Parlement européen
2019-2024

Commission du marché intérieur et de la protection des consommateurs

2020/0359(COD)

14.7.2021

AVIS

de la commission du marché intérieur et de la protection des consommateurs

à l'intention de la commission de l'industrie, de la recherche et de l'énergie

concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Rapporteur pour avis: Morten Løkkegaard

PA_Legam

JUSTIFICATION SUCCINCTE

De manière générale, le rapporteur approuve la proposition législative de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2). Dans un monde de plus en plus numérisé, la sécurité en ligne est essentielle pour garantir un environnement numérique sûr ainsi que le fonctionnement du marché unique, dans lequel les consommateurs et les opérateurs peuvent opérer librement.

La proposition de directive SRI 2 constitue une amélioration importante par rapport à la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI 1). Elle recense les principales défaillances de la directive SRI 1, notamment le faible niveau de cyber-résilience des entreprises et des secteurs, ainsi que le degré de résilience variable et l'insuffisance d'une appréciation commune de la situation et d'une réaction aux crises, dans les États membres et entre eux. Le rapporteur salue les ambitions visant à corriger ces défaillances dans la directive SRI 2.

Champ d'application

Le rapporteur se félicite de l'élargissement du champ d'application de la proposition de directive SRI 2, en particulier de la prise en compte de nouveaux secteurs tels que l'administration publique. La liste explicite des secteurs et services couverts réduira certainement la marge d'appréciation des États membres dans la définition des entités relevant de la directive et limitera par conséquent la fragmentation du marché unique.

Pour les secteurs et services concernés, la Commission propose d'appliquer la règle du plafond en tant que critère uniforme déterminant les entités qui relèvent du champ d'application de la directive. Ce critère présente sans aucun doute l'avantage de garantir la sécurité juridique tout en réduisant les divergences entre États membres.

Tout en se félicitant de l'élargissement du champ d'application sectoriel, le rapporteur estime cependant que ce critère général devrait être combiné à une évaluation du niveau de risque des entités au sein de chaque secteur. Cela permettrait d'exclure du champ d'application de la directive les entités de taille moyenne et de grande taille qui sont considérées, à la suite d'une évaluation des risques, comme présentant un faible degré de criticité et de dépendance à l'égard d'entités par ailleurs critiques.

Le rapporteur insiste sur le fait qu'il ne faudrait pas considérer que cela laisse le champ libre à des divergences d'interprétation entre les États membres. Afin d'éviter une fragmentation supplémentaire de la mise en œuvre dans les États membres, la Commission est encouragée à publier des orientations claires à cet égard.

Enfin, tout en saluant le fait que les microentreprises et les petites entreprises soient exclues du champ d'application, le rapporteur estime qu'il est nécessaire d'encourager leur inclusion volontaire, dès lors que ces entreprises font également l'objet de cyberattaques et en sont affectées.

Cadres réglementaires coordonnés en matière de cybersécurité

Le rapporteur accueille favorablement le chapitre définissant différents éléments des stratégies nationales en matière de cybersécurité et leurs outils de gestion des situations de crise. Il est proposé aux États membres, dans le cadre de leur stratégie nationale en matière de cybersécurité, d'adopter des mesures de promotion de l'utilisation de la cryptographie et du cryptage, en particulier dans le cas des PME.

Le rapporteur se félicite de la mise en place par l'ENISA d'un registre européen des vulnérabilités, mais il estime important que l'enregistrement respecte la confidentialité des informations commerciales et les secrets d'affaires, et qu'il ne constitue pas une charge inutile pour les entités.

Coopération entre les États membres

La directive SRI 2 prévoit une coopération plus structurée – particulièrement bienvenue – entre les États membres au sein du groupe de coopération, du réseau des CSIRT et du groupe chargé des incidents majeurs, nouvellement créé. Toutefois, il est nécessaire de veiller à une amélioration du niveau de confiance et de la volonté d'échanger des informations entre États membres, étant donné qu'il est essentiel que cette coopération soit efficace pour garantir un niveau élevé de cybersécurité dans l'Union.

Compte tenu de ce qui précède, plusieurs amendements ont été élaborés en vue de renforcer le rôle des réseaux. Le rapporteur considère, en particulier, que l'examen par les pairs est une manière constructive de renforcer la confiance partagée des États membres, et il est d'avis que ces derniers devraient jouer un rôle de premier plan dans l'évaluation de l'efficacité des politiques de chacun d'entre eux en matière de cybersécurité.

Gestion des risques en matière de cybersécurité

Le rapporteur se félicite de l'extension de l'évaluation des risques à l'ensemble de la chaîne d'approvisionnement (articles 18 et 19), mais souligne toutefois qu'il convient de clarifier ce point pour apporter des orientations claires aux entités soumises à cette exigence ainsi qu'aux États membres lorsqu'ils procèdent à une évaluation coordonnée des risques en matière de sécurité dans les secteurs ou les chaînes d'approvisionnement particulièrement critiques.

Obligations en matière de communication d'informations

Le rapporteur estime qu'il convient de clarifier certains points de la directive révisée, en particulier en ce qui concerne certaines des obligations qu'elle impose aux entreprises. Il s'agit de réduire la bureaucratie et de faciliter le respect des nouvelles règles par les entreprises en gardant à l'esprit l'objectif final, à savoir une mise en œuvre effective de la directive.

Le rapporteur propose d'étendre de 24 heures à 72 heures le délai de signalement des incidents pour les premières notifications, afin de permettre aux entreprises de répondre efficacement à la cyberattaque en cours avant de la notifier. En outre, il est proposé de supprimer toute référence à la notification obligatoire des «incidents potentiels».

AMENDMENTS

La commission du marché intérieur et de la protection des consommateurs invite la commission de l'industrie, de la recherche et de l'énergie, compétente au fond, à prendre en considération les amendements suivants:

Amendement 1
Proposition de directive
Considérant 5

Texte proposé par la Commission	*Amendement*
(5) L'ensemble de ces divergences donnent lieu à une fragmentation du marché intérieur et sont susceptibles de produire un effet nuisible sur le fonctionnement de celui-ci, affectant plus particulièrement la fourniture transfrontière de services et le niveau de cyber-résilience en raison de l'adoption de normes différentes. La présente directive a pour objectif de supprimer ces divergences importantes entre les États membres, notamment en définissant des règles minimales concernant le fonctionnement d'un cadre réglementaire coordonné, en établissant des mécanismes permettant une coopération efficace entre les autorités compétentes de chaque État membre, en mettant à jour la liste des secteurs et activités soumis à des obligations en matière de cybersécurité, et en prévoyant des recours et des sanctions effectifs qui sont essentiels à l'application effective de ces obligations. Il convient, par conséquent, que la directive (UE) 2016/1148 soit abrogée et remplacée par la présente directive.	(5) L'ensemble de ces divergences donnent lieu à une fragmentation du marché intérieur et sont susceptibles de produire un effet nuisible sur le fonctionnement de celui-ci, affectant plus particulièrement la fourniture transfrontière de services et le niveau de cyber-résilience en raison de l'adoption de normes différentes. La présente directive a pour objectif de supprimer ces divergences importantes entre les États membres ***et de renforcer le marché intérieur***, notamment en définissant des règles minimales concernant le fonctionnement d'un cadre réglementaire coordonné, en établissant des mécanismes permettant une coopération efficace entre les autorités compétentes de chaque État membre, en mettant à jour la liste des secteurs et activités soumis à des obligations en matière de cybersécurité, et en prévoyant des recours et des sanctions effectifs qui sont essentiels à l'application effective de ces obligations. Il convient, par conséquent, que la directive (UE) 2016/1148 soit abrogée et remplacée par la présente directive.

Amendement 2
Proposition de directive
Considérant 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(6 bis) La présente directive est sans préjudice des règles établies par la législation de l'Union relative à la

protection des données à caractère personnel.

Amendement 3
Proposition de directive
Considérant 9

Texte proposé par la Commission	*Amendement*
(9) Toutefois, les microentités ou les entités de petite taille qui remplissent certains critères indiquant qu'elles jouent un rôle essentiel pour les économies ou les sociétés des États membres ou pour des secteurs ou des types de services particuliers devraient également être couvertes par la présente directive, et les États membres devraient être chargés d'établir une liste de ces entités, et de la transmettre à la Commission.	(9) Toutefois, les microentités ou les entités de petite taille qui remplissent certains critères indiquant qu'elles jouent un rôle essentiel pour les économies ou les sociétés des États membres ou pour des secteurs ou des types de services particuliers devraient également être couvertes par la présente directive, et les États membres devraient être chargés d'établir une liste de ces entités, et de la transmettre à la Commission. ***La Commission devrait donner des orientations claires concernant les critères qui déterminent quelles microentités ou entités de petite taille seraient essentielles ou importantes, en particulier lorsqu'elles fournissent des services dans plusieurs États membres.***

Amendement 4
Proposition de directive
Considérant 10

Texte proposé par la Commission	*Amendement*
(10) La Commission, en coopération avec le groupe de coopération, ***peut*** publier des lignes directrices concernant la mise en œuvre des critères applicables aux microentreprises et aux entreprises de petite taille.	(10) La Commission, en coopération avec le groupe de coopération, ***devrait*** publier des lignes directrices concernant la mise en œuvre des critères applicables aux microentreprises et aux entreprises de petite taille.

Amendement 5
Proposition de directive
Considérant 12 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(12 bis) L'élargissement du champ d'application de cette directive implique l'inclusion d'entités soumises à une réglementation sectorielle. Afin d'éviter toute duplication ou charge réglementaire, la Commission devrait veiller à ce que les actes sectoriels exigeant que les entités essentielles ou importantes adoptent des mesures de gestion des risques en matière de cybersécurité ou notifient les incidents ou les cybermenaces importantes soient compatibles avec la présente directive.

Amendement 6
Proposition de directive
Considérant 12 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(12 ter) La Commission devrait publier des lignes directrices claires accompagnant la présente directive afin de garantir l'harmonisation de la mise en œuvre dans les États membres et d'éviter la fragmentation.

Amendement 7
Proposition de directive
Considérant 12 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	(12 quater) La Commission devrait également publier des lignes directrices afin d'aider les États membres à mettre correctement en œuvre les dispositions relatives au champ d'application, et d'évaluer la proportionnalité des obligations énoncées dans la présente directive compte tenu du caractère critique des entités entrant dans le champ d'application, en particulier lorsqu'elles

s'appliquent aux entités dotées d'un modèle économique ou d'environnements d'exploitation complexes, au titre desquels ces dernières peuvent satisfaire à la fois aux critères attribués aux entités essentielles et importantes, ou exercer simultanément des activités dont certaines relèvent du champ d'application de la présente directive et d'autres non. Dans les cas où l'activité principale des entités se situe en dehors du champ d'application de la présente directive, mais qu'une autre activité secondaire entre dans le champ d'application, les dispositions ne devraient s'appliquer qu'au niveau des fonctions ou des unités au sein d'une entité relevant du champ d'application de la présente directive.

Amendement 8
Proposition de directive
Considérant 14

Texte proposé par la Commission	*Amendement*
(14) Vu les liens qui existent entre la cybersécurité et la sécurité physique des entités, il convient d'assurer la cohérence des approches entre la directive (UE) XXXX/XXXX du Parlement européen et du Conseil[17] et la présente directive. À cet effet, les États membres devraient veiller à ce que les entités critiques et les entités équivalentes, au titre de la directive (UE) XXXX/XXXX, soient considérées comme des entités essentielles en vertu de la présente directive. Les États membres devraient également veiller à ce que leurs stratégies de cybersécurité prévoient un cadre politique pour une coordination renforcée entre l'autorité compétente en vertu de la présente directive et l'autorité compétente en vertu de la directive (UE) XXXX/XXXX dans le cadre du partage d'informations relatives aux incidents et aux cybermenaces ainsi que de l'exercice des tâches de surveillance. Les autorités en vertu des deux directives devraient	(14) Vu les liens qui existent entre la cybersécurité et la sécurité physique des entités, il convient d'assurer la cohérence des approches entre la directive (UE) XXXX/XXXX du Parlement européen et du Conseil[17] et la présente directive. À cet effet, les États membres devraient veiller à ce que les entités critiques et les entités équivalentes, au titre de la directive (UE) XXXX/XXXX, soient considérées comme des entités essentielles en vertu de la présente directive. Les États membres devraient également veiller à ce que leurs stratégies ***nationales*** de cybersécurité prévoient un cadre politique pour une coordination renforcée entre l'autorité compétente en vertu de la présente directive et l'autorité compétente en vertu de la directive (UE) XXXX/XXXX dans le cadre du ***signalement d'incidents, du*** partage d'informations relatives aux incidents***, aux incidents évités*** et aux cybermenaces ainsi que de l'exercice des

coopérer et échanger des informations, notamment en ce qui concerne le recensement des entités critiques, les cybermenaces, les risques en matière de cybersécurité, les incidents affectant les entités critiques ainsi que les mesures de cybersécurité adoptées par les entités critiques. Sur demande des autorités compétentes au titre de la directive (UE) XXX/XXX, les autorités compétentes au titre de la présente directive devraient être autorisées à exercer leurs pouvoirs de surveillance et d'exécution sur une entité essentielle définie comme critique. Les deux autorités devraient coopérer et échanger des informations à cette fin.

tâches de surveillance. Les autorités en vertu des deux directives devraient coopérer et échanger des informations, notamment en ce qui concerne le recensement des entités critiques, les cybermenaces, les risques en matière de cybersécurité, les incidents affectant les entités critiques ainsi que les mesures de cybersécurité adoptées par les entités critiques. Sur demande des autorités compétentes au titre de la directive (UE) XXX/XXX, les autorités compétentes au titre de la présente directive devraient être autorisées à exercer leurs pouvoirs de surveillance et d'exécution sur une entité essentielle définie comme critique. Les deux autorités devraient coopérer et échanger des informations à cette fin.

---

[17][insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]

[17] [insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]

Amendement 9
Proposition de directive
Considérant 15

Texte proposé par la Commission

(15) Le fait de maintenir et préserver un système de noms de domaines (DNS) fiable, résilient et sécurisé constitue un facteur crucial pour la protection de l'intégrité d'internet et est essentiel à son fonctionnement continu et stable, dont dépendent l'économie numérique et la société. Par conséquent, la présente directive devrait s'appliquer à tous les fournisseurs de services DNS, y compris les opérateurs de serveurs racines de noms de domaines, aux serveurs de noms de domaines de premier niveau (TLD), aux serveurs d'autorité pour les noms de domaines et aux résolveurs récursifs.

Amendement

(15) Le fait de maintenir et préserver un système de noms de domaines (DNS) fiable, résilient et sécurisé constitue un facteur crucial pour la protection de l'intégrité d'internet et est essentiel à son fonctionnement continu et stable, dont dépendent l'économie numérique***, le marché intérieur*** et la société. Par conséquent, la présente directive devrait s'appliquer à tous les fournisseurs de services DNS, y compris les opérateurs de serveurs racines de noms de domaines, aux serveurs de noms de domaines de premier niveau (TLD), aux serveurs d'autorité pour les noms de domaines et aux résolveurs récursifs***, ainsi qu'aux fournisseurs de services d'anonymisation et de services d'enregistrement fiduciaire, les courtiers***

	ou les revendeurs de domaines, et tout autre service lié à l'enregistrement des noms de domaines.

