Procedure file

Informations de base

COD - Procédure législative ordinaire (ex-procedure codécision) Directive	2020/0359(COD)	En attente de la position du Parlement en 1ère lecture
Un niveau élevé commun de cybersécurité Abrogation Directive (EU) 2016/1148 2013/0027(COD) Sujet 2.80 Coopération et simplification administratives 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 7.30.09 Sécurité publique Priorités législatives Déclaration commune 2021		

Acteurs principaux

Parlement européen	Commission au fond	Rapporteur(e)	Date de nomination
	ITRE Industrie, recherche et énergie		14/01/2021
		renew europe. GROOTHUIS Bart	
		Rapporteur(e) fictif/fictive	
		epp MAYDELL Eva	
		S&D KAILI Eva	
		ANDRESEN Rasmus	
		MARIANI Thierry	
		ECR TOŠENOVSKÝ Evžen	
		MATIAS Marisa	
	Commission pour avis	Rapporteur(e) pour avis	Date de nomination
	CULT Culture et éducation	La commission a décidé de ne pas donner d'avis.	
	AFET Affaires étrangères		22/02/2021
		GREGOROVÁ Markéta	
	TRAN Transports et tourisme		03/02/2021
		DALUNDE Jakop G.	
	LIBE Libertés civiles, justice et affaires intérieures (Commission associée)		12/04/2021

		MANDL Lukas	
	IMCO Marché intérieur et protection des consommateurs		09/02/2021
		LØKKEGAARD Morten	
	ECON Affaires économiques et monétaires	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

16/12/2020	Publication de la proposition législative	COM(2020)0823	Résumé
21/01/2021	Annonce en plénière de la saisine de la commission, 1ère lecture		
20/05/2021	Annonce en plénière de la saisine des commissions associées		
28/10/2021	Vote en commission,1ère lecture		
28/10/2021	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d?un rapport adopté en commission		
04/11/2021	Dépôt du rapport de la commission, 1ère lecture	A9-0313/2021	Résumé
10/11/2021	Décision de la commission parlementaire d?engager des négociations interinstitutionnelles annoncée en plénière (Article 71)		
22/11/2021	Décision de la commission parlementaire d?engager des négociations interinstitutionnelles confirmée par la plénière (Article 71)		

Prévisions

17/10/2022	Date indicative de la séance plénière

Informations techniques

Référence de procédure	2020/0359(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Législation
Instrument législatif	Directive
	Abrogation Directive (EU) 2016/1148 2013/0027(COD)
Base juridique	Règlement du Parlement EP 57; Traité sur le fonctionnement de l'UE TFEU 114-p1
Autre base juridique	Règlement du Parlement EP 159
Consultation obligatoire d'autres institutions	Comité économique et social européen

Etape de la procédure	En attente de la position du Parlement en 1ère lecture
Dossier de la commission parlementaire	ITRE/9/04961

Portail de documentation

Document de base législatif		COM(2020)0823	16/12/2020	EC	Résumé
Document annexé à la procédure		SEC(2020)0430	16/12/2020	EC	
Document annexé à la procédure		SWD(2020)0344	16/12/2020	EC	
Document annexé à la procédure		SWD(2020)0345	16/12/2020	EC	
Document annexé à la procédure		N9-0025/2021 JO C 183 11.05.2021, p. 0003	11/03/2021	EDPS	
Projet de rapport de la commission		PE692.602	03/05/2021	EP	
Amendements déposés en commission		PE693.680	03/06/2021	EP	
Amendements déposés en commission		PE693.723	03/06/2021	EP	
Avis de la commission	TRAN	PE689.861	14/07/2021	EP	
Avis de la commission	IMCO	PE691.156	14/07/2021	EP	
Avis de la commission	AFET	PE691.371	15/07/2021	EP	
Avis de la commission	LIBE	PE693.822	15/10/2021	EP	
Rapport déposé de la commission, 1ère lecture/lecture unique		A9-0313/2021	04/11/2021	EP	Résumé
Banque centrale européenne: avis, orientation, rapport		CON/2022/0014 JO C 233 16.06.2022, p. 0022	11/04/2022	ECB	

Informations complémentaires

Un niveau élevé commun de cybersécurité

OBJECTIF : introduire des mesures visant à un niveau commun élevé de cybersécurité dans toute lUnion.

