ESET Slovak
CUTAJAR Josianne	Rapporteur(e)	ITRE	05/07/2023	European Commission, DG CNECT

Autres membres

Transparence		
Nom	Date	Représentant(e)s d'intérêts
DANTI Nicola	12/10/2023	Leonardo S.p.A.

Acte final
Règlement 2025/0037 JO OJ L 15.01.2025
Rectificatif à l'acte final 32025R0037R(01) JO OJ L 24.01.2025

Résumé

Services de sécurité gérés

2023/0108(COD) - 15/01/2025 - Acte final

OBJECTIF : permettre la mise en place de schémas européens de certification de cybersécurité pour les services de sécurité gérés.

ACTE LÉGISLATIF : Règlement (UE) 2025/37 du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés.

CONTENU : le présent règlement s'inscrit dans le cadre du paquet législatif sur la cybersécurité qui comprend également le nouveau [règlement](#) sur la cybersolidarité.

Schémas européens de certification

La présente modification ciblée du règlement sur la cybersécurité vise à renforcer la cyberrésilience de l'UE en permettant l'adoption à l'avenir de schémas européens de certification pour les «**services de sécurité gérés**».

Les services de sécurité gérés tels que les services concernant la gestion des incidents de cybersécurité, les tests d'intrusion, les audits de sécurité et les conseils liés à l'assistance technique, ont gagné en importance en ce qui concerne la prévention et la limitation des incidents.

Les fournisseurs de services de sécurité gérés ont été la cible de cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque particulier. Il est donc important que les entités essentielles et importantes fassent preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité géré.

La modification ciblée contribuera à **améliorer la qualité des services de sécurité gérés** et à accroître leur comparabilité, elle facilitera l'émergence de fournisseurs de services de cybersécurité fiables, et elle permettra d'éviter la fragmentation du marché intérieur. Elle contribuera à la réalisation de l'objectif consistant à ce que **75%** des entreprises de l'Union commencent à utiliser les services d'informatique en nuage, les mégadonnées ou l'intelligence artificielle ou, à ce que plus de **90%** des PME, y compris les microentreprises, atteignent au moins un niveau élémentaire d'intensité numérique et à ce que les services publics essentiels soient accessibles en ligne.

Rôle de l'Agence de l'Union européenne pour la cybersécurité (ENISA)

L'ENISA jouera un rôle important dans la préparation des schémas européens de certification de cybersécurité candidats. L'ENISA :

- favorisera le recours à la certification européenne de cybersécurité en vue d'éviter la fragmentation du marché intérieur;
- contribuera à l'établissement et au maintien d'un **cadre européen de certification** de cybersécurité;
- favorisera l'élaboration et la mise en œuvre de la politique de l'Union en matière de certification de cybersécurité des produits TIC et services de sécurité gérés;
- facilitera l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits TIC services de sécurité gérés.

À la suite d'une demande formulée par la Commission, l'ENISA préparera un **schéma candidat** qui satisfait aux exigences applicables énoncées au règlement. Lors de la préparation d'un schéma candidat, l'ENISA consultera en temps utile toutes les parties prenantes concernées au moyen d'un processus de consultation formel, ouvert, transparent et inclusif. Pour chaque schéma candidat, l'ENISA créera un groupe de travail ad hoc afin qu'il lui fournit des conseils et des compétences spécifiques.

Information et consultation sur les schémas européens de certification de cybersécurité

La Commission rendra **publiques** les informations relatives à sa demande à l'ENISA de préparer un schéma candidat. Au cours de la préparation d'un schéma candidat par l'ENISA, le Parlement européen et le Conseil pourront demander à la Commission et à l'ENISA, de présenter tous les trimestres des informations pertinentes sur un projet de schéma candidat.

Objectifs de sécurité des schémas européens de certification de cybersécurité

Un schéma européen de certification de cybersécurité pour les services de sécurité gérés doit être conçu de façon à réaliser, selon le cas, au moins les objectifs de sécurité suivants:

- que les services de sécurité gérés soient fournis avec la compétence, l'expertise et l'expérience requises;
- que le fournisseur ait mis en place des procédures internes pour garantir que les services de sécurité gérés sont fournis à tout moment à un niveau de qualité suffisant;
- que les données consultées, stockées, transmises ou traitées dans le cadre de la fourniture de services de sécurité gérés soient protégées contre l'accès, le stockage, la diffusion, la destruction ou tout autre traitement accidentels ou non autorisés, ou contre la perte ou l'altération ou l'indisponibilité;
- que la disponibilité des données, services et fonctions ainsi que l'accès à ceux-ci soient rétablis dans les plus brefs délais en cas d'incident physique ou technique;
- qu'un registre soit tenu et disponible pour l'évaluation des données, services ou fonctions qui ont été consultés, utilisés ou traités de toute autre façon, du moment où ils l'ont été et par qui, et faire en sorte qu'il soit possible d'évaluer ces éléments.