Amendement 10
Proposition de directive
Considérant 20

Texte proposé par la Commission	*Amendement*
(20) Ces interdépendances croissantes découlent d'un réseau de fourniture de services de plus en plus transfrontière et interdépendant, qui utilise des infrastructures essentielles dans toute l'Union dans les secteurs de l'énergie, des transports, des infrastructures numériques, de l'eau potable, des eaux usées, de la santé, de certains aspects de l'administration publique et de l'espace, dans la mesure où la fourniture de certains services dépendant de structures terrestres détenues, gérées et exploitées par des États membres ou par des parties privées est concernée, ce qui ne couvre donc pas les infrastructures détenues, gérées ou exploitées par ou au nom de l'Union dans le cadre de ses programmes spatiaux. Ces interdépendances signifient que toute perturbation, même initialement limitée à une entité ou un secteur, peut produire des effets en cascade plus larges, entraînant éventuellement des incidences négatives durables et de grande ampleur pour la fourniture de services dans l'ensemble du marché intérieur. La pandémie de COVID-19 a mis en évidence la vulnérabilité de nos sociétés de plus en plus interdépendantes face à des risques peu probables.	(20) Ces interdépendances croissantes découlent d'un réseau de fourniture de services de plus en plus transfrontière et interdépendant, qui utilise des infrastructures essentielles dans toute l'Union dans les secteurs de l'énergie, des transports, des infrastructures numériques, de l'eau potable, des eaux usées, de la santé, de certains aspects de l'administration publique et de l'espace, dans la mesure où la fourniture de certains services dépendant de structures terrestres détenues, gérées et exploitées par des États membres ou par des parties privées est concernée, ce qui ne couvre donc pas les infrastructures détenues, gérées ou exploitées par ou au nom de l'Union dans le cadre de ses programmes spatiaux. Ces interdépendances signifient que toute perturbation, même initialement limitée à une entité ou un secteur, peut produire des effets en cascade plus larges, entraînant éventuellement des incidences négatives durables et de grande ampleur pour la fourniture de services dans l'ensemble du marché intérieur. La pandémie de COVID-19 a mis en évidence la vulnérabilité de nos sociétés de plus en plus interdépendantes face à des risques peu probables ***et la nécessité de protéger le marché intérieur au moyen de stratégies et d'actions communes à l'échelle de l'Union***.

Amendement 11
Proposition de directive
Considérant 23

Texte proposé par la Commission	*Amendement*
(23) Les autorités compétentes ou les CSIRT devraient recevoir les notifications d'incidents provenant des entités de manière efficace et efficiente. Les points de contact uniques devraient être chargés de transmettre les notifications d'incidents aux points de contact uniques des autres États membres touchés. ***Au niveau des autorités des États membres,*** afin de garantir l'existence d'un seul point d'entrée dans chaque État membre, les points de contact uniques devraient également être les destinataires des informations pertinentes portant sur les incidents concernant les entités du secteur financier fournies par les autorités compétentes au titre du règlement XXXX/XXXX, qu'ils devraient pouvoir transmettre, le cas échéant, aux autorités nationales compétentes ou aux CSIRT en vertu de la présente directive.	(23) Les autorités compétentes ou les CSIRT devraient recevoir les notifications d'incidents provenant des entités de manière ***standardisée,*** efficace et efficiente. Les points de contact uniques devraient être chargés de transmettre les notifications d'incidents aux points de contact uniques des autres États membres touchés. Afin de garantir l'existence d'un seul point d'entrée dans chaque État membre, les points de contact uniques devraient également être les destinataires des informations pertinentes portant sur les incidents concernant les entités du secteur financier fournies par les autorités compétentes au titre du règlement XXXX/XXXX, qu'ils devraient pouvoir transmettre, le cas échéant, aux autorités nationales compétentes ou aux CSIRT en vertu de la présente directive.

Amendement 12
Proposition de directive
Considérant 25

Texte proposé par la Commission	*Amendement*
(25) En ce qui concerne les données à caractère personnel, les CSIRT devraient être en mesure de réaliser, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil[19] relatif aux données à caractère personnel, au nom et sur demande d'une entité en vertu de la présente directive, une analyse des réseaux et des systèmes d'information utilisés pour la fourniture de leurs services. Les États membres devraient avoir pour but d'assurer l'égalité du niveau des capacités techniques de tous les CSIRT sectoriels. Les États membres peuvent solliciter l'assistance de	(25) ***Afin de détecter, d'atténuer et d'éviter les menaces spécifiques en*** ce qui concerne les données à caractère personnel, les CSIRT devraient être en mesure de réaliser, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil[19] relatif aux données à caractère personnel, au nom et sur demande d'une entité en vertu de la présente directive, une analyse ***proactive*** des réseaux et des systèmes d'information utilisés pour la fourniture de leurs services. Les États membres devraient avoir pour but d'assurer l'égalité du niveau des

l’agence européenne pour la cybersécurité (ENISA) pour la mise en place des CSIRT nationaux.

capacités techniques de tous les CSIRT sectoriels. Les États membres peuvent solliciter l’assistance de l’agence européenne pour la cybersécurité (ENISA) pour la mise en place des CSIRT nationaux.

---

[19]Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

[19]Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

Amendement 13
Proposition de directive
Considérant 26 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(26 bis) Dans le cadre de leurs stratégies nationales en matière de cybersécurité, les États membres devraient adopter des politiques de promotion et d’intégration de systèmes intelligents en vue de la prévention et de la détection des incidents et des menaces de cybersécurité. Les États membres devraient mettre en place, conformément à leurs stratégies nationales en matière de cybersécurité, des politiques axées sur la sensibilisation à la cybersécurité et la cyberculture, en vue de protéger les consommateurs. Lorsqu’ils adoptent des stratégies nationales de cybersécurité, les États membres devraient veiller à mettre en place des cadres d’action pour traiter la question de l’accès licite à l’information.

Amendement 14
Proposition de directive
Considérant 27

Texte proposé par la Commission	*Amendement*
(27) Conformément à l'annexe de la recommandation (UE) 2017/1584 de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs («plan d'action»)[20] , un incident majeur signifie un incident qui frappe plusieurs États membres ou qui provoque des perturbations dépassant les capacités d'action du seul État membre concerné. En fonction de leur cause et de leurs conséquences, les incidents majeurs peuvent dégénérer et se transformer en crises à part entière, empêchant le bon fonctionnement du marché intérieur. Vu la large portée et, dans la plupart des cas, la nature transfrontalière de ces incidents, les États membres et les institutions, organes et agences compétents de l'Union devraient coopérer au niveau technique, opérationnel et politique afin de coordonner correctement la réaction dans toute l'Union.	(27) Conformément à l'annexe de la recommandation (UE) 2017/1584 de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs («plan d'action»)[20], un incident majeur signifie un incident qui frappe plusieurs États membres ou qui provoque des perturbations dépassant les capacités d'action du seul État membre concerné***, mettant ainsi en péril le marché intérieur***. En fonction de leur cause et de leurs conséquences, les incidents majeurs peuvent dégénérer et se transformer en crises à part entière, empêchant le bon fonctionnement du marché intérieur. Vu la large portée et, dans la plupart des cas, la nature transfrontalière de ces incidents, les États membres et les institutions, organes et agences compétents de l'Union devraient coopérer au niveau technique, opérationnel et politique afin de coordonner correctement la réaction dans toute l'Union.
[20] Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).	[20] Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

Amendement 15
Proposition de directive
Considérant 28

Texte proposé par la Commission	*Amendement*
(28) Puisque l'exploitation des vulnérabilités dans les réseaux et les systèmes d'information peut causer des perturbations et des dommages considérables, l'identification et la correction rapide de ces vulnérabilités est un facteur important de la réduction du risque en matière de cybersécurité. Les	(28) Puisque l'exploitation des vulnérabilités dans les réseaux et les systèmes d'information peut causer des perturbations et des dommages considérables ***touchant les entreprises et les consommateurs***, l'identification et la correction rapide de ces vulnérabilités est un facteur important de la réduction du

entités qui mettent au point de tels systèmes devraient dont établir des procédures appropriées pour gérer les vulnérabilités découvertes. Puisque les vulnérabilités sont souvent découvertes et signalées (divulguées) par des tiers (les entités effectuant le signalement), le fabricant de produits ou le fournisseur de services TIC devraient également mettre en place les procédures nécessaires pour recevoir les informations relatives aux vulnérabilités communiquées par les tiers. À cet égard, les normes internationales ISO/CEI 30111 et ISO/CEI 29417 fournissent des orientations sur la gestion des vulnérabilités et la divulgation des vulnérabilités respectivement. En ce qui concerne la divulgation des vulnérabilités, la coordination entre les entités effectuant le signalement et les fabricants ou les fournisseurs de produits ou de services TIC est particulièrement importante. La divulgation coordonnée des vulnérabilités consiste en un processus structuré dans lequel les vulnérabilités sont signalées aux organisations de manière à leur donner la possibilité de diagnostiquer la vulnérabilité et d'y remédier avant que des informations détaillées à ce sujet soient divulguées à des tiers ou au public. La divulgation coordonnée des vulnérabilités devrait également comprendre la coordination entre l'entité effectuant le signalement et l'organisation en ce qui concerne le calendrier des corrections et la publication des vulnérabilités.

risque en matière de cybersécurité. Les entités qui mettent au point de tels systèmes devraient dont établir des procédures appropriées pour gérer les vulnérabilités découvertes. Puisque les vulnérabilités sont souvent découvertes et signalées (divulguées) par des tiers (les entités effectuant le signalement), le fabricant de produits ou le fournisseur de services TIC devraient également mettre en place les procédures nécessaires pour recevoir les informations relatives aux vulnérabilités communiquées par les tiers. À cet égard, les normes internationales ISO/CEI 30111 et ISO/CEI 29417 fournissent des orientations sur la gestion des vulnérabilités et la divulgation des vulnérabilités respectivement. En ce qui concerne la divulgation des vulnérabilités, la coordination entre les entités effectuant le signalement et les fabricants ou les fournisseurs de produits ou de services TIC est particulièrement importante. La divulgation coordonnée des vulnérabilités consiste en un processus structuré dans lequel les vulnérabilités sont signalées aux organisations de manière à leur donner la possibilité de diagnostiquer la vulnérabilité et d'y remédier avant que des informations détaillées à ce sujet soient divulguées à des tiers ou au public. La divulgation coordonnée des vulnérabilités devrait également comprendre la coordination entre l'entité effectuant le signalement et l'organisation en ce qui concerne le calendrier des corrections et la publication des vulnérabilités.

Amendement 16
Proposition de directive
Considérant 28 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(28 bis) La Commission, l'ENISA et les États membres devraient continuer à encourager l'harmonisation internationale avec les normes et les

bonnes pratiques existantes du secteur dans le domaine de la gestion des risques, par exemple dans les domaines des évaluations de la sécurité de la chaîne d'approvisionnement, du partage d'informations et de la divulgation des vulnérabilités.

Amendement 17
Proposition de directive
Considérant 30

Texte proposé par la Commission	*Amendement*
(30) L'accès en temps utile à des informations correctes relatives aux vulnérabilités touchant les produits et services TIC contribue à une meilleure gestion des risques en matière de cybersécurité. À cet égard, les sources d'informations publiquement accessibles concernant les vulnérabilités sont des outils importants pour les entités et leurs utilisateurs, mais également pour les autorités nationales compétentes et les CSIRT. C'est pour cette raison que l'ENISA devrait mettre en place ***un registre*** des vulnérabilités dans ***lequel*** les entités essentielles et importantes et leurs fournisseurs, ainsi que les entités qui ne relèvent pas du champ d'application de la présente directive, peuvent, à titre volontaire, divulguer les vulnérabilités et fournir des informations à cet égard afin de permettre aux utilisateurs de prendre les mesures d'atténuation appropriées.	(30) L'accès en temps utile à des informations correctes relatives aux vulnérabilités touchant les produits et services TIC contribue à une meilleure gestion des risques en matière de cybersécurité. À cet égard, les sources d'informations publiquement accessibles concernant les vulnérabilités sont des outils importants pour les entités et leurs utilisateurs, mais également pour les autorités nationales compétentes et les CSIRT. C'est pour cette raison que l'ENISA devrait mettre en place ***une base de données*** des vulnérabilités dans ***laquelle*** les entités essentielles et importantes et leurs fournisseurs, ainsi que les entités qui ne relèvent pas du champ d'application de la présente directive, peuvent, à titre volontaire, divulguer les vulnérabilités et fournir des informations à cet égard afin de permettre aux utilisateurs de prendre les mesures d'atténuation appropriées.

Amendement 18
Proposition de directive
Considérant 31

Texte proposé par la Commission	*Amendement*
(31) Bien que des registres ou des bases de données similaires sur les vulnérabilités existent, ils sont hébergés et gérés par des	(31) Bien que des registres ou des bases de données similaires sur les vulnérabilités existent, ils sont hébergés et gérés par des

entités qui ne sont pas établies dans l'Union. ***Un registre européen*** des vulnérabilités ***géré*** par l'ENISA améliorerait la transparence du processus de publication avant la divulgation officielle d'une vulnérabilité et la résilience en cas de perturbation ou d'interruption de la fourniture de services similaires. Afin d'éviter la duplication des efforts déployés et de viser la complémentarité dans la mesure du possible, l'ENISA devrait étudier la possibilité de conclure des accords de coopération structurés avec les registres ***existants*** sur le territoire de pays tiers.

entités qui ne sont pas établies dans l'Union. ***Une base de données européenne*** des vulnérabilités ***gérée*** par l'ENISA améliorerait la transparence du processus de publication avant la divulgation officielle d'une vulnérabilité et la résilience en cas de perturbation ou d'interruption de la fourniture de services similaires. Afin d'éviter la duplication des efforts déployés et de viser la complémentarité dans la mesure du possible, l'ENISA devrait étudier la possibilité de conclure des accords de coopération structurés avec les ***bases de données ou*** registres ***sur les vulnérabilités*** sur le territoire de pays tiers ***et de transmettre des rapports aux registres appropriés, à condition que ces actions ne portent pas atteinte à la protection de la confidentialité et des secrets d'affaires***.

Amendement 19
Proposition de directive
Considérant 32

Texte proposé par la Commission	*Amendement*
(32) Tous les deux ans, le groupe de coopération devrait élaborer un programme de travail qui inclurait les actions qu'il doit réaliser afin de mettre en œuvre ses objectifs et ses tâches. Le calendrier du premier programme adopté au titre de la présente directive devrait être aligné sur le calendrier du dernier programme adopté au titre de la directive (UE) 2016/1148 afin d'éviter de perturber les travaux du groupe.	(32) Tous les deux ans, le groupe de coopération devrait ***débattre des priorités politiques et des principaux défis en matière de cybersécurité, et*** élaborer un programme de travail qui inclurait les actions qu'il doit réaliser afin de mettre en œuvre ses objectifs et ses tâches. Le calendrier du premier programme adopté au titre de la présente directive devrait être aligné sur le calendrier du dernier programme adopté au titre de la directive (UE) 2016/1148 afin d'éviter de perturber les travaux du groupe.

Amendement 20
Proposition de directive
Considérant 32 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(32 bis) Le groupe de coopération devrait être composé de représentants des États membres, de la Commission et de l'ENISA.

Amendement 21
Proposition de directive
Considérant 34

Texte proposé par la Commission	*Amendement*
(34) Le groupe de coopération devrait conserver sa forme de forum flexible et continuer d'être en mesure de réagir aux priorités politiques et aux difficultés nouvelles et en évolution, tout en tenant compte de la disponibilité des ressources. Il devrait régulièrement organiser des réunions conjointes avec les parties intéressées privées de toute l'Union en vue de discuter des activités menées par le groupe et de recueillir des informations sur les nouveaux défis politiques. Afin d'améliorer la coopération au niveau de l'Union, le groupe devrait envisager d'inviter les organes et agences de l'Union participant à la politique de cybersécurité, comme le Centre européen de lutte contre la cybercriminalité (EC3), l'Agence de l'Union européenne pour la sécurité aérienne (AESA) et l'Agence de l'Union européenne pour le programme spatial (EUSPA), à participer à ses travaux.	(34) Le groupe de coopération devrait conserver sa forme de forum flexible et continuer d'être en mesure de réagir aux priorités politiques et aux difficultés nouvelles et en évolution, tout en tenant compte de la disponibilité des ressources. Il devrait régulièrement organiser des réunions conjointes avec les parties intéressées privées de toute l'Union en vue de discuter des activités menées par le groupe et de recueillir des informations sur les nouveaux défis politiques. Afin d'améliorer la coopération au niveau de l'Union, le groupe devrait envisager d'inviter les organes et agences de l'Union participant à la politique de cybersécurité, comme le Centre européen de lutte contre la cybercriminalité (EC3), l'Agence de l'Union européenne pour la sécurité aérienne (AESA) et l'Agence de l'Union européenne pour le programme spatial (EUSPA), ***ainsi que d'autres organes et agences compétents de l'Union*** à participer à ses travaux.