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 : la directive (UE) 2016/1148 du Parlement européen et du Conseil vise à renforcer les capacités de cybersécurité dans l'UE, à atténuer les menaces pesant sur les systèmes de réseaux et d'information utilisés pour fournir des services essentiels dans des secteurs clés et à assurer la continuité de ces services en cas d'incidents de cybersécurité, contribuant ainsi au bon fonctionnement de l'économie et de la société de l'UE.

Toutefois, depuis l'entrée en vigueur de la directive (UE) 2016/1148, des progrès significatifs ont été réalisés pour accroître le niveau de résilience de l'Union en matière de cybersécurité.

CONTENU : la présente proposition vise à remplacer la directive (UE) 2016/1148 relative à la sécurité des réseaux et des systèmes d'information (directive NIS). Il s'agit du premier acte législatif européen en matière de cybersécurité, qui prévoit des mesures juridiques visant à renforcer le niveau général de cybersécurité dans l'UE. La proposition modernise le cadre juridique existant en tenant compte de la numérisation accrue du marché intérieur au cours des dernières années et de l'évolution du paysage des menaces en matière de cybersécurité.

Champ d'application

La proposition devrait s'appliquer à certaines entités essentielles publiques ou privées opérant dans les secteurs énumérés à l'annexe I (énergie ; transports ; banques ; infrastructures des marchés financiers ; santé, eau potable ; eaux usées ; infrastructures numériques ; administration publique et espace) et à certaines entités importantes opérant dans les secteurs énumérés à l'annexe II (services postaux et de courrier ; gestion des déchets ; fabrication, production et distribution de produits chimiques ; production, transformation et distribution de denrées alimentaires ; fabrication et fournisseurs numériques).

Les micro et petites entités seraient exclues du champ d'application de la directive, à l'exception des fournisseurs de réseaux de communications électroniques ou de services de communications électroniques accessibles au public, des fournisseurs de services fiduciaires, des registres de noms de domaine de premier niveau (TLD) et de l'administration publique, ainsi que de certaines autres entités, telles que le fournisseur unique d'un service dans un État membre.

Cadres nationaux de cybersécurité

La proposition prévoit que les États membres seront tenus d'adopter une stratégie nationale de cybersécurité définissant les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue d'atteindre et de maintenir un niveau élevé de cybersécurité.

Elle établit également un cadre pour la divulgation coordonnée des vulnérabilités et exige des États membres qu'ils désignent des équipes d'intervention en cas d'incident de sécurité informatique qui agiront comme intermédiaires de confiance et faciliteront l'interaction entre les entités déclarantes et les fabricants ou fournisseurs de produits et services de technologies de linformation et de la communication (TIC).

Les États membres seraient tenus de mettre en place des cadres nationaux de gestion des crises de cybersécurité, en désignant des autorités nationales compétentes chargées de la gestion des incidents et des crises de cybersécurité à grande échelle.

Gestion des risques liés à la cybersécurité et obligations d'information

La proposition exige des États membres qu'ils prévoient que les organes de gestion de toutes les entités relevant du champ d'application approuvent les mesures de gestion des risques en matière de cybersécurité prises par les entités respectives et suivent une formation spécifique à la cybersécurité. Les entités relevant du champ d'application devraient des mesures techniques et organisationnelles appropriées et proportionnées pour gérer les risques de cybersécurité posés à la sécurité des réseaux et des systèmes d'information.