La Commission **évaluera régulièrement** l'efficacité et l'utilisation des schémas européens de certification de cybersécurité adoptés ainsi que la question de savoir si un schéma européen de certification de cybersécurité spécifique doit être rendu obligatoire, au moyen de dispositions pertinentes du droit de l'Union.

Une **nouvelle annexe** contient les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité qui souhaitent être accrédités.

ENTRÉE EN VIGUEUR : 4.2.2025.

Services de sécurité gérés

2023/0108(COD) - 24/04/2024 - Texte adopté du Parlement, 1ère lecture/lecture unique

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 l'adoption 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 d'intrusion, les audits de sécurité et le conseil en matière de sécurité, y compris les conseils d'experts, liés à l'assistance technique.

Les schémas de certification faciliteront l'entrée sur le marché et l'offre 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 lorsqu'ils proposent des services de sécurité gérés.

En outre, afin d'encourager l'adoption de services de sécurité gérés et d'en 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 l'Union 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 d'action pour la décennie numérique, en particulier en ce qui concerne l'objectif consistant à ce que 75% des entreprises de l'Union commencent à utiliser l'informatique en nuage, l'IA ou les mégadonnées, à ce que plus de 90% des microentreprises et des PME atteignent au moins un niveau élémentaire d'intensité numérique et à ce que les services publics essentiels soient proposés en ligne.

Préparation, adoption et réexamen d'un schéma européen de certification de cybersécurité

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

Lors de la préparation d'un schéma candidat, l'**ENISA** consultera en temps utile toutes les parties prenantes concernées au moyen d'un processus de consultation formel, ouvert, transparent et inclusif. Pour chaque schéma candidat, l'**ENISA** créera un groupe de travail ad hoc afin qu'il lui fournit 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 l'Union 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 l'**ENISA** de préparer un schéma candidat. Au cours de la préparation d'un schéma candidat par l'**ENISA**, le Parlement européen et le Conseil pourront demander à la Commission, en sa qualité de président du GECC, et à l'**ENISA**, de présenter **tous les trimestres** des informations pertinentes sur un projet de schéma candidat.

À la demande du Parlement européen ou du Conseil, l'**ENISA**, en accord avec la Commission, pourra mettre à la disposition du Parlement européen et du Conseil des parties pertinentes d'un projet de schéma candidat d'une manière adaptée au niveau de confidentialité requis et, le cas échéant, de manière restreinte.

Afin de renforcer le dialogue entre les institutions de l'Union et de contribuer à un processus de consultation formel, ouvert, transparent et inclusif, le Parlement européen et le Conseil pourront inviter la Commission et l'**ENISA** 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 d'évaluation de la conformité qui souhaitent être accrédités.

Dans une **déclaration**, la Commission rappelle qu'il est reconnu qu'un réexamen approfondi du règlement sur la cybersécurité est de la plus haute importance, y compris l'évaluation des procédures conduisant à l'élaboration, à l'adoption et au réexamen des schémas européens de certification de cybersécurité.

Ce réexamen devrait se fonder sur une analyse approfondie et une vaste consultation sur l'incidence, l'efficacité et l'efficience du fonctionnement du cadre européen de certification de cybersécurité. L'analyse effectuée dans le cadre de l'évaluation établie à l'article 67 du règlement sur la cybersécurité devrait inclure des activités d'élaboration 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 l'article 67 lorsqu'elle présente le réexamen aux collégisateurs.

Services de sécurité gérés

2023/0108(COD) - 18/04/2023 - Document de base législatif

OBJECTIF : proposer une modification ciblée du règlement sur la cybersécurité, afin de permettre l'adoption 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 d'information 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 d'actes d'exécution de la Commission, **l'adoption de schémas européens de certification de cybersécurité pour les «services de sécurité gérés»**, en plus des produits d'information 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

2023/0108(COD) - 26/10/2023 - Rapport déposé de la commission, 1ère lecture/lecture unique

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.