Amendement 22
Proposition de directive
Considérant 35

Texte proposé par la Commission	*Amendement*
(35) Les autorités compétentes et les	(35) Les autorités compétentes et les

CSIRT devraient pouvoir participer ***aux*** programmes d'échange ***d'agents*** provenant d'autres États membres afin d'améliorer la coopération. Elles devraient prendre les mesures nécessaires pour que les agents d'autres États membres puissent jouer un rôle effectif dans les activités de l'autorité compétente hôte.	CSIRT devraient pouvoir participer ***à des*** programmes d'échange ***et des programmes de formation en commun pour les agents*** provenant d'autres États membres afin d'améliorer la coopération ***et de renforcer la confiance entre les États membres***. Elles devraient prendre les mesures nécessaires pour que les agents d'autres États membres puissent jouer un rôle effectif dans les activités de l'autorité compétente hôte ***ou du CSIRT***.

Amendement 23
Proposition de directive
Considérant 39

Texte proposé par la Commission	*Amendement*
(39) Aux fins de la présente directive, le terme «incidents évités» devrait faire référence à un événement qui aurait potentiellement pu causer des dommages, mais dont la réalisation totale a pu être empêchée.	***supprimé***

Amendement 24
Proposition de directive
Considérant 45 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(45 bis) En outre, les entités devraient également assurer une éducation et une formation adéquates à leur personnel en matière de cybersécurité à tous les niveaux de l'organisation.

Amendement 25
Proposition de directive
Considérant 46

Texte proposé par la Commission	*Amendement*
(46) Afin de mieux répondre aux risques principaux liés aux chaînes	(46) Afin de mieux répondre aux risques principaux liés aux chaînes

d'approvisionnement et d'aider les entités actives dans les secteurs couverts par la présente directive à bien gérer les risques de cybersécurité liés aux chaînes d'approvisionnement et aux fournisseurs, le groupe de coopération impliquant les autorités nationales compétentes, en collaboration avec la Commission et l'ENISA, devrait réaliser des évaluations coordonnées sectorielles des risques liés aux chaînes d'approvisionnement, comme cela a été le cas pour les réseaux 5G suite à la recommandation (UE) 2019/534 sur la cybersécurité des réseaux 5G[21] , dans le but de déterminer, ***secteur par*** secteur, les services, systèmes ou produits TIC critiques, les menaces pertinentes et les vulnérabilités.

d'approvisionnement et d'aider les entités actives dans les secteurs couverts par la présente directive à bien gérer les risques de cybersécurité liés aux chaînes d'approvisionnement et aux fournisseurs, le groupe de coopération impliquant les autorités nationales compétentes, en collaboration avec la Commission et l'ENISA, devrait réaliser des évaluations coordonnées sectorielles des risques liés aux chaînes d'approvisionnement, comme cela a été le cas pour les réseaux 5G suite à la recommandation (UE) 2019/534 sur la cybersécurité des réseaux 5G[21], dans le but de déterminer, ***dans chaque*** secteur, les services, systèmes ou produits TIC critiques, les menaces pertinentes et les vulnérabilités.

[21] Recommandation (UE) 2019/534 de la Commission du 26 mars 2019 Cybersécurité des réseaux 5G (JO L 88 du 29.3.2019, p. 42).

[21] Recommandation (UE) 2019/534 de la Commission du 26 mars 2019 Cybersécurité des réseaux 5G (JO L 88 du 29.3.2019, p. 42).

Amendement 26
Proposition de directive
Considérant 47

Texte proposé par la Commission

(47) Les évaluations des risques liés aux chaînes d'approvisionnement, à la lumière des caractéristiques du secteur concerné, devraient tenir compte des facteurs techniques et, le cas échéant, non techniques, y compris ceux définis dans la recommandation (UE) 2019/534, dans l'évaluation coordonnée à l'échelle de l'Union des risques concernant la sécurité des réseaux 5G et dans la boîte à outils de l'UE pour la cybersécurité 5G convenue par le groupe de coopération. Afin de déterminer quelles chaînes d'approvisionnement devraient être soumises à une évaluation coordonnée des risques, il convient de tenir compte des critères suivants: i) la mesure dans laquelle

Amendement

(47) Les évaluations des risques liés aux chaînes d'approvisionnement, à la lumière des caractéristiques du secteur concerné ***et de sa criticité***, devraient tenir compte des facteurs techniques et, le cas échéant, non techniques, y compris ceux définis dans la recommandation (UE) 2019/534, dans l'évaluation coordonnée à l'échelle de l'Union des risques concernant la sécurité des réseaux 5G et dans la boîte à outils de l'UE pour la cybersécurité 5G convenue par le groupe de coopération. Afin de déterminer quelles chaînes d'approvisionnement devraient être soumises à une évaluation coordonnée des risques, il convient de tenir compte des critères suivants: i) la mesure dans laquelle

les entités essentielles et importantes utilisent des services, systèmes ou produits TIC critiques spécifiques et en dépendent; ii) la pertinence des services, systèmes ou produits TIC critiques spécifiques pour la réalisation des fonctions sensibles ou critiques, notamment le traitement de données à caractère personnel; iii) la disponibilité d'autres services, systèmes ou produits TIC; iv) la résilience de la chaîne d'approvisionnement générale des services, systèmes ou produits TIC face aux événements perturbateurs et v) concernant les services, systèmes ou produits TIC émergents, leur potentielle importance à l'avenir pour les activités des entités.	les entités essentielles et importantes utilisent des services, systèmes ou produits TIC critiques spécifiques et en dépendent; ii) la pertinence des services, systèmes ou produits TIC critiques spécifiques pour la réalisation des fonctions sensibles ou critiques, notamment le traitement de données à caractère personnel; iii) la disponibilité d'autres services, systèmes ou produits TIC; iv) la résilience de la chaîne d'approvisionnement générale des services, systèmes ou produits TIC face aux événements perturbateurs et v) concernant les services, systèmes ou produits TIC émergents, leur potentielle importance à l'avenir pour les activités des entités.

Amendement 27
Proposition de directive
Considérant 51

Texte proposé par la Commission	*Amendement*
(51) Le marché intérieur dépend plus que jamais du fonctionnement d'internet. Les services de la quasi-totalité des entités essentielles et importantes dépendent de services fournis sur internet. Afin d'assurer la prestation harmonieuse des services fournis par les entités essentielles et importantes, il est important que les réseaux de communications électroniques publics, comme les dorsales internet ou les câbles de communication sous-marins, disposent de mesures de cybersécurité appropriées et signalent les incidents qui les concernent.	(51) Le marché intérieur dépend plus que jamais du fonctionnement d'internet. Les services de la quasi-totalité des entités essentielles et importantes dépendent de services fournis sur internet ***et les consommateurs dépendent de l'internet pour des éléments essentiels de leur vie quotidienne***. Afin d'assurer la prestation harmonieuse des services fournis par les entités essentielles et importantes, il est important que les réseaux de communications électroniques publics, comme les dorsales internet ou les câbles de communication sous-marins, disposent de mesures de cybersécurité appropriées et signalent les incidents qui les concernent.

Amendement 28
Proposition de directive
Considérant 52

Texte proposé par la Commission	*Amendement*
(52) ***Lorsque cela est approprié, les entités devraient*** informer les destinataires de leurs services des menaces importantes et considérables, ainsi que des mesures qu'ils peuvent prendre pour atténuer le risque qui en résulte pour eux***. L'obligation qui est faite aux entités d'informer les destinataires de ces menaces*** ne devrait pas les dispenser de l'obligation de prendre immédiatement, à leurs frais, les mesures appropriées pour prévenir ou remédier à toute cybermenace pour la sécurité et pour rétablir le niveau normal de sécurité du service. ***Informer les*** destinataires au sujet des menaces pour la sécurité devrait être ***gratuit***.	(52) ***Les entités devraient viser à*** informer les destinataires de leurs services des menaces importantes et considérables, ainsi que des mesures qu'ils peuvent prendre pour atténuer le risque qui en résulte pour eux***, en particulier lorsque ces mesures sont susceptibles d'améliorer la protection des consommateurs. Cela*** ne devrait pas les dispenser de l'obligation de prendre immédiatement, à leurs frais, les mesures appropriées pour prévenir ou remédier à toute cybermenace pour la sécurité et pour rétablir le niveau normal de sécurité du service. ***L'information fournie aux*** destinataires au sujet des menaces pour la sécurité devrait être ***gratuite et formulée dans un langage facile à comprendre***.

Amendement 29
Proposition de directive
Considérant 53

Texte proposé par la Commission	*Amendement*
(53) Plus particulièrement, il convient que les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public informent les destinataires des services des cybermenaces particulières et importantes pour la sécurité et des mesures qu'ils peuvent prendre pour sécuriser leurs communications, par exemple en recourant à des types spécifiques de logiciels ou de techniques de chiffrement.	(53) Plus particulièrement, il convient que les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public informent les destinataires des services des cybermenaces particulières et importantes pour la sécurité et des mesures ***supplémentaires*** qu'ils peuvent prendre pour sécuriser leurs ***appareils et*** communications, par exemple en recourant à des types spécifiques de logiciels ou de techniques de chiffrement.

Amendement 30
Proposition de directive
Considérant 54

Texte proposé par la Commission	*Amendement*
(54) Afin de préserver la sécurité des réseaux et services de communications électroniques, il convient d'encourager l'utilisation du chiffrement, notamment du chiffrement de bout en bout, voire si nécessaire de l'imposer, pour les fournisseurs de ces services et réseaux, conformément aux principes de sécurité et de respect de la vie privée par défaut et dès la conception aux fins de ***l'article 18. Il convient*** de ***concilier*** l'utilisation du chiffrement de bout en bout ***avec les*** pouvoirs dont disposent les États membres pour garantir la protection de leurs intérêts essentiels de sécurité et de la sécurité publique et pour permettre la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union. Les solutions pour un accès légal aux informations contenues dans les communications chiffrées de bout en bout devraient préserver l'efficacité du cryptage pour ce qui est de la protection de la vie privée et de la sécurité des communications, tout en apportant une réponse efficace à la criminalité.	(54) Afin de préserver la sécurité des réseaux et services de communications électroniques, il convient d'encourager l'utilisation du chiffrement, notamment du chiffrement de bout en bout, voire si nécessaire de l'imposer, pour les fournisseurs de ces services et réseaux, conformément aux principes de sécurité et de respect de la vie privée par défaut et dès la conception aux fins ***des mesures de gestion du risque en matière de cybersécurité.*** L'utilisation du chiffrement de bout en bout ***ne porte pas préjudice aux*** pouvoirs***, aux politiques et aux procédures*** dont disposent les États membres pour garantir la protection de leurs intérêts essentiels de sécurité et de la sécurité publique et pour permettre la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union. Les solutions pour un accès légal aux informations contenues dans les communications chiffrées de bout en bout devraient préserver l'efficacité du cryptage pour ce qui est de la protection de la vie privée et de la sécurité des communications, tout en apportant une réponse efficace à la criminalité. ***Toute action entreprise doit respecter strictement les principes de proportionnalité et de subsidiarité.***

Amendement 31
Proposition de directive
Considérant 55

Texte proposé par la Commission	*Amendement*
(55) La présente directive établit une approche ***en deux étapes*** du signalement des incidents afin de trouver le juste équilibre entre, d'une part, le signalement rapide qui aide à atténuer la propagation potentielle des incidents et permet aux entités de chercher de l'aide et, d'autre	(55) La présente directive établit une approche ***consécutive*** du signalement des incidents afin de trouver le juste équilibre entre, d'une part, le signalement rapide qui aide à atténuer la propagation potentielle des incidents et permet aux entités de chercher de l'aide et, d'autre part, le

part, le signalement approfondi qui permet de tirer des leçons précieuses des incidents individuels et d'améliorer au fil du temps la résilience des entreprises individuelles et de secteurs tout entiers face aux cybermenaces. Lorsque les entités prennent connaissance d'un incident, elles devraient être tenues de présenter une notification initiale dans les ***24*** heures, suivie d'un rapport ***final un*** mois après au plus tard. La notification initiale ne devrait inclure que les informations strictement nécessaires pour porter l'incident à la connaissance des autorités compétentes et permettre à l'entité de demander une assistance, le cas échéant. Cette notification, le cas échéant, devrait indiquer si l'incident semble être causé par des actions illégales ou malveillantes. Les États membres devraient veiller à ce que l'obligation de présenter cette notification initiale ne détourne pas les ressources de l'entité effectuant le signalement des activités liées à la gestion de l'incident, qui doivent être prioritaires. Afin ***d'évider*** que les obligations de signalement des incidents détournent les ressources des activités de gestion des incidents ou compromettent de quelque manière que ce soit les efforts déployés par les entités à cet égard, les États membres devraient également prévoir que, dans des cas dûment justifiés et en accord avec les autorités compétentes ou avec le CSIRT, l'entité concernée peut ne pas respecter les délais ***de 24 heures pour la notification initiale et de un mois pour le rapport final***.

signalement approfondi qui permet de tirer des leçons précieuses des incidents individuels et d'améliorer au fil du temps la résilience des entreprises individuelles et de secteurs tout entiers face aux cybermenaces. Lorsque les entités prennent connaissance d'un incident ***ou d'un incident évité***, elles devraient être tenues de présenter une notification initiale dans les ***72*** heures, suivie d'un rapport ***complet au plus tard trois*** mois après ***la présentation de la notification initiale, et d'un rapport final*** au plus tard ***un mois après avoir remédié à l'incident***. La notification initiale ne devrait inclure que les informations strictement nécessaires pour porter l'incident à la connaissance des autorités compétentes et permettre à l'entité de demander une assistance, le cas échéant. Cette notification, le cas échéant, devrait indiquer si l'incident semble être causé par des actions illégales ou malveillantes. Les États membres devraient veiller à ce que l'obligation de présenter cette notification initiale ne détourne pas les ressources de l'entité effectuant le signalement des activités liées à la gestion de l'incident, qui doivent être prioritaires. ***La notification initiale devrait être précédée d'une alerte précoce dans les 24 premières heures, sans obligation de communication d'informations supplémentaires. Ce premier avertissement devrait être soumis dès que possible, ce qui permettrait aux entités de demander rapidement l'aide des autorités compétentes ou des CSIRT et aux autorités compétentes ou aux CSIRT de limiter la propagation potentielle de l'incident signalé, ainsi qu'aux CSIRT de bénéficier d'un outil de connaissance de la situation.*** Afin ***d'éviter*** que les obligations de signalement des incidents détournent les ressources des activités de gestion des incidents ou compromettent de quelque manière que ce soit les efforts déployés par les entités à cet égard, les États membres devraient également prévoir que, dans des cas dûment justifiés et en

accord avec les autorités compétentes ou avec le CSIRT, l'entité concernée peut ne pas respecter les délais ***prévus***.

Amendement 32
Proposition de directive
Considérant 56

Texte proposé par la Commission	*Amendement*
(56) Les entités essentielles et importantes se retrouvent souvent dans une situation dans laquelle un incident en particulier, en raison de ses caractéristiques, doit être signalé à différentes autorités en raison d'obligations de notification incluses dans différents instruments juridiques. De tels cas créent des charges supplémentaires et peuvent également conduire à des incertitudes en ce qui concerne le format et les procédures de ces notifications. C'est pourquoi, afin de simplifier le signalement des incidents de sécurité, les États membres devraient mettre en place un point d'entrée unique pour toutes les notifications requises en vertu de la présente directive et d'autres actes législatifs de l'Union, comme le règlement (UE) 2016/679 et la directive 2002/58/CE. L'ENISA, en collaboration avec le groupe de coopération, devrait mettre au point des formulaires de notification communs au moyen de lignes directrices qui permettraient de simplifier et de rationaliser les informations de signalement exigées par le droit de l'Union et de réduire les charges pesant sur les entreprises.	(56) Les entités essentielles et importantes se retrouvent souvent dans une situation dans laquelle un incident en particulier, en raison de ses caractéristiques, doit être signalé à différentes autorités en raison d'obligations de notification incluses dans différents instruments juridiques. De tels cas créent des charges supplémentaires et peuvent également conduire à des incertitudes en ce qui concerne le format et les procédures de ces notifications. C'est pourquoi, afin de simplifier le signalement des incidents de sécurité ***et de respecter le principe de la transmission unique d'informations***, les États membres devraient mettre en place un point d'entrée unique pour toutes les notifications requises en vertu de la présente directive et d'autres actes législatifs de l'Union, comme le règlement (UE) 2016/679 et la directive 2002/58/CE. L'ENISA, en collaboration avec le groupe de coopération, devrait mettre au point des formulaires de notification communs au moyen de lignes directrices qui permettraient de simplifier et de rationaliser les informations de signalement exigées par le droit de l'Union et de réduire les charges pesant sur les entreprises.