Les registres du TLD et les entités fournissant des services d'enregistrement de noms de domaine pour le TLD devraient collecter et conserver des données exactes et complètes sur l'enregistrement des noms de domaine. En outre, ces entités seraient tenues de fournir un accès efficace aux données d'enregistrement de domaine pour les demandeurs d'accès légitimes.

Compétence et enregistrement

En règle générale, les entités essentielles et importantes sont considérées comme relevant de la juridiction de l'État membre où elles fournissent leurs services. La proposition prévoit que certains types d'entités (fournisseurs de services DNS, registres de noms de TLD, fournisseurs de services d'informatique en nuage, fournisseurs de services de centres de données et fournisseurs de réseaux de diffusion de contenu, ainsi que certains fournisseurs numériques) seraient réputés relever de la juridiction de l'État membre dans lequel ils ont leur principal établissement dans l'Union.

Partage d'informations

Les États membres devraient prévoir des règles permettant aux entités de s'engager dans le partage d'informations liées à la cybersécurité dans le cadre d'accords spécifiques de partage d'informations sur la cybersécurité.

Supervision et application

Les autorités compétentes seraient tenues de superviser les entités relevant du champ d'application de la directive proposée, et notamment de veiller à ce qu'elles respectent les exigences en matière de sécurité et de notification des incidents. La proposition exige également que les États membres imposent des amendes administratives aux entités essentielles et importantes et définit certaines amendes maximales.

Un niveau élevé commun de cybersécurité

La commission de lindustrie, de la recherche et de lénergie a adopté le rapport de Bart GROOTHUIS (Renew Europe, NL) sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans lensemble de lUnion, abrogeant la directive (UE) 2016/1148

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

Objet et champ dapplication

La directive sappliquerait aux entités publiques et privées essentielles et importantes dun type appelé «entités essentielles» à lannexe I et « entités importantes» à lannexe II, qui fournissent leurs services ou mènent leurs activités au sein de lUnion. Elle ne sappliquerait pas aux petites entreprises ou aux microentreprises. Au plus tard 6 mois après le délai de transposition, les États membres devraient établir une liste des entités essentielles et importantes. Cette liste devrait être mise à jour régulièrement et au moins tous les deux ans.

Les entités essentielles et importantes devraient soumettre au moins les informations suivantes aux autorités compétentes: i) le nom de lentité, ii) ladresse et les coordonnées actualisées, y compris les adresses électroniques, iii) les plages dIP, iv) les numéros de téléphone et v) le ou les secteurs et sous-secteurs concernés mentionnés aux annexes I et II. Les entités devraient informer les autorités compétentes de toute modification de ces informations.

À cette fin, lAgence de lUnion européenne pour la cybersécurité (ENISA), en coopération avec le groupe de coopération, devrait publier dans les meilleurs délais des lignes directrices et des modèles concernant les obligations de notification. Le traitement de données à caractère personnel au titre de la directive serait effectué conformément au règlement général sur la protection des données (RGPD).

Stratégie nationale en matière de cybersécurité

Cette stratégie devrait également comprendre un cadre pour la répartition des rôles et des responsabilités des organismes et entités publics ainsi que des autres acteurs concernés, un point de contact unique en matière de cybersécurité pour les PME ainsi quune évaluation du niveau général de sensibilisation des citoyens à la cybersécurité.

Les États membres devraient par ailleurs adopter :

- une politique en matière de cybersécurité pour chaque secteur couvert par la directive;

- des prescriptions relatives au cryptage et lutilisation de produits de cybersécurité à code source ouvert;

- une politique liée au maintien de la disponibilité générale et de lintégrité du noyau public de linternet ouvert, y compris la cybersécurité des câbles de communications sous-marins;

- une politique visant à promouvoir le développement et lintégration de technologies émergentes, telles que lintelligence artificielle, dans les outils et applications de renforcement de la cybersécurité;

- une politique de promotion de lhygiène informatique augmentant la sensibilisation générale des citoyens aux menaces et aux meilleures pratiques en matière de cybersécurité;

- une politique de promotion de la cyberdéfense active;

- une politique pour aider les autorités à développer des compétences et à mieux comprendre les aspects de sécurité nécessaires pour concevoir, construire et gérer des lieux connectés;

- une politique traitant spécifiquement de la menace des logiciels rançonneurs et sefforçant de désorganiser le modèle économique de ces derniers;

- une politique comprenant des procédures et des cadres de gouvernance pour soutenir la mise en place de partenariats public-privé en matière de cybersécurité.