Amendement 33
Proposition de directive
Considérant 59

Texte proposé par la Commission	*Amendement*
(59) Le maintien à jour des bases de données précises et complètes de noms de domaines et de données d'enregistrement (appelées «données WHOIS») ainsi que la fourniture d'un accès licite à ces données sont essentiels pour garantir la sécurité, la stabilité et la résilience du système de noms de domaines (DNS), lequel contribue en retour à assurer un niveau élevé commun de cybersécurité dans l'Union. Lorsque le traitement comprend des données à caractère personnel, ce traitement doit s'effectuer conformément au droit de l'Union en matière de protection des données.	(59) Le maintien à jour des bases de données précises***, vérifiées*** et complètes de noms de domaines et de données d'enregistrement (appelées «données WHOIS») ainsi que la fourniture d'un accès licite à ces données sont essentiels pour garantir la sécurité, la stabilité et la résilience du système de noms de domaines (DNS), lequel contribue en retour à assurer un niveau élevé commun de cybersécurité dans l'Union. Lorsque le traitement comprend des données à caractère personnel, ce traitement doit s'effectuer conformément au droit de l'Union en matière de protection des données.

Amendement 34
Proposition de directive
Considérant 61

Texte proposé par la Commission	*Amendement*
(61) Afin d'assurer la disponibilité de données exactes et complètes sur l'enregistrement des noms de domaines, les registres des noms de domaines de premier niveau ainsi que les entités qui fournissent des services d'enregistrement de noms de domaines ***pour le registre*** de noms de domaines de ***premier niveau (appelées «bureaux d'enregistrement»***) doivent collecter et garantir l'intégrité et la disponibilité des données relatives à l'enregistrement des noms de domaines. En particulier, les registres de noms domaines de premier niveau ainsi que les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau devraient établir des politiques et des procédures aux fins de collecter et maintenir des données d'enregistrement exactes et complètes, ainsi que pour prévenir et corriger les données d'enregistrement inexactes, conformément	(61) Afin d'assurer la disponibilité de données exactes et complètes sur l'enregistrement des noms de domaines, les registres des noms de domaines de premier niveau ainsi que les entités qui fournissent des services d'enregistrement de noms de domaines ***(y compris les services fournis par les registres*** de noms de domaines ***et les bureaux d'enregistrement, les fournisseurs de services d'anonymisation et de services d'enregistrement fiduciaire, les courtiers ou les revendeurs de domaines, et tout autre service lié à l'enregistrement des noms de domaines***) doivent collecter et garantir l'intégrité et la disponibilité des données relatives à l'enregistrement des noms de domaines. En particulier, les registres de noms domaines de premier niveau ainsi que les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau devraient établir des politiques et des

aux règles de l'Union en matière de protection des données.

procédures aux fins de collecter et maintenir des données d'enregistrement exactes et complètes, ainsi que pour prévenir et corriger les données d'enregistrement inexactes, conformément aux règles de l'Union en matière de protection des données.

Amendement 35
Proposition de directive
Considérant 68

Texte proposé par la Commission	*Amendement*
(68) Les entités devraient être encouragées à exploiter collectivement leurs connaissances individuelles et leur expérience pratique aux niveaux stratégique, tactique et opérationnel en vue d'améliorer leurs capacités à évaluer, surveiller, se défendre et répondre de manière adéquate aux cybermenaces. Il est donc nécessaire de permettre l'émergence, au niveau de l'Union, d'accords de partage volontaire d'informations. À cette fin, les États membres devraient activement soutenir et encourager également les entités concernées qui ne relèvent pas du champ d'application de la présente directive à participer à ces mécanismes d'échange d'informations. Ces mécanismes devraient être opérés dans le plein respect des règles de concurrence de l'Union ainsi que des règles du droit de l'Union en matière de protection des données.	(68) Les entités devraient être encouragées ***et aidées par les États membres*** à exploiter collectivement leurs connaissances individuelles et leur expérience pratique aux niveaux stratégique, tactique et opérationnel en vue d'améliorer leurs capacités à évaluer, surveiller, se défendre et répondre de manière adéquate aux cybermenaces. Il est donc nécessaire de permettre l'émergence, au niveau de l'Union, d'accords de partage volontaire d'informations. À cette fin, les États membres devraient activement soutenir et encourager également les entités concernées qui ne relèvent pas du champ d'application de la présente directive à participer à ces mécanismes d'échange d'informations. Ces mécanismes devraient être opérés dans le plein respect des règles de concurrence de l'Union ainsi que des règles du droit de l'Union en matière de protection des données.

Amendement 36
Proposition de directive
Considérant 69

Texte proposé par la Commission	*Amendement*
(69) Le traitement de données à caractère personnel, ***dans la mesure*** strictement nécessaire et ***proportionnée***	(69) Le traitement de données à caractère personnel, ***qui devrait se limiter à ce qui est*** strictement nécessaire et

aux fins de garantir la sécurité du réseau et des informations par des entités, des autorités publiques, des CERT, des CSIRT et des fournisseurs de technologies et de services de sécurité devrait constituer un intérêt légitime du responsable du traitement concerné, tel que visé dans le règlement (UE) 2016/679. Cela devrait comprendre des mesures liées à la prévention, à la détection, à l'analyse et à la réaction aux incidents, des mesures de sensibilisation à des cybermenaces spécifiques, l'échange d'informations dans le cadre de la correction des vulnérabilités et de la divulgation coordonnée, ainsi que l'échange volontaire d'informations sur ces incidents, les cybermenaces et les vulnérabilités, de même que les indicateurs de compromis, les tactiques, techniques et procédures, les alertes de cybersécurité et les outils de configuration. Ces mesures peuvent nécessiter le traitement des types de données à caractère personnel suivants: Adresses IP, localisateurs de ressources uniformes (URL), noms de domaines et adresses électroniques.

proportionné aux fins de garantir la sécurité du réseau et des informations ***ainsi que de veiller à la protection des consommateurs,*** par des entités, des autorités publiques, des CERT, des CSIRT et des fournisseurs de technologies et de services de sécurité devrait constituer un intérêt légitime du responsable du traitement concerné, tel que visé dans le règlement (UE) 2016/679. Cela devrait comprendre des mesures liées à la prévention, à la détection, à l'analyse et à la réaction aux incidents, des mesures de sensibilisation à des cybermenaces spécifiques, l'échange d'informations dans le cadre de la correction des vulnérabilités et de la divulgation coordonnée, ainsi que l'échange volontaire d'informations sur ces incidents, les cybermenaces et les vulnérabilités, de même que les indicateurs de compromis, les tactiques, techniques et procédures, les alertes de cybersécurité et les outils de configuration. Ces mesures peuvent nécessiter le traitement des types de données à caractère personnel suivants: Adresses IP, localisateurs de ressources uniformes (URL), noms de domaines et adresses électroniques.

Amendement 37
Proposition de directive
Considérant 70

Texte proposé par la Commission	*Amendement*
(70) Afin de renforcer les pouvoirs et actions de surveillance qui contribuent à assurer un respect effectif des règles, la présente directive devrait prévoir une liste minimale d'actions et de moyens de surveillance par lesquels les autorités compétentes peuvent contrôler les entités essentielles et importantes. En outre, la présente directive devrait établir une différenciation du régime de surveillance entre les entités essentielles et les entités importantes en vue de garantir un juste équilibre des obligations tant pour les	(70) Afin de renforcer les pouvoirs et actions de surveillance qui contribuent à assurer un respect effectif des règles ***et d'atteindre un niveau commun élevé de sécurité au sein du secteur numérique, notamment en prévenant les risques pour les utilisateurs et autres réseaux, systèmes d'information et services***, la présente directive devrait prévoir une liste minimale d'actions et de moyens de surveillance par lesquels les autorités compétentes peuvent contrôler les entités essentielles et importantes. En outre, la présente directive

entités que pour les autorités compétentes. Ainsi, les entités essentielles devraient être soumises à un régime de surveillance à part entière (ex ante et ex post), tandis que les entités importantes devraient pour leur part être soumises à un régime de surveillance léger, uniquement ex post. Pour ces dernières, cela signifie que les entités importantes ne sont pas tenues de documenter systématiquement le respect des exigences en matière de gestion des risques de cybersécurité, tandis que les autorités compétentes sont quant à elles invitées à mettre en œuvre une approche réactive de la surveillance ex post et, par conséquent, ne pas être assujetties à une obligation générale de surveillance de ces entités.

devrait établir une différenciation du régime de surveillance entre les entités essentielles et les entités importantes en vue de garantir un juste équilibre des obligations tant pour les entités que pour les autorités compétentes. Ainsi, les entités essentielles devraient être soumises à un régime de surveillance à part entière (ex ante et ex post), tandis que les entités importantes devraient pour leur part être soumises à un régime de surveillance léger, uniquement ex post***, en tenant compte d'une approche fondée sur le risque***. Pour ces dernières, cela signifie que les entités importantes ne sont pas tenues de documenter systématiquement le respect des exigences en matière de gestion des risques de cybersécurité, tandis que les autorités compétentes sont quant à elles invitées à mettre en œuvre une approche réactive de la surveillance ex post et, par conséquent, ne pas être assujetties à une obligation générale de surveillance de ces entités***, sauf en cas de violation avérée des obligations***.

Amendement 38
Proposition de directive
Considérant 76

Texte proposé par la Commission	*Amendement*
(76) Afin de renforcer encore l'efficacité et le caractère dissuasif des sanctions applicables aux violations des obligations prévues en vertu de la présente directive, les autorités compétentes devraient être habilitées à imposer des sanctions consistant en la suspension d'une certification ou d'une autorisation concernant ***tout ou partie des services*** fournis par une entité essentielle ***et en l'interdiction temporaire de l'exercice de fonctions de direction par une personne physique***. Compte tenu de leur gravité et de leur incidence sur les activités des entités et, en définitive, sur leurs consommateurs, ces sanctions ne devraient	(76) Afin de renforcer encore l'efficacité et le caractère dissuasif des sanctions applicables aux violations des obligations prévues en vertu de la présente directive, les autorités compétentes devraient être habilitées à imposer des sanctions consistant en la suspension d'une certification ou d'une autorisation concernant ***les services en question*** fournis par une entité essentielle. Compte tenu de leur gravité et de leur incidence sur les activités des entités et, en définitive, sur leurs consommateurs, ces sanctions ne devraient être appliquées que proportionnellement à la gravité de la violation et en tenant compte des

être appliquées que proportionnellement à la gravité de la violation et en tenant compte des circonstances spécifiques de chaque cas, notamment le caractère intentionnel ou négligent de la violation, les mesures prises pour prévenir ou atténuer les dommages et/ou les pertes subis. Ces sanctions ne devraient être appliquées qu'à titre d'ultima ratio, c'est-à-dire uniquement après que les autres mesures d'exécution pertinentes prévues par la présente directive ont été épuisées, et seulement pendant la période durant laquelle les entités auxquelles elles s'appliquent prennent les mesures nécessaires pour remédier aux manquements ou se conformer aux exigences de l'autorité compétente pour laquelle ces sanctions ont été appliquées. L'imposition de ces sanctions est soumise à des garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et à la charte des droits fondamentaux de l'Union européenne, y compris le droit à une protection juridictionnelle effective, une procédure régulière, la présomption d'innocence et les droits de la défense.	circonstances spécifiques de chaque cas, notamment le caractère intentionnel ou négligent de la violation, les mesures prises pour prévenir ou atténuer les dommages et/ou les pertes subis. Ces sanctions ne devraient être appliquées qu'à titre d'ultima ratio, c'est-à-dire uniquement après que les autres mesures d'exécution pertinentes prévues par la présente directive ont été épuisées, et seulement pendant la période durant laquelle les entités auxquelles elles s'appliquent prennent les mesures nécessaires pour remédier aux manquements ou se conformer aux exigences de l'autorité compétente pour laquelle ces sanctions ont été appliquées. L'imposition de ces sanctions est soumise à des garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et à la charte des droits fondamentaux de l'Union européenne, y compris le droit à une protection juridictionnelle effective, une procédure régulière, la présomption d'innocence et les droits de la défense.

Amendement 39
Proposition de directive
Considérant 79

Texte proposé par la Commission	*Amendement*
(79) Un mécanisme d'évaluation par les pairs devrait être mis en place, permettant l'évaluation par des experts désignés par les États membres de la mise en œuvre des politiques de cybersécurité, y compris le niveau des capacités et des ressources disponibles des États membres.	(79) Un mécanisme d'évaluation par les pairs devrait être mis en place, permettant l'évaluation par des experts désignés par les États membres ***et de l'ENISA*** de la mise en œuvre des politiques de cybersécurité, y compris le niveau des capacités et des ressources disponibles des États membres***, et l'échange de bonnes pratiques***.

Amendement 40
Proposition de directive
Considérant 80

Texte proposé par la Commission	*Amendement*
(80) Afin de tenir compte des nouvelles cybermenaces, de l'évolution technologique ou des spécificités sectorielles, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en ce qui concerne les éléments en rapport avec les mesures de gestion des risques requis en vertu de la présente directive. La Commission devrait également être habilitée à adopter des actes délégués ***établissant quelles catégories d'entités essentielles sont tenues d'obtenir un certificat*** et ***dans le cadre*** de ***quels régimes européens*** de ***certification*** de ***cybersécurité spécifiques***. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer»[26]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.	(80) Afin de tenir compte des nouvelles cybermenaces, de l'évolution technologique ou des spécificités sectorielles, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en ce qui concerne les éléments en rapport avec les mesures de gestion des risques requis en vertu de la présente directive. La Commission devrait ***être habilitée à adopter des actes délégués établissant les éléments techniques des mesures de gestion des risques. La Commission devrait*** également être habilitée à adopter des actes délégués ***qui précisent le type d'informations présentées par les entités essentielles*** et ***importantes au sujet*** de ***tout incident ayant une incidence significative sur la fourniture*** de ***leurs services ou*** de ***tout incident évité, et qui précisent les cas dans lesquels un incident devrait être considéré comme significatif***. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer»[26]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.
[26] JO L 123 du 12.5.2016, p. 1.	[26] JO L 123 du 12.5.2016, p. 1.

Amendement 41
Proposition de directive
Considérant 81

Texte proposé par la Commission	*Amendement*
(81) Afin d'assurer des conditions uniformes de mise en œuvre des dispositions pertinentes de la présente directive concernant les modalités de procédure nécessaires au fonctionnement du groupe de coopération, ***les éléments techniques des mesures de gestion des risques ou le type d'informations,*** le format et la procédure de notification des incidents, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil[27].	(81) Afin d'assurer des conditions uniformes de mise en œuvre des dispositions pertinentes de la présente directive concernant les modalités de procédure nécessaires au fonctionnement du groupe de coopération, le format et la procédure de notification des incidents, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil[27].
[27] Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).	[27] Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

Amendement 42
Proposition de directive
Article 1, paragraphe 1

Texte proposé par la Commission	*Amendement*
1. La présente directive établit des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union.	1. La présente directive établit des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union ***afin de créer un environnement numérique fiable pour les consommateurs et les opérateurs économiques, ainsi que d'améliorer le fonctionnement du marché***

intérieur et d'en supprimer les obstacles.

Amendement 43
Proposition de directive
Article 2 – paragraphe 2 – alinéa 1 – partie introductive

Texte proposé par la Commission	*Amendement*
2. Toutefois, quelle que soit leur taille, la présente directive s'applique également aux entités ***visées*** aux annexes I et II, dans les cas suivants:	2. Toutefois, quelle que soit leur taille, la présente directive s'applique également aux entités ***d'un type visé*** aux annexes I et II, dans les cas suivants:

Amendement 44
Proposition de directive
Article 2 – paragraphe 2 – alinéa 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	La Commission publie des lignes directrices afin d'aider les États membres à mettre correctement en œuvre les dispositions relatives au champ d'application, et afin d'accorder d'éventuelles dérogations au champ d'application de la directive ou à certaines de ses dispositions pour certaines entités importantes, compte tenu de leur faible criticité dans leur secteur spécifique et/ou de leur faible dépendance à l'égard d'autres secteurs ou types de services. Les États membres, en tenant pleinement compte des lignes directrices de la Commission, notifient à la Commission leurs décisions motivées à cet égard.

Amendement 45
Proposition de directive
Article 4 – alinéa 1 – point 4

Texte proposé par la Commission	*Amendement*
(4) «stratégie nationale en matière de cybersécurité», le cadre cohérent d'un État membre fournissant des objectifs et des	(4) «stratégie nationale en matière de cybersécurité», le cadre cohérent d'un État membre fournissant des objectifs et des

priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information dans cet État membre;	priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information dans cet État membre***, ainsi que les politiques nécessaires pour les concrétiser***;

Amendement 46
Proposition de directive
Article 4 – alinéa 1 – point 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(5 bis) «incident transfrontalier», tout incident touchant des opérateurs sous le contrôle des autorités nationales compétentes d'au moins deux États membres différents;

Amendement 47
Proposition de directive
Article 4 – alinéa 1 – point 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(6 bis) «incident évité», un événement qui aurait potentiellement pu causer des dommages, mais dont la réalisation totale a pu être empêchée;

Amendement 48
Proposition de directive
Article 4 – alinéa 1 – point 15 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(15 bis) «services d'enregistrement des noms de domaines», les services fournis par les registres et les bureaux d'enregistrement des noms de domaines, les fournisseurs de services d'anonymisation et de services d'enregistrement fiduciaire, les courtiers ou les revendeurs de domaines, et tout autre service lié à l'enregistrement des noms de domaines;

Amendement 49
Proposition de directive
Article 5 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. Chaque État membre adopte une stratégie nationale en matière de cybersécurité qui définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir. La stratégie nationale en matière de cybersécurité comprend notamment les éléments suivants:	1. Chaque État membre adopte une stratégie nationale en matière de cybersécurité qui définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées, ***notamment les ressources humaines et financières appropriées,*** en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir. La stratégie nationale en matière de cybersécurité comprend notamment les éléments suivants:

Amendement 50
Proposition de directive
Article 5 – alinéa 1 – point b

Texte proposé par la Commission	*Amendement*
b) un cadre de gouvernance visant à atteindre ces objectifs et priorités, y compris les politiques visées au paragraphe 2 ainsi que les rôles et responsabilités des organismes et entités publics ainsi que des autres acteurs concernés;	b) un cadre de gouvernance visant à atteindre ces objectifs et priorités, y compris les politiques visées au paragraphe 2 ainsi que les rôles et responsabilités des organismes et entités publics ainsi que des autres acteurs concernés***, notamment ceux chargés du cyberrenseignement et de la cyberdéfense***;

Amendement 51
Proposition de directive
Article 5 – paragraphe 1 – point c

Texte proposé par la Commission	*Amendement*
c) une évaluation visant à déterminer les actifs pertinents et les risques de cybersécurité dans cet État membre;	c) une évaluation visant à déterminer les actifs pertinents et les risques de cybersécurité dans cet État membre***, y compris les éventuelles pénuries qui pourraient avoir une incidence négative***

sur le marché unique;

Amendement 52
Proposition de directive
Article 5 – paragraphe 1 – point e

Texte proposé par la Commission	*Amendement*
e) une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité;	e) une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité***, y compris un guichet unique pour les PME***;

Amendement 53
Proposition de directive
Article 5 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
b) des lignes directrices concernant l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics;	b) des lignes directrices concernant l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics***, y compris l'utilisation de produits de cybersécurité open source***;

Amendement 54
Proposition de directive
Article 5 – paragraphe 2 – point c

Texte proposé par la Commission	*Amendement*
c) une politique visant à promouvoir et à faciliter la divulgation coordonnée des vulnérabilités au sens de l'article 6;	c) une politique visant à promouvoir et à faciliter la divulgation coordonnée des vulnérabilités au sens de l'article 6***, notamment par la définition de lignes directrices et de bonnes pratiques fondées sur des normes établies et reconnues à l'échelle internationale en matière de traitement et de divulgation des vulnérabilités***;

Amendement 55
Proposition de directive
Article 5 – paragraphe 2 – point e

Texte proposé par la Commission	*Amendement*
e) une politique de promotion ***et de développement*** des compétences en matière de cybersécurité***, de sensibilisation*** et ***d'initiatives*** de recherche et développement;	e) une politique de promotion ***de la cybersécurité pour les consommateurs, qui les sensibilise aux cybermenaces, augmente la cyberculture, renforce la confiance*** des ***utilisateurs, développe les*** compétences ***et l'éducation*** en matière de cybersécurité ***technologiquement neutres,*** et ***favorise les initiatives*** de recherche et développement ***ainsi que la cybersécurité des produits connectés***;

Amendement 56
Proposition de directive
Article 5 – paragraphe 2 – point e bis (nouveau)

Texte proposé par la Commission	*Amendement*
	e bis) des mesures de promotion de l'utilisation de la cryptographie et du cryptage, en particulier par les PME;

Amendement 57
Proposition de directive
Article 5 – paragraphe 2 – point h

Texte proposé par la Commission	*Amendement*
h) une politique répondant aux besoins spécifiques des PME, ***en particulier*** de celles qui sont exclues du champ d'application de la présente directive, en matière d'orientation et de soutien visant à améliorer leur résilience aux menaces de cybersécurité.	h) une politique ***de promotion de la cybersécurité*** répondant aux besoins spécifiques des PME ***lorsqu'elles s'acquittent des obligations fixées par la présente directive***, ***ainsi qu'aux besoins spécifiques*** de celles qui sont exclues du champ d'application de la présente directive, en matière d'orientation et de soutien visant à améliorer leur résilience aux menaces de cybersécurité***, y compris, par exemple, le financement et l'éducation dans le but de favoriser***

l'adoption de mesures en matière de cybersécurité.

Amendement 58
Proposition de directive
Article 5 – paragraphe 2 – point h bis (nouveau)

Texte proposé par la Commission	*Amendement*
	h bis) cette politique comprend la mise en place d'un point de contact national unique pour les PME et d'un cadre favorisant l'utilisation la plus efficace des pôles d'innovation numérique et des fonds disponibles en vue de l'atteinte des objectifs politiques.

Amendement 59
Proposition de directive
Article 5 – paragraphe 2 – point h ter (nouveau)

Texte proposé par la Commission	*Amendement*
	h ter) une politique promouvant l'utilisation cohérente et synergique des fonds disponibles;

Amendement 60
Proposition de directive
Article 5 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les États membres évaluent leurs stratégies nationales de cybersécurité au moins tous les quatre ans sur la base d'indicateurs clés de performance et, le cas échéant, les modifient. L'Agence de l'Union européenne pour la cybersécurité (ENISA) aide les États membres, sur demande, à élaborer une stratégie nationale et des indicateurs clés de performance aux fins de l'évaluation de la stratégie.	4. Les États membres évaluent leurs stratégies nationales de cybersécurité au moins tous les quatre ans sur la base d'indicateurs clés de performance et, le cas échéant, les modifient. L'Agence de l'Union européenne pour la cybersécurité (ENISA) aide les États membres, sur demande, à élaborer une stratégie nationale et des indicateurs clés de performance aux fins de l'évaluation de la stratégie. ***L'ENISA adresse également des recommandations aux États membres sur l'élaboration d'indicateurs clés de***

	performance en vue de l'évaluation de la stratégie nationale, qui soient comparables au niveau de l'Union.

Amendement 61
Proposition de directive
Article 6 – titre

Texte proposé par la Commission	*Amendement*
Divulgation coordonnée des vulnérabilités et ***registre européen*** des vulnérabilités	Divulgation coordonnée des vulnérabilités et ***base de données européenne*** des vulnérabilités

Amendement 62
Proposition de directive
Article 6 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. L'ENISA élabore et tient à jour ***un registre européen*** des vulnérabilités. À cette fin, l'ENISA établit et maintient les systèmes d'information, les politiques et les procédures appropriés en vue notamment de permettre aux entités importantes et essentielles et à leurs fournisseurs de réseaux et de systèmes d'information de divulguer et d'enregistrer les vulnérabilités présentes dans les produits TIC ou les services TIC, ainsi que de donner accès à toutes les parties intéressées aux informations sur les vulnérabilités contenues dans le registre. ***Le registre*** comprend notamment des informations décrivant la vulnérabilité, le produit TIC ou les services TIC affectés ainsi que la gravité de la vulnérabilité en termes de circonstances dans lesquelles elle peut être exploitée, la disponibilité des correctifs correspondants et, en l'absence de correctifs disponibles, des orientations adressées aux utilisateurs de produits et services vulnérables sur la manière dont les risques résultant des vulnérabilités divulguées peuvent être atténués.	2. L'ENISA élabore et tient à jour ***une base de données européenne*** des vulnérabilités. À cette fin, l'ENISA établit et maintient les systèmes d'information, les politiques et les procédures appropriés***, ainsi que les politiques pertinentes en matière de divulgation,*** en vue notamment de permettre aux entités importantes et essentielles et à leurs fournisseurs de réseaux et de systèmes d'information de divulguer et d'enregistrer ***facilement*** les vulnérabilités présentes dans les produits TIC ou les services TIC, ainsi que de donner accès à toutes les parties intéressées aux informations ***pertinentes*** sur les vulnérabilités contenues dans le registre***, à condition que ces actions ne portent pas atteinte à la protection de la confidentialité et des secrets d'affaires***. ***La base de données des vulnérabilités*** comprend notamment des informations décrivant la vulnérabilité, le produit TIC ou les services TIC affectés ainsi que la gravité de la vulnérabilité en termes de circonstances dans lesquelles elle peut être exploitée, la disponibilité des correctifs

correspondants et, en l'absence de correctifs disponibles, des orientations adressées aux utilisateurs de produits et services vulnérables sur la manière dont les risques résultant des vulnérabilités divulguées peuvent être atténués. ***Afin d'éviter les doubles emplois, l'ENISA conclut un accord de partage d'informations et un accord de coopération structurée avec le registre mondial Common Vulnerabilities and Exposures (CVE) et, le cas échéant, avec d'autres bases de données développées et gérées à l'échelle mondiale par des partenaires de confiance.***

Amendement 63
Proposition de directive
Article 7 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Lorsqu'un État membre désigne plus d'une autorité compétente visée au paragraphe 1, il doit indiquer clairement laquelle de ces autorités compétentes fera office de point de contact principal lors d'un incident ou d'une crise de grande ampleur.

Amendement 64
Proposition de directive
Article 7 – paragraphe 3 – point f

Texte proposé par la Commission	*Amendement*
f) les procédures et ***arrangements*** nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs de l'État membre à la gestion coordonnée des incidents et des crises de cybersécurité majeurs au niveau de l'Union.	f) les procédures et ***la coordination*** nationaux entre les autorités et les organismes nationaux compétents***, y compris ceux chargés du cyber-renseignement et de la cyberdéfense,*** visant à garantir la participation et le soutien effectifs de l'État membre à la gestion coordonnée des incidents et des crises de cybersécurité majeurs au niveau de l'Union.

Amendement 65
Proposition de directive
Article 10 – paragraphe 2 – point d

Texte proposé par la Commission	*Amendement*
d) l'analyse dynamique des risques et incidents et la conscience situationnelle en matière de cybersécurité;	d) l'analyse dynamique des risques et incidents et la conscience situationnelle en matière de cybersécurité***, notamment par l'analyse des alertes précoces et des notifications visées à l'article 20***;

Amendement 66
Proposition de directive
Article 10 – paragraphe 2 – point e

Texte proposé par la Commission	*Amendement*
e) la réalisation, à la demande d'une entité, d'un scannage ***proactif*** du réseau et des systèmes d'information utilisés pour la fourniture de leurs services;	e) la réalisation, à la demande d'une entité, d'un scannage du réseau et des systèmes d'information utilisés pour la fourniture de leurs services ***afin de repérer, d'atténuer ou de prévenir des menaces spécifiques***;

Amendement 67
Proposition de directive
Article 10 – paragraphe 2 – point f

Texte proposé par la Commission	*Amendement*
f) la participation au réseau des CSIRT ainsi que la fourniture d'une assistance mutuelle aux autres membres du réseau à leur demande**.**	f) la participation ***active*** au réseau des CSIRT ainsi que la fourniture d'une assistance mutuelle aux autres membres du réseau à leur demande***;***

Amendement 68
Proposition de directive
Article 10 – paragraphe 2 – point f bis (nouveau)

Texte proposé par la Commission	*Amendement*
	f bis) la fourniture d'une assistance

	opérationnelle et d'orientations aux entités visées aux annexes I et II, et en particulier aux PME;

Amendement 69
Proposition de directive
Article 10 – paragraphe 2 – point f ter (nouveau)

Texte proposé par la Commission	*Amendement*
	f ter) la participation à des exercices conjoints de cybersécurité au niveau de l'Union.

Amendement 70
Proposition de directive
Article 11 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les États membres veillent à ce que leurs autorités compétentes ou leurs CSIRT reçoivent des notifications relatives aux incidents, aux cybermenaces importantes et quasi-accidents, soumises en application de la présente directive. Lorsqu'un État membre décide que ses CSIRT ne reçoivent pas ces notifications, ils se voient accorder, dans la mesure nécessaire à l'accomplissement de leurs tâches, un accès aux données relatives aux incidents notifiés par les entités essentielles ou importantes conformément à l'article 20.	2. Les États membres veillent à ce que leurs autorités compétentes ou leurs CSIRT reçoivent des notifications relatives aux incidents, aux cybermenaces importantes et quasi-accidents, soumises en application de la présente directive. Lorsqu'un État membre décide que ses CSIRT ne reçoivent pas ces notifications, ils se voient accorder, dans la mesure nécessaire à l'accomplissement ***efficace*** de leurs tâches, un accès ***adéquat*** aux données relatives aux incidents notifiés par les entités essentielles ou importantes conformément à l'article 20.

Amendement 71
Proposition de directive
Article 11 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Dans la mesure nécessaire pour s'acquitter efficacement des tâches et obligations prévues par la présente directive, les États membres assurent une	4. Dans la mesure nécessaire pour s'acquitter efficacement des tâches et obligations prévues par la présente directive, les États membres assurent une

coopération appropriée entre les autorités compétentes et les points de contact uniques et les services répressifs, les autorités chargées de la protection des données et les autorités responsables des infrastructures critiques en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] et les autorités financières nationales désignées conformément au règlement (UE) XXXX/XXXX du Parlement européen et du Conseil [39][le règlement sur la résilience opérationnelle numérique du secteur financier] dans cet État membre**.**	coopération appropriée entre les autorités compétentes et les points de contact uniques et les services répressifs, les autorités chargées de la protection des données et les autorités responsables des infrastructures critiques en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] et les autorités financières nationales désignées conformément au règlement (UE) XXXX/XXXX du Parlement européen et du Conseil[39] [le règlement sur la résilience opérationnelle numérique du secteur financier] dans cet État membre***, ainsi qu'avec les autorités chargées de la cyberdéfense et du cyberrenseignement.***
[39] [insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]	[39] [insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]

Amendement 72
Proposition de directive
Article 12 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le groupe de coopération exécute ses tâches en s'appuyant sur les programmes de travail bisannuels visés au paragraphe 6.	2. Le groupe de coopération ***se réunit régulièrement et*** exécute ses tâches en s'appuyant sur les programmes de travail bisannuels visés au paragraphe 6.