LENISA devrait fournir des conseils aux États membres afin daligner les stratégies nationales de cybersécurité sur les exigences et les obligations énoncées dans la directive.

Divulgation coordonnée des vulnérabilités et base de données européenne des vulnérabilités

LENISA devrait élaborer et tenir à jour une base de données européenne des vulnérabilités qui exploite le registre mondial Common Vulnerabilities and Exposures (CVE). À cette fin, lENISA devrait adopter les mesures techniques et organisationnelles nécessaires pour assurer la sécurité et lintégrité de la base de données.

Centres de réponse aux incidents de sécurité informatique (CSIRT)

Les États membres devraient garantir la possibilité dun échange dinformations efficace et sécurisé à tous les niveaux de classification entre leurs propres CSIRT et les CSIRT de pays tiers au même niveau de classification. Les CSIRT devraient développer au moins les capacités techniques suivantes:

- mener une surveillance en temps réel ou quasi-réel des réseaux et des systèmes dinformation, et à détecter les anomalies;

- soutenir la prévention et la détection des intrusions;

- collecter et analyser les données de police scientifique;

- filtrer le trafic malveillant;

- mettre en uvre une authentification poussée et des privilèges et contrôles daccès forts;

- analyser les cybermenaces.

Les CSIRT devraient assumer la surveillance des cybermenaces, des vulnérabilités et des incidents au niveau national et lacquisition de renseignements sur les menaces en temps réel, la réaction aux incidents et lassistance aux entités concernées ainsi que la contribution au déploiement doutils de partage dinformations sécurisés.

LENISA devrait publier, en coopération avec la Commission, un rapport bisannuel sur létat de la cybersécurité dans lUnion et le soumettre au Parlement européen.

Obligations en matière de communication dinformations

Les États membres devraient mettre en place un point dentrée unique pour toutes les notifications requises en vertu de la directive et dautres actes pertinents de lUnion.

Les entités essentielles et importantes devraient informer les CSIRT des incidents importants qui ont une incidence sur la disponibilité de leur service dans les 24 heures suivant la prise de connaissance de lincident. Elles devront informer les CSIRT des incidents importants qui portent atteinte à la confidentialité et à lintégrité de leurs services dans un délai de 72 heures à compter de la prise de connaissance de lincident.

Amendes

Afin de garantir une application efficace des obligations prévues par la directive, chaque autorité compétente pourrait imposer ou demander limposition damendes administratives si la violation a été commise délibérément ou par négligence ou si lentité concernée avait été informée de son infraction.

Transparence

GROOTHUIS Bart	Rapporteur(e)	ITRE	10/02/2022	Provincie Flevoland
GROOTHUIS Bart	Rapporteur(e)	ITRE	03/03/2022	Hanbury Strategy and Communications Limited
GROOTHUIS Bart	Rapporteur(e)	ITRE	03/03/2022	DIGITALEUROPE

GROOTHUIS Bart	Rapporteur(e)	ITRE	09/03/2022	Palo Alto Networks Inc.
GROOTHUIS Bart	Rapporteur(e)	ITRE	17/03/2022	BUSINESSEUROPE
GROOTHUIS Bart	Rapporteur(e)	ITRE	23/03/2022	Broadcom
GROOTHUIS Bart	Rapporteur(e)	ITRE	24/03/2022	ICANN
PETERSEN Morten	Membre	11/11/2021	Euritas	