Amendement 73
Proposition de directive
Article 12 – paragraphe 3 – alinéa 2

Texte proposé par la Commission	*Amendement*
Si besoin est, le groupe de coopération peut inviter des représentants des acteurs concernés à participer à ses travaux.	Si besoin est, le groupe de coopération peut inviter des représentants des ***organes et agences compétents de l'Union ainsi que des*** acteurs concernés à participer à ses travaux.

Amendement 74
Proposition de directive
Article 12 – paragraphe 4 – point a

Texte proposé par la Commission	*Amendement*
a) la fourniture d'orientations aux autorités compétentes en rapport avec la transposition et la mise en œuvre de la présente directive;	a) la fourniture d'orientations aux autorités compétentes en rapport avec la transposition et la mise en œuvre de la présente directive ***et la promotion de sa mise en œuvre uniforme dans les États membres***;

Amendement 75
Proposition de directive
Article 12 – paragraphe 4 – point a bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) l'échange d'informations sur les priorités politiques et les principaux défis en matière de cybersécurité et la définition des principaux objectifs de la cybersécurité;

Amendement 76
Proposition de directive
Article 12 – paragraphe 4 – point a ter (nouveau)

Texte proposé par la Commission	*Amendement*
	a ter) l'étude des stratégies nationales des États membres et de leur état de préparation;

Amendement 77
Proposition de directive
Article 12 – paragraphe 4 – point c

Texte proposé par la Commission	*Amendement*
c) l'échange de conseils et la coopération avec la Commission sur les initiatives politiques émergentes en matière de cybersécurité;	c) l'échange de conseils et la coopération avec la Commission sur les initiatives politiques émergentes en matière de cybersécurité***, ainsi qu'avec le Service***

	européen pour l'action extérieure sur les aspects géopolitiques de la cybersécurité dans l'Union;

Amendement 78
Proposition de directive
Article 12 – paragraphe 4 – point f

Texte proposé par la Commission	*Amendement*
f) la discussion portant sur les rapports relatifs à l'évaluation par les pairs visés à l'article 16, paragraphe 7;	f) la discussion portant sur les rapports relatifs à l'évaluation par les pairs visés à l'article 16, paragraphe 7***, sur l'évaluation de son fonctionnement et sur les conclusions qui en découlent***;

Amendement 79
Proposition de directive
Article 12 – paragraphe 4 – point k bis (nouveau)

Texte proposé par la Commission	*Amendement*
	k bis) l'accompagnement de l'ENISA dans l'organisation de formations communes des autorités nationales compétentes au niveau de l'Union.

Amendement 80
Proposition de directive
Article 12 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Au plus tard ***le ...*** □ ***24*** mois après la date d'entrée en vigueur de la présente ***directive***□ et ensuite tous les deux ans, le groupe de coopération établit un programme de travail concernant les actions à entreprendre pour mettre en œuvre ses objectifs et ses tâches. Le calendrier du premier programme adopté au titre de la présente directive est aligné sur le calendrier du dernier programme adopté au titre de la directive (UE) 2016/1148.	6. Au plus tard [***12*** mois après la date d'entrée en vigueur de la présente directive] et ensuite tous les deux ans, le groupe de coopération établit un programme de travail concernant les actions à entreprendre pour mettre en œuvre ses objectifs et ses tâches. Le calendrier du premier programme adopté au titre de la présente directive est aligné sur le calendrier du dernier programme adopté au titre de la directive (UE) 2016/1148.

Amendement 81
Proposition de directive
Article 12 – paragraphe 8 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	8 bis. Le groupe de coopération publie régulièrement un rapport de synthèse de ses activités, sans préjudice de la confidentialité des informations échangées au cours de ses réunions.

Amendement 82
Proposition de directive
Article 13 – paragraphe 3 – point a

Texte proposé par la Commission	*Amendement*
a) l'échange d'informations sur les capacités des CSIRT;	a) l'échange d'informations sur les capacités ***et la préparation*** des CSIRT;

Amendement 83
Proposition de directive
Article 13 – paragraphe 3 – point b

Texte proposé par la Commission	*Amendement*
b) l'échange d'informations pertinentes sur les incidents, les quasi-accidents, les cybermenaces, les risques et les vulnérabilités;	b) l'échange d'informations pertinentes sur les incidents, les quasi-accidents, les cybermenaces, les risques et les vulnérabilités ***et le soutien aux capacités opérationnelles des États membres***;

Amendement 84
Proposition de directive
Article 13 – paragraphe 3 – point d bis (nouveau)

Texte proposé par la Commission	*Amendement*
	d bis) l'échange et la discussion portant sur les informations relatives aux incidents de nature transfrontalière;

Amendement 85
Proposition de directive
Article 13 – paragraphe 3 – point g – sous-point i bis (nouveau)

Texte proposé par la Commission	*Amendement*
	i bis) le partage d'informations;

Amendement 86
Proposition de directive
Article 13 – paragraphe 3 – point j

Texte proposé par la Commission	*Amendement*
j) ***à la demande d'un CSIRT donné***, l'étude des capacités et de l'état de préparation ***dudit CSIRT***;	j) l'étude des capacités et de l'état de préparation dudit CSIRT;

Amendement 87
Proposition de directive
Article 13 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Aux fins du réexamen visé à l'article 35 et d'ici le 24 mois après la date d'entrée en vigueur de la présente directive, puis tous les ***deux ans***, le réseau des CSIRT évalue les progrès réalisés dans le cadre de la coopération opérationnelle et produit un rapport. Le rapport tire notamment des conclusions sur les résultats des évaluations par les pairs visées à l'article 16, effectuées en rapport avec les CSIRT nationaux, y compris des conclusions et des recommandations, conformément au présent article. Ce rapport est aussi transmis au groupe de coopération.	4. Aux fins du réexamen visé à l'article 35 et d'ici le 24 mois après la date d'entrée en vigueur de la présente directive, puis ***chaque année***, le réseau des CSIRT évalue les progrès réalisés dans le cadre de la coopération opérationnelle et produit un rapport. Le rapport tire notamment des conclusions sur les résultats des évaluations par les pairs visées à l'article 16, effectuées en rapport avec les CSIRT nationaux, y compris des conclusions et des recommandations, conformément au présent article. Ce rapport est aussi transmis au groupe de coopération.

Amendement 88
Proposition de directive
Article 14 – paragraphe 3 – point a

Texte proposé par la Commission	*Amendement*
a) de renforcer le niveau de préparation à la gestion des crises et incidents majeurs;	a) de renforcer le niveau de préparation à la gestion des crises et incidents majeurs***, y compris des cybermenaces transfrontières***;

Amendement 89
Proposition de directive
Article 14 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. UE-CyCLONe rend régulièrement compte au groupe de coopération des cybermenaces ainsi que des incidents et tendances en matière de cybersécurité, en mettant notamment l'accent sur leur incidence sur les entités essentielles et importantes.	5. UE-CyCLONe rend régulièrement compte au groupe de coopération des cybermenaces ainsi que des incidents et tendances en matière de cybersécurité, en mettant notamment l'accent sur leur incidence sur les entités essentielles et importantes ***ainsi que sur leur résilience***.

Amendement 90
Proposition de directive
Article 14, paragraphe 6

Texte proposé par la Commission	*Amendement*
6. EU-CyCLONe coopère avec le réseau des CSIRT sur la base des modalités procédurales convenues.	6. EU-CyCLONe coopère ***étroitement*** avec le réseau des CSIRT sur la base des modalités procédurales convenues.

Amendement 91
Proposition de directive
Article 15 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. L'ENISA publie, en coopération avec la Commission, un rapport bisannuel sur l'état de la cybersécurité dans l'Union. Le rapport comporte notamment une évaluation des éléments suivants:	1. L'ENISA publie, en coopération avec la Commission, un rapport bisannuel sur l'état de la cybersécurité dans l'Union ***et le présente au Parlement européen***. Le rapport comporte notamment une évaluation des éléments suivants:

Amendement 92
Proposition de directive
Article 15 – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
a) le développement des capacités de cybersécurité dans l'ensemble de l'Union;	a) le développement des capacités de cybersécurité dans l'ensemble de l'Union***, y compris le niveau général des compétences en matière de cybersécurité, le degré global de résilience du marché intérieur face aux cybermenaces et le niveau de mise en œuvre de la directive dans l'ensemble des États membres***;

Amendement 93
Proposition de directive
Article 15 – paragraphe 1 – point c

Texte proposé par la Commission	*Amendement*
c) un indice de cybersécurité permettant une évaluation globale du niveau de maturité des capacités de cybersécurité**.**	c) un indice de cybersécurité permettant une évaluation globale du niveau de maturité des capacités de cybersécurité***, y compris une évaluation globale de la cybersécurité pour les consommateurs;***

Amendement 94
Proposition de directive
Article 15 – paragraphe 1 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) les aspects géopolitiques ayant une incidence directe ou indirecte sur la situation en matière de cybersécurité dans l'Union.

Amendement 95
Proposition de directive
Article 16 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. La Commission établit, après consultation du groupe de coopération et de l'ENISA, et au plus tard ***18*** mois après l'entrée en vigueur de la présente directive, la méthodologie et le contenu d'un système d'évaluation par les pairs pour apprécier l'efficacité des politiques en matière de cybersécurité des États membres. Les évaluations sont effectuées par des experts techniques en cybersécurité provenant ***d'États*** membres différents de celui qui fait l'objet de l'évaluation et portent au moins sur les points suivants:	1. La Commission établit, après consultation du groupe de coopération et de l'ENISA, et au plus tard ***12*** mois après l'entrée en vigueur de la présente directive, la méthodologie et le contenu d'un système d'évaluation par les pairs pour apprécier l'efficacité des politiques en matière de cybersécurité des États membres. Les évaluations sont effectuées par des experts techniques en cybersécurité provenant ***d'au moins deux États*** membres ***et de l'ENISA,*** différents de celui qui fait l'objet de l'évaluation et portent au moins sur les points suivants:

Amendement 96
Proposition de directive
Article 16 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La méthodologie comprend des critères objectifs, non discriminatoires, équitables et transparents sur la base desquels les États membres désignent les experts habilités à effectuer les évaluations par les pairs. L'ENISA et la Commission désignent des experts pour participer en tant qu'observateurs aux évaluations par les pairs. La Commission, soutenue par l'ENISA, établit, dans le cadre de la méthodologie visée au paragraphe 1, un système objectif, non discriminatoire, équitable et transparent aux fins de la sélection et de la répartition aléatoire des experts pour chaque évaluation par les pairs.	2. La méthodologie comprend des critères objectifs, non discriminatoires, ***technologiquement neutres,*** équitables et transparents sur la base desquels les États membres désignent les experts habilités à effectuer les évaluations par les pairs. L'ENISA et la Commission désignent des experts pour participer en tant qu'observateurs aux évaluations par les pairs. La Commission, soutenue par l'ENISA, établit, dans le cadre de la méthodologie visée au paragraphe 1, un système objectif, non discriminatoire, équitable et transparent aux fins de la sélection et de la répartition aléatoire des experts pour chaque évaluation par les pairs.

Amendement 97
Proposition de directive
Article 18 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les États membres veillent à ce que les entités essentielles et importantes prennent les ***mesures techniques et organisationnelles appropriées*** et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de la fourniture de leurs services. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances.	1. Les États membres veillent à ce que les entités essentielles et importantes prennent ***des*** mesures techniques et organisationnelles pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de la fourniture de leurs services. ***Ces mesures sont appropriées et proportionnées au niveau de criticité du secteur ou du type de service, ainsi qu'au niveau de dépendance de l'entité par rapport à d'autres secteurs ou types de services, et sont adoptées à la suite d'une évaluation fondée sur les risques.*** Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances. ***En particulier, des mesures sont prises pour prévenir et réduire autant que possible les conséquences des incidents de sécurité sur les destinataires de leurs services.***

Amendement 98
Proposition de directive
Article 18 – paragraphe 2 – point d

Texte proposé par la Commission	*Amendement*
d) ***la*** sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services tels que les fournisseurs de services de stockage et de traitement des données ou de services de sécurité gérés;	d) ***les mesures en vue de l'évaluation des risques liés à la*** sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services tels que les fournisseurs de services de stockage et de traitement des données ou de services de sécurité gérés;

Amendement 99
Proposition de directive
Article 18 – paragraphe 2 – point f

Texte proposé par la Commission	*Amendement*
f) des politiques et des procédures (tests et audits) pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;	f) des politiques et des procédures (tests et audits)***, ainsi que des exercices réguliers de cybersécurité*** pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;

Amendement 100
Proposition de directive
Article 18 – paragraphe 2 – point g

Texte proposé par la Commission	*Amendement*
g) l'utilisation de la cryptographie et du ***cryptage.***	g) l'utilisation de la cryptographie***, du cryptage*** et***, en particulier,*** du ***chiffrement de bout en bout;***

Amendement 101
Proposition de directive
Article 18 – paragraphe 2 – point g bis (nouveau)

Texte proposé par la Commission	*Amendement*
	g bis) des politiques visant à garantir une formation et une sensibilisation adéquates en matière de cybersécurité.

Amendement 102
Proposition de directive
Article 18 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les États membres veillent à ce que, lorsqu'elles envisagent de prendre les mesures appropriées visées au paragraphe 2, point d), les entités tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de	3. Les États membres veillent à ce que, lorsqu'elles envisagent de prendre les mesures appropriées visées au paragraphe 2, point d), les entités tiennent compte***, lorsqu'elles ont accès aux informations pertinentes,*** des vulnérabilités propres à chaque fournisseur et prestataire de services et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et

développement sécurisé.

prestataires de services, y compris de leurs procédures de développement sécurisé.

Amendement 103
Proposition de directive
Article 18 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. La Commission ***peut*** adopter des actes ***d'exécution*** afin d'établir les spécifications techniques et méthodologiques des éléments visés au paragraphe 2***. Lorsqu'elle prépare ces actes, la Commission procède conformément à la procédure d'examen visée à l'article 37, paragraphe 2,*** et suit, dans toute la mesure du possible, les normes internationales et européennes, ainsi que les spécifications techniques pertinentes.	5. La Commission ***est habilitée à*** adopter des actes ***délégués*** afin d'établir les spécifications techniques et méthodologiques des éléments visés au paragraphe 2 et suit, dans toute la mesure du possible, les normes internationales et européennes, ainsi que les spécifications techniques pertinentes. ***Lors de l'élaboration des actes délégués, la Commission consulte également toutes les parties prenantes concernées.***

Amendement 104
Proposition de directive
Article 18 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. La Commission ***est habilitée à adopter des actes délégués conformément à l'article 36 pour compléter les éléments prévus au paragraphe 2 afin*** de ***tenir compte des nouvelles cybermenaces***, ***des évolutions technologiques ou des spécificités sectorielles***.	6. La Commission***, en coopération avec le groupe de coopération et l'ENISA, fournit des orientations et des bonnes pratiques sur le respect, par les entités,*** de ***façon proportionnée, conformément aux exigences énoncées au paragraphe 2***, ***et en particulier à l'exigence énoncée au point d) dudit paragraphe***.

Amendement 105
Proposition de directive
Article 19 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le groupe de coopération, en coopération avec la Commission et	1. ***En vue d'accroître le niveau global de cybersécurité, le*** groupe de coopération,

l'ENISA, peut procéder à des évaluations coordonnées des risques de sécurité inhérents à des chaînes d'approvisionnement de services, de systèmes ou de produits TIC critiques spécifiques, en tenant compte des facteurs de risque techniques et, le cas échéant, non techniques.	en coopération avec la Commission et l'ENISA, peut procéder à des évaluations coordonnées des risques de sécurité inhérents à des chaînes d'approvisionnement de services, de systèmes ou de produits TIC critiques spécifiques, en tenant compte des facteurs de risque techniques et, le cas échéant, non techniques***, tels que les risques géopolitiques***.

Amendement 106
Proposition de directive
Article 20 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les États membres veillent à ce que les entités essentielles et importantes notifient dans les meilleurs délais aux autorités compétentes ou au CSIRT conformément aux paragraphes 3 et 4 tout incident ayant une incidence significative sur la fourniture de leurs services. Le cas échéant, ces entités notifient dans les meilleurs délais aux destinataires de leurs services les incidents susceptibles de nuire à la fourniture de ces services. Les États membres veillent à ce que ces entités signalent, entre autres, toute information permettant aux autorités compétentes ou au CSIRT de déterminer si l'incident a une incidence au niveau transfrontalier.	1. Les États membres veillent à ce que les entités essentielles et importantes notifient dans les meilleurs délais aux autorités compétentes ou au CSIRT conformément aux paragraphes 3 et 4 tout incident ayant une incidence significative sur la fourniture de leurs services ***ou de tout incident évité***. Le cas échéant, ces entités notifient dans les meilleurs délais aux destinataires de leurs services les incidents susceptibles de nuire à la fourniture de ces services. Les États membres veillent à ce que ces entités signalent, entre autres, toute information permettant aux autorités compétentes ou au CSIRT de déterminer si l'incident ***ou l'incident évité*** a une incidence au niveau transfrontalier.

Amendement 107
Proposition de directive
Article 20 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Afin de simplifier les obligations de signalement, les États membres mettent en place un point d'entrée unique pour toutes les notifications requises en vertu

	de la présente directive et d'autres actes législatifs de l'Union, comme le règlement (UE) 2016/679 et la directive 2002/58/CE.

Amendement 108
Proposition de directive
Article 20 – paragraphe 1 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	1 ter. L'ENISA, en collaboration avec le groupe de coopération, met au point des formulaires de notification communs au moyen de lignes directrices qui permettraient de simplifier et de rationaliser les informations de signalement exigées par le droit de l'Union et de réduire la charge pesant sur les entreprises en matière de conformité.

Amendement 109
Proposition de directive
Article 20 – paragraphe 2 – alinéa 1

Texte proposé par la Commission	*Amendement*
2. ***Les États membres veillent à ce que les entités essentielles et importantes notifient dans les meilleurs délais aux autorités compétentes ou au CSIRT toute cybermenace importante que ces entités décèlent et qui aurait pu entraîner un incident significatif.***	***supprimé***

Amendement 110
Proposition de directive
Article 20 – paragraphe 2 – alinéa 2

Texte proposé par la Commission	*Amendement*
Le cas échéant, ces entités notifient dans les meilleurs délais aux destinataires de leurs services qui sont potentiellement affectés par une cybermenace importante	***supprimé***

toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, les entités informent également leurs destinataires de la menace elle-même. La notification n'accroît pas la responsabilité de l'entité qui en est à l'origine.

Amendement 111
Proposition de directive
Article 20 – paragraphe 3 – point a

Texte proposé par la Commission	*Amendement*
a) l'incident a causé ou est susceptible de causer une perturbation opérationnelle importante ***ou des pertes*** financières substantielles pour l'entité concernée;	a) l'incident a causé une perturbation opérationnelle importante ou des pertes financières substantielles pour l'entité concernée;

Amendement 112
Proposition de directive
Article 20 – paragraphe 3 – point b

Texte proposé par la Commission	*Amendement*
b) l'incident a affecté ou ***est susceptible d'affecter*** d'autres personnes physiques ou morales en causant des pertes matérielles ou non matérielles considérables.	b) l'incident a affecté d'autres personnes physiques ou morales en causant des pertes matérielles ou non matérielles considérables.

Amendement 113
Proposition de directive
Article 20 – paragraphe 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	3 bis. La Commission est habilitée à adopter des actes délégués, conformément à l'article 36, pour compléter la présenta directive en précisant le type d'informations soumises en vertu du paragraphe 1 du présent article et en précisant, en outre, les cas dans lesquels un incident est considéré comme

significatif au sens du paragraphe 3 du présent article.

Amendement 114
Proposition de directive
Article 20 – paragraphe 4 – point -a (nouveau)

Texte proposé par la Commission	*Amendement*
	-a) une alerte précoce dans les 24 heures après avoir eu connaissance d'un incident, sans obligation pour l'entité concernée de divulguer des informations supplémentaires concernant l'incident;

Amendement 115
Proposition de directive
Article 20 – paragraphe 4 – point a

Texte proposé par la Commission	*Amendement*
a) sans retard injustifié et en tout cas dans les ***24*** heures après avoir eu connaissance de l'incident, une première notification qui, le cas échéant, indique si l'incident est vraisemblablement causé par une action illicite ou malveillante;	a) sans retard injustifié et en tout cas dans les ***72*** heures après avoir eu connaissance de l'incident, une première notification qui, le cas échéant, indique si l'incident est vraisemblablement causé par une action illicite ou malveillante;

Amendement 116
Proposition de directive
Article 20 – paragraphe 4 – point c – partie introductive

Texte proposé par la Commission	*Amendement*
c) un rapport ***final*** au plus tard ***un*** mois après la présentation du rapport visé au point a), comprenant au moins les éléments suivants:	c) un rapport ***complet*** au plus tard ***trois*** mois après la présentation du rapport visé au point a), comprenant au moins les éléments suivants:

Amendement 117
Proposition de directive
Article 20 – paragraphe 4 – point c – sous-point i

Texte proposé par la Commission	*Amendement*
i) une description détaillée de l'incident, de sa gravité et de son incidence;	i) une description ***plus*** détaillée de l'incident, de sa gravité et de son incidence;

Amendement 118
Proposition de directive
Article 20 – paragraphe 4 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) en cas d'incident toujours en cours au moment de la présentation du rapport complet visé au point c), un rapport final est fourni un mois après que l'incident a été atténué;

Amendement 119
Proposition de directive
Article 20 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou pour faire face à un incident en cours, ou lorsque la divulgation de l'incident est par ailleurs dans l'intérêt public, l'autorité compétente ou le CSIRT et, le cas échéant, les autorités ou les CSIRT des autres États membres concernés ***peuvent***, après avoir consulté l'entité concernée, ***informer*** le public de l'incident ou exiger de l'entité qu'elle le fasse.	7. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou pour faire face à un incident en cours, ou lorsque la divulgation de l'incident est par ailleurs dans l'intérêt public, l'autorité compétente ou le CSIRT et, le cas échéant, les autorités ou les CSIRT des autres États membres concernés , après avoir consulté l'entité concernée, ***informent*** le public de l'incident ou exiger de l'entité qu'elle le fasse.

Amendement 120
Proposition de directive
Article 20 – paragraphe 8

Texte proposé par la Commission	*Amendement*
8. À la demande de l'autorité compétente ou du CSIRT, le point de	8. À la demande de l'autorité compétente ou du CSIRT, le point de

contact unique transmet les notifications reçues en vertu ***des paragraphes*** 1 ***et 2*** aux points de contact uniques des autres États membres touchés.	contact unique transmet les notifications reçues en vertu ***du paragraphe*** 1 aux points de contact uniques des autres États membres touchés.

Amendement 121
Proposition de directive
Article 20 – paragraphe 9

Texte proposé par la Commission	*Amendement*
9. Le point de contact unique soumet mensuellement à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents, les cybermenaces majeures et les quasi-accidents notifiés conformément ***aux paragraphes*** 1 ***et 2*** et conformément à l'article 27. Afin de contribuer à la fourniture d'informations comparables, l'ENISA peut émettre des orientations techniques sur les paramètres des informations incluses dans le rapport de synthèse.	9. Le point de contact unique soumet mensuellement à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents, les cybermenaces majeures et les quasi-accidents notifiés conformément ***au paragraphe*** 1 et conformément à l'article 27. Afin de contribuer à la fourniture d'informations comparables, l'ENISA peut émettre des orientations techniques sur les paramètres des informations incluses dans le rapport de synthèse.

Amendement 122
Proposition de directive
Article 20 – paragraphe 10

Texte proposé par la Commission	*Amendement*
10. Les autorités compétentes fournissent aux autorités compétentes désignées en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] des informations sur les incidents et les cybermenaces notifiés conformément ***aux paragraphes*** 1 ***et 2*** par les entités essentielles identifiées comme des entités critiques, ou comme des entités équivalentes aux entités critiques, en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques].	10. Les autorités compétentes fournissent aux autorités compétentes désignées en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] des informations sur les incidents et les cybermenaces notifiés conformément ***au paragraphe*** 1 par les entités essentielles identifiées comme des entités critiques, ou comme des entités équivalentes aux entités critiques, en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques].

Amendement 123
Proposition de directive
Article 20 – paragraphe 11

Texte proposé par la Commission	*Amendement*
11. La Commission peut adopter des actes d'exécution précisant plus en détail le type d'informations, le format et la procédure d'une notification présentée en vertu ***des paragraphes 1 et 2***. La Commission peut également adopter des actes d'exécution pour préciser plus en détail les cas dans lesquels un incident est considéré comme significatif au sens du paragraphe 3. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 37, paragraphe 2.	11. La Commission peut adopter des actes d'exécution précisant plus en détail le type d'informations, le format et la procédure d'une notification présentée en vertu ***du paragraphe 1***. La Commission peut également adopter des actes d'exécution pour préciser plus en détail les cas dans lesquels un incident est considéré comme significatif au sens du paragraphe 3. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 37, paragraphe 2.

Amendement 124
Proposition de directive
Article 21 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Afin de démontrer la conformité à certaines exigences visées à l'article 18, les États membres ***peuvent exiger que des*** entités essentielles et importantes ***certifient*** certains produits TIC, services TIC et processus TIC dans le cadre de schémas européens ***de certification*** en matière de cybersécurité ***spécifiques*** adoptés conformément à l'article 49 du règlement (UE) 2019/881***. Les produits, services et processus soumis à*** la ***certification peuvent être développés par une entité essentielle ou importante ou achetés à des tiers***.	1. Afin de démontrer la conformité à certaines exigences visées à l'article 18 ***et pour accroître le niveau de cybersécurité***, les États membres***, après consultation du groupe de coopération et de l'ENISA, encouragent les*** entités essentielles et importantes ***à certifier*** certains produits TIC, services TIC et processus TIC***, soit mis au point par l'entité essentielle ou importante, soit acquis auprès de tiers,*** dans le cadre de schémas européens en matière de cybersécurité adoptés conformément à l'article 49 du règlement (UE) 2019/881 ***ou de schémas de certification similaires reconnus au niveau international. Dans*** la ***mesure du possible, les États membres encouragent l'utilisation de schémas de certification adoptés de façon harmonisée***.

Amendement 125
Proposition de directive
Article 21 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La Commission ***est habilitée à adopter*** des ***actes délégués précisant*** quelles catégories d'entités essentielles sont ***tenues d'obtenir*** un certificat et dans le cadre de quels régimes européens de certification de cybersécurité spécifiques en application du ***paragraphe*** 1. ***Les actes délégués sont adoptés conformément à l'article 36.***	2. La Commission ***évalue régulièrement l'efficacité et l'utilisation*** des ***schémas européens de certification en matière de cybersécurité adoptés conformément à l'article 49 du règlement (UE) 2019/881 et détermine*** quelles catégories d'entités essentielles sont ***encouragées à obtenir*** un certificat et dans le cadre de quels régimes européens de certification de cybersécurité spécifiques en application du ***paragraphe*** 1.

Amendement 126
Proposition de directive
Article 22 – paragraphe -1 (nouveau)

Texte proposé par la Commission	*Amendement*
	-1 bis. La Commission, en collaboration avec l'ENISA, soutient et promeut l'élaboration et la mise en œuvre de normes établies par les organismes de normalisation de l'Union et internationaux compétents aux fins de la mise en œuvre convergente de l'article 18, paragraphes 1 et 2. La Commission soutient la mise à jour des normes à la lumière de l'évolution technologique.

Amendement 127
Proposition de directive
Article 22 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Afin de favoriser la convergence de la mise en œuvre de l'article 18, paragraphes 1 et 2, les États membres encouragent, sans imposer l'utilisation	1. Afin de favoriser la convergence de la mise en œuvre de l'article 18, paragraphes 1 et 2, les États membres encouragent, sans imposer l'utilisation

d'un type particulier de technologies ni créer de discrimination en faveur d'un tel type particulier de technologies, le recours à des normes et des spécifications européennes ou internationalement reconnues pour la sécurité des réseaux et des systèmes d'information.	d'un type particulier de technologies ni créer de discrimination en faveur d'un tel type particulier de technologies, ***et selon les orientations de l'ENISA et du groupe de coopération,*** le recours à des normes et des spécifications européennes ou internationalement reconnues pour la sécurité des réseaux et des systèmes d'information.

Amendement 128
Proposition de directive
Article 23 – titre

Texte proposé par la Commission	*Amendement*
Bases de données des noms de domaines et des données d'enregistrement	***Infrastructure de*** bases de données des noms de domaines et des données d'enregistrement

Amendement 129
Proposition de directive
Article 23 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Afin de contribuer à la sécurité, à la stabilité et à la résilience du DNS, les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau collectent et maintiennent les données d'enregistrement de noms de domaines exactes et complètes au sein d'une base de données dédiée avec la diligence requise, sous réserve du droit de l'Union en matière de protection des données à caractère personnel.	1. Afin de contribuer à la sécurité, à la stabilité et à la résilience du DNS, les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau***,*** collectent***, vérifient*** et maintiennent les données d'enregistrement de noms de domaines exactes et complètes ***nécessaires à la fourniture de leurs services*** au sein d'une base de données dédiée avec la diligence requise, sous réserve du droit de l'Union en matière de protection des données à caractère personnel.

Amendement 130
Proposition de directive
Article 23 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les États membres veillent à ce que ***les bases*** de données ***relatives*** à l'enregistrement des noms de domaines ***visées*** au paragraphe 1 ***contiennent*** des informations pertinentes pour identifier et contacter les titulaires des noms de domaines et les points de contact qui gèrent les noms de domaines dans les registres des noms de domaines de premier niveau.	2. Les États membres veillent à ce que ***l'infrastructure de base*** de données ***relative*** à l'enregistrement des noms de domaines ***visée*** au paragraphe 1 ***contienne*** des informations pertinentes***, qui comprennent au moins le nom des titulaires de noms de domaines, leur adresse physique et électronique, ainsi que leur numéro de téléphone, nécessaires*** pour identifier et contacter les titulaires des noms de domaines et les points de contact qui gèrent les noms de domaines dans les registres des noms de domaines de premier niveau***, notamment au moins le nom des titulaires de noms de domaines, leur adresse physique, leur adresse électronique, ainsi que leur numéro de téléphone***.

Amendement 131
Proposition de directive
Article 23 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau aient mis en place des politiques et des procédures visant à garantir que ***les*** bases de données ***contiennent*** des informations exactes et complètes. Les États membres veillent à ce que ces politiques et procédures soient mises à la disposition du public.	3. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau aient mis en place des politiques et des procédures visant à garantir que ***l'infrastructure de*** bases de données ***contienne*** des informations exactes***, vérifiées*** et complètes***, et que les données inexactes ou incomplètes soient corrigées ou supprimées par le titulaire du nom de domaine sans délai***. Les États membres veillent à ce que ces politiques et procédures soient mises à la disposition du

public.

Amendement 132
Proposition de directive
Article 23 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines ***pour le registre de noms de domaines de premier niveau publient***, dans les meilleurs délais après l'enregistrement d'un nom de domaine, des données d'enregistrement de domaine ***qui ne sont pas des données personnelles***.	4. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines ***mettent à la disposition du public***, dans les meilleurs délais ***et en tout état de cause dans les 24 heures*** après l'enregistrement d'un nom de domaine, ***l'ensemble*** des données d'enregistrement de domaine ***de personnes morales titulaires de noms de domaines***.

Amendement 133
Proposition de directive
Article 23 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines ***pour le registre de noms de domaines*** de ***premier niveau donnent*** accès aux données spécifiques d'enregistrement de noms de domaines sur demande ***légitime et*** dûment justifiée des demandeurs d'accès légitimes, dans le respect du droit de l'Union en matière de protection des données. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines ***pour le registre de noms de domaines de premier niveau répondent*** dans ***les meilleurs délais*** à toutes les demandes d'accès. Les États membres veillent à ce que les politiques et	5. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines ***soient tenus*** de ***donner*** accès aux données spécifiques d'enregistrement de noms de domaines sur demande dûment justifiée des demandeurs d'accès légitimes, dans le respect du droit de l'Union en matière de protection des données. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines ***répondent dans les meilleurs délais et dans tous les cas*** dans ***un délai de 72 heures*** à toutes les demandes d'accès ***légitimes et dûment justifiées***. Les États membres veillent à ce que les politiques et procédures de divulgation de ces données

procédures de divulgation de ces données soient rendues publiques.	soient rendues publiques.

Amendement 134
Proposition de directive
Article 24 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Aux fins de la présente directive, les entités visées au paragraphe 1 sont réputées avoir leur établissement principal dans l'Union dans l'État membre où sont prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité. Si ces décisions ne sont pas prises dans un quelconque établissement de l'Union, l'établissement principal doit être considéré comme se trouvant dans les États membres où les entités possèdent un établissement comptant le plus grand nombre de salariés dans l'Union.	2. Aux fins de la présente directive, les entités visées au paragraphe 1 sont réputées avoir leur établissement principal dans l'Union dans l'État membre où sont prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité. Si ces décisions ne sont pas prises dans un quelconque établissement de l'Union, l'établissement principal doit être considéré comme se trouvant dans les États membres où les entités possèdent un établissement comptant le plus grand nombre de salariés dans l'Union. ***Ceci est fait de manière à garantir qu'aucune charge disproportionnée ne pèse sur les autorités de régulation nationales.***

Amendement 135
Proposition de directive
Article 25 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. L'ENISA crée et tient un registre des entités essentielles et importantes visées à l'article 24, paragraphe 1. Les entités doivent soumettre les informations suivantes à l'ENISA au plus tard [12 mois après l'entrée en vigueur de la directive]:	1. L'ENISA crée et tient un registre des entités essentielles et importantes visées à l'article 24, paragraphe 1. ***À cette fin,*** les entités doivent soumettre les informations suivantes à l'ENISA au plus tard [12 mois après l'entrée en vigueur de la directive]:

Amendement 136
Proposition de directive
Article 26 – paragraphe 1 – point b

Texte proposé par la Commission	*Amendement*
b) renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur «capacité de se propager», en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement.	b) renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur «capacité de se propager», en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection ***et de prévention*** des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement.

Amendement 137
Proposition de directive
Article 26 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les États membres établissent des ***règles*** précisant la procédure, les éléments opérationnels (y compris l'utilisation de plateformes TIC dédiées), le contenu et les conditions des accords de partage d'informations visés au paragraphe 2. Ces ***règles fixent*** également les détails de la participation des autorités publiques à ces accords, ainsi que les éléments opérationnels, y compris l'utilisation de plateformes informatiques dédiées. Les États membres offrent un soutien à l'application de ces accords conformément à leurs politiques visées à l'article 5, paragraphe 2, point g).	3. Les États membres établissent des ***lignes directrices*** précisant la procédure, les éléments opérationnels (y compris l'utilisation de plateformes TIC dédiées), le contenu et les conditions des accords de partage d'informations visés au paragraphe 2. Ces ***lignes directrices incluent*** également les détails de la participation***, le cas échéant,*** des autorités publiques ***et des experts indépendants*** à ces accords, ainsi que les éléments opérationnels, y compris l'utilisation de plateformes informatiques dédiées. Les États membres offrent un soutien à l'application de ces accords conformément à leurs politiques visées à l'article 5, paragraphe 2, point g).

Amendement 138
Proposition de directive
Article 26 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Conformément au droit de l'Union,	5. Conformément au droit de l'Union,

l'ENISA soutient la mise en place des mécanismes de partage d'informations en matière de cybersécurité visés au paragraphe 2 par la fourniture de bonnes pratiques et d'orientations.	l'ENISA soutient la mise en place des mécanismes de partage d'informations en matière de cybersécurité visés au paragraphe 2 par la fourniture de bonnes pratiques et d'orientations***, ainsi qu'en facilitant le partage d'informations au niveau de l'Union, tout en sauvegardant les informations commerciales sensibles. À la demande des entités essentielles et importantes, le groupe de coopération est invité à fournir des bonnes pratiques et des orientations.***

Amendement 139
Proposition de directive
Article 27 – alinéa -1 (nouveau)

Texte proposé par la Commission	*Amendement*
	-1 bis. Les États membres veillent à ce que les entités essentielles et importantes puissent notifier, sur une base volontaire, les cybermenaces que ces entités décèlent et qui aurait pu entraîner un incident significatif. Les États membres veillent à ce qu'aux fins de ces notifications, les entités agissent conformément à la procédure établie à l'article 20. Les signalements volontaires n'ont pas pour effet d'imposer à l'entité qui est à l'origine du signalement des obligations supplémentaires.

Amendement 140
Proposition de directive
Article 27 – alinéa 1

Texte proposé par la Commission	*Amendement*
Sans préjudice de l'article 3, les États membres veillent à ce que les entités qui ne relèvent pas du champ d'application de la présente directive puissent, à titre volontaire, transmettre des notifications relatives aux incidents importants, aux cybermenaces ou aux incidents évités. Lorsqu'ils traitent des notifications, les	***1.*** ***Sans*** préjudice de l'article 3, les États membres veillent à ce que les entités qui ne relèvent pas du champ d'application de la présente directive puissent, à titre volontaire, transmettre des notifications relatives aux incidents importants, aux cybermenaces ou aux incidents évités. Lorsqu'ils traitent des notifications, les

États membres agissent conformément à la procédure énoncée à l'article 20. Les États membres ***peuvent traiter*** les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Un signalement volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine du signalement des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis ladite notification.

États membres agissent conformément à la procédure énoncée à l'article 20. Les États membres ***traitent*** les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Un signalement volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine du signalement des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis ladite notification***, mais l'État membre peut lui faire bénéficier de l'assistance des CSIRT***.

Amendement 141
Proposition de directive
Article 28 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les États membres veillent à ce que les autorités compétentes procèdent à une surveillance efficace et prennent les mesures nécessaires pour assurer le respect de la présente directive, et notamment des obligations énoncées aux articles 18 et 20.	1. Les États membres veillent à ce que les autorités compétentes procèdent à une surveillance efficace et prennent les mesures nécessaires pour assurer le respect de la présente directive, et notamment des obligations énoncées aux articles 18 et 20***, et bénéficient de moyens suffisants pour jouer leur rôle***.

Amendement 142
Proposition de directive
Article 28 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Pour traiter des incidents donnant lieu à des violations de données à caractère personnel, les autorités compétentes coopèrent étroitement avec les autorités chargées de la protection des données.	2. Pour traiter des incidents donnant lieu à des violations de données à caractère personnel, les autorités compétentes coopèrent étroitement avec les autorités chargées de la protection des données***, notamment avec celles d'autres États membres, le cas échéant***.

Amendement 143
Proposition de directive
Article 29 – paragraphe 2 – point c

Texte proposé par la Commission	*Amendement*
c) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques;	c) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques***, réalisés par un organisme indépendant qualifié ou une autorité compétente***;

Amendement 144
Proposition de directive
Article 29 – paragraphe 2 – point f

Texte proposé par la Commission	*Amendement*
f) des demandes d'accès à des données, à des documents ou à ***toutes*** informations nécessaires à l'accomplissement de leurs missions de surveillance;	f) des demandes d'accès à des données, documents ou informations ***pertinents*** nécessaires à l'accomplissement de leurs missions de surveillance;

Amendement 145
Proposition de directive
Article 29 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points e) à g), les autorités compétentes mentionnent la finalité de la demande ***et*** précisent quelles sont les informations exigées.	3. Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points e) à g), les autorités compétentes mentionnent la finalité de la demande**,** précisent quelles sont les informations exigées ***et limitent leurs demandes au périmètre de l'incident ou du sujet de préoccupation***.

Amendement 146
Proposition de directive
Article 29 – paragraphe 5 – alinéa 1 – point a

Texte proposé par la Commission	*Amendement*
a) de suspendre ou de demander à un organisme de certification ou d'autorisation de suspendre une certification ou une autorisation concernant ***tout ou partie des*** services ou activités fournis par une entité essentielle;	a) de suspendre ou de demander à un organisme de certification ou d'autorisation de suspendre une certification ou une autorisation concernant des services ou activités ***concernés*** fournis par une entité essentielle;

Amendement 147
Proposition de directive
Article 29 – paragraphe 5 – alinéa 1 – point b

Texte proposé par la Commission	*Amendement*
b) d'imposer ou de demander aux juridictions ou organes compétents d'imposer, conformément à la législation nationale, une interdiction temporaire interdisant à toute personne exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans cette entité essentielle, ainsi qu'à toute autre personne physique tenue pour responsable de la violation, d'exercer des responsabilités dirigeantes dans cette entité.	***supprimé***

Amendement 148
Proposition de directive
Article 30, paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque, selon les éléments de preuve ou les indications communiquées, une entité importante ne respecte pas les obligations énoncées dans la présente directive, et notamment aux articles 18 et 20, les États membres veillent à ce que les autorités compétentes prennent des mesures, le cas échéant, dans le cadre de mesures de contrôle ex post.	1. Lorsque, selon les éléments de preuve ou les indications communiquées, une entité importante ne respecte pas les obligations énoncées dans la présente directive, et notamment aux articles 18 et 20, les États membres veillent à ce que les autorités compétentes prennent des mesures, le cas échéant ***et en compte tenu d'une approche fondée sur le risque***, dans le cadre de mesures de contrôle ex post.

Amendement 149
Proposition de directive
Article 30 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
b) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques;	b) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques***, réalisés par un organisme indépendant qualifié ou une autorité compétente***;

Amendement 150
Proposition de directive
Article 30 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points d) ou e), les autorités compétentes mentionnent la finalité de la demande ***et*** précisent quelles sont les informations exigées.	3. Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points d) ou e), les autorités compétentes mentionnent la finalité de la demande***,*** précisent quelles sont les informations exigées ***et limitent leurs demandes au périmètre de l'incident ou du sujet de préoccupation***.

Amendement 151
Proposition de directive
Article 31 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les États membres veillent à ce que les violations des obligations énoncées à l'article 18 ou à l'article 20, conformément aux paragraphes 2 et 3 du présent article, soient soumises à des amendes administratives d'un montant maximum s'élevant à ***au moins*** 10 000 000 EUR ou à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle ou importante appartient, le montant le plus élevé étant retenu.	4. Les États membres veillent à ce que les violations des obligations énoncées à l'article 18 ou à l'article 20, conformément aux paragraphes 2 et 3 du présent article, soient soumises à des amendes administratives d'un montant maximum s'élevant à 10 000 000 EUR ou à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle ou importante appartient, le montant le plus élevé étant retenu.

Amendement 152
Proposition de directive
Article 32 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque les autorités compétentes disposent d'indications selon lesquelles l'infraction commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 18 et 20 donne lieu à une violation de données à caractère personnel au sens de l'article 4, paragraphe 12, du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent les autorités de contrôle compétentes en vertu des articles 55 et 56 dudit règlement dans un délai ***raisonnable***.	1. Lorsque les autorités compétentes disposent d'indications selon lesquelles l'infraction commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 18 et 20 donne lieu à une violation de données à caractère personnel au sens de l'article 4, paragraphe 12, du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent les autorités de contrôle compétentes en vertu des articles 55 et 56 dudit règlement ***sans retard injustifié et, dans tous les cas,*** dans un délai ***de 72 heures***.

Amendement 153
Proposition de directive
Article 32 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Lorsque l'autorité de contrôle compétente en vertu du règlement (UE) 2016/679 est établie dans un autre État membre que l'autorité compétente, l'autorité compétente informe l'autorité de contrôle établie dans le même État membre.	3. Lorsque l'autorité de contrôle compétente en vertu du règlement (UE) 2016/679 est établie dans un autre État membre que l'autorité compétente, l'autorité compétente informe ***également*** l'autorité de contrôle établie dans le même État membre.

Amendement 154
Proposition de directive
Article 36 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le pouvoir d'adopter des actes délégués visé à l'article ***18, paragraphe 6, et à l'article 21, paragraphe 2***, est conféré	2. Le pouvoir d'adopter des actes délégués visé à l'article ***18, paragraphe 5, et à l'article 20, paragraphe 3***, est conféré

à la Commission pour une période de cinq ans à compter du […].	à la Commission pour une période de cinq ans à compter du […].

Amendement 155
Proposition de directive
Article 36 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. ***La délégation de pouvoir visée à*** l'article 18, paragraphe ***6***, et ***à*** l'article ***21***, paragraphe ***2***, ***peut être révoquée à tout moment par*** le Parlement européen ou le Conseil***. La décision de révocation met fin*** à la ***délégation*** de ***pouvoir qui y est précisée. La révocation prend effet le jour suivant celui*** de ***la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision***. ***Elle ne porte pas atteinte*** à ***la validité des actes délégués déjà en vigueur***.	3. ***Un acte délégué adopté en vertu de*** l'article 18, paragraphe ***5***, et ***de*** l'article ***20***, paragraphe ***3***, ***n'entre en vigueur que si*** le Parlement européen ou le Conseil ***n'a pas exprimé d'objections dans un délai de trois mois*** à ***compter de*** la ***notification*** de ***cet acte au Parlement européen et au Conseil ou si, avant l'expiration*** de ***ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections***. ***Ce délai est prolongé de trois mois*** à ***l'initiative du Parlement européen ou du Conseil***.

Amendement 156
Proposition de directive
Article 36 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Un acte délégué adopté en vertu de l'article 18, paragraphe ***6***, et de l'article ***21***, paragraphe ***2***, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.	6. Un acte délégué adopté en vertu de l'article 18, paragraphe ***5***, et de l'article ***20***, paragraphe ***3***, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

ANNEXE: LISTE DES ENTITÉS OU PERSONNES AYANT APPORTÉ LEUR CONTRIBUTION À LA RAPPORTEURE

La liste suivante est établie sur une base purement volontaire, sous la responsabilité exclusive de la rapporteure. La rapporteure a reçu des contributions des entités ou personnes suivantes pour l'élaboration du projet d'avis, jusqu'à son adoption en commission.

Person	Entity
	BSA (The Software Alliance)
	BusinessEurope
	Confederation of Danish Industries
	Danish Permanent Representation
	Deutsche Telekom
	Digital Europe
	DOT Europe
	ETNO (European Telecommunications Network Operators)
	French Permanent Representation
	German Permanent Representation
	HUAWEI
	IFPI
	INTEL
	ITI (The Information Technology Industry Council)
	Kaspersky
	MÆRSK
	Microsoft
	ICANN
	MOTION PICTURE ASSOCIATION
	Orgalim
	Palo Alto Networks

	Rettighedsalliancen

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

Titre	Mesures en vue d'un niveau commun élevé de cybersécurité à travers l'Union, abrogation de la directive (UE) 2016/1148
Références	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Commission compétente au fond Date de l'annonce en séance	ITRE 21.1.2021
Avis émis par Date de l'annonce en séance	IMCO 21.1.2021
Rapporteur(e) pour avis Date de la nomination	Morten Løkkegaard 9.2.2021
Examen en commission	26.5.2021 21.6.2021
Date de l'adoption	12.7.2021
Résultat du vote final	+: 42 –: 1 0: 2
Membres présents au moment du vote final	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Andrea Caroppo, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Carlo Fidanza, Evelyne Gebhardt, Alexandra Geese, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Antonius Manders, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Marco Zullo
Suppléants présents au moment du vote final	Clara Aguilera, Maria da Graça Carvalho, Christian Doleschal, Claude Gruffat, Jiří Pospíšil, Kosma Złotowski

VOTE FINAL PAR APPEL NOMINAL
EN COMMISSION SAISIE POUR AVIS

42	+
ECR	Adam Bielan, Carlo Fidanza, Kosma Złotowski
ID	Alessandra Basso, Hynek Blaško, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle
PPE	Pablo Arias Echeverría, Andrea Caroppo, Maria da Graça Carvalho, Deirdre Clune, Christian Doleschal, Andrey Kovatchev, Antonius Manders, Jiří Pospíšil, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Morten Løkkegaard, Marco Zullo
S&D	Alex Agius Saliba, Clara Aguilera, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Claude Gruffat, Marcel Kolaja

1	-
NI	Miroslav Radačovský

2	0
ECR	Eugen Jurzyca
Renew	Svenja Hahn

Légende des signes utilisés:
+ : pour
- : contre
0 : abstention