Conseil de
l'Union européenne

**Bruxelles, le 6 avril 2021**
**(OR. en)**

**5628/21**

**Dossier interinstitutionnel:**
**2018/0328 (COD)**

**CYBER 13**
**TELECOM 25**
**COPEN 35**
**COPS 33**
**COSI 14**
**CSC 26**
**CSCI 13**
**IND 25**
**RECH 36**
**ESPACE 6**
**CODEC 92**

**ACTES LÉGISLATIFS ET AUTRES INSTRUMENTS**

| | |
|---|---|
| Objet: | Position du Conseil en première lecture en vue de l'adoption du RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination |

**RÈGLEMENT (UE) 2021/…**
**DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**du …**

**établissant le Centre de compétences européen**
**pour l'industrie, les technologies et la recherche en matière de cybersécurité**
**et le Réseau de centres nationaux de coordination**

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 173, paragraphe 3, et son article 188, premier alinéa,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[1],

statuant conformément à la procédure législative ordinaire[2],

---

1 JO C … du …, p. ….

2 Position du Parlement européen du 17 avril 2019 (non encore parue au Journal officiel) et position du Conseil en première lecture du … (non encore parue au Journal officiel). Position du Parlement européen du … (non encore parue au Journal officiel).

considérant ce qui suit:

(1) La majorité de la population de l'Union est connectée à l'internet. La vie quotidienne des personnes et les économies deviennent de plus en plus tributaires des technologies numériques. Les citoyens et les entreprises sont de plus en plus exposés à de graves incidents de cybersécurité et de nombreuses entreprises dans l'Union connaissent au moins un incident de cybersécurité chaque année. Cela met en évidence le besoin de résilience, de renforcer les capacités technologiques et industrielles, et d'utiliser des normes élevées et des solutions globales en matière de cybersécurité, qui concernent les personnes, les produits, les processus et la technologie dans l'Union, ainsi que le besoin de leadership de l'Union dans les domaines de la cybersécurité et de l'autonomie numérique. La cybersécurité peut également être renforcée en sensibilisant aux menaces en la matière et en développant les compétences, les moyens et les capacités dans l'ensemble de l'Union, tout en prenant pleinement en compte les implications et préoccupations d'ordre social et éthique.

(2) L'Union n'a cessé d'intensifier ses activités pour relever les défis croissants en matière de cybersécurité, dans le prolongement de la stratégie de cybersécurité présentée par la Commission et le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (ci-après dénommé "haut représentant") dans leur communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 7 février 2013 intitulée "Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé" (ci-après dénommée "stratégie de cybersécurité de 2013"). Cette stratégie visait à favoriser un cyberécosystème fiable, sûr et ouvert. En 2016, l'Union a adopté les premières mesures dans le domaine de la cybersécurité avec la directive (UE) 2016/1148 du Parlement européen et du Conseil[1] relative à la sécurité des réseaux et des systèmes d'information.

(3) En septembre 2017, la Commission et le haut représentant ont présenté au Parlement européen et au Conseil une communication conjointe intitulée "Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide" afin de renforcer encore la résilience, la capacité de dissuasion et la capacité de réaction de l'Union face aux cyberattaques.

---

[1] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

(4) Lors du sommet numérique de Tallinn, en septembre 2017, les chefs d'État et de gouvernement ont appelé l'Union à devenir un acteur mondial de premier plan dans le domaine de la cybersécurité d'ici à 2025, afin de s'assurer de la confiance des citoyens, consommateurs et entreprises, d'assurer leur protection en ligne et de permettre un internet libre, plus sûr et réglementé, et déclaré leur intention d'utiliser davantage de solutions de source ouverte et de normes ouvertes lors de la (re)construction de systèmes et de solutions des technologies de l'information et de la communication (TIC), évitant notamment les situations de verrouillage à l'égard du vendeur, y compris celles développées ou promues par des programmes de l'Union en matière d'interopérabilité et de normalisation, telles que ISA[2].

(5) Le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité (ci-après dénommé "Centre de compétences") établi par le présent règlement devrait contribuer à accroître la sécurité des réseaux et des systèmes d'information, y compris l'internet et les autres infrastructures critiques pour le fonctionnement de la société, telles que les transports, la santé, l'énergie, les infrastructures numériques, l'eau, les marchés financiers et les systèmes bancaires.

(6) La perturbation importante des réseaux et des systèmes d'information peut affecter les différents États membres et l'Union dans son ensemble. Un niveau élevé de sécurité des réseaux et des systèmes d'information dans l'ensemble de l'Union est donc essentiel pour la société comme pour l'économie. Actuellement, l'Union dépend de fournisseurs de services de cybersécurité non européens. Cependant, il est dans l'intérêt stratégique de l'Union de veiller à maintenir et à développer des capacités essentielles dans les domaines de la recherche et des technologies en matière de cybersécurité pour sécuriser les réseaux et les systèmes d'information des citoyens et des entreprises et, en particulier, pour sécuriser les réseaux et les systèmes d'information critiques, ainsi que pour fournir des services clés de cybersécurité.

(7) L'Union dispose d'une expertise et d'une expérience considérables dans les domaines de la recherche, des technologies et du développement industriel en matière de cybersécurité, mais les efforts des milieux industriels et de la recherche sont fragmentés, manquent de cohésion et d'une mission commune, ce qui entrave la compétitivité et la protection efficace des réseaux et systèmes dans ce domaine. Ces efforts et cette expertise doivent être mis en commun, mis en réseau et utilisés de manière efficace afin de renforcer et de compléter les capacités et les qualifications dans les domaines des technologies, de l'industrie et de la recherche existantes au niveau de l'Union et au niveau national. Bien que le secteur des TIC soit confronté à des problèmes de taille, par exemple pour trouver la main-d'œuvre qualifiée dont il a besoin, il peut tirer profit d'une représentation de la diversité de la société dans son ensemble et d'une représentation équilibrée des sexes, de la diversité ethnique et de la non-discrimination à l'égard des personnes handicapées, ainsi que d'un accès facilité à la connaissance et à la formation pour les futurs experts en cybersécurité, y compris l'éducation de ces experts dans des contextes non formels, par exemple dans des projets de logiciels libres et ouverts, des projets de technologie civique, des start-up et des microentreprises.

(8) Les petites et moyennes entreprises (PME) sont des parties prenantes essentielles du secteur de la cybersécurité de l'Union, et elles peuvent apporter des solutions de pointe grâce à leur agilité. Toutefois, les PME qui ne sont pas spécialisées en cybersécurité ont également tendance à être plus vulnérables aux incidents de cybersécurité en raison du niveau élevé d'investissements et de connaissances requis pour mettre en place des solutions efficaces en matière de cybersécurité. Il est dès lors nécessaire que le Centre de compétences et le Réseau de centres nationaux de coordination (ci-après dénommé "Réseau") apportent un soutien aux PME en les aidant à accéder aux connaissances et en leur fournissant un accès sur mesure aux résultats de la recherche et développement, afin de permettre aux PME de se protéger suffisamment et de permettre à celles dont l'activité se rapporte à la cybersécurité d'être concurrentielles et de contribuer au leadership de l'Union dans le domaine de la cybersécurité.

(9) L'expertise existe en dehors des contextes industriels et de recherche. Les projets non commerciaux et avant commercialisation, dénommés projets "de technologie civique", utilisent des normes ouvertes, des données ouvertes et des logiciels libres et ouverts, dans l'intérêt de la société et du bien public.

(10) Le domaine de la cybersécurité est varié. Les parties prenantes concernées comprennent des parties prenantes provenant d'organismes publics, d'États membres et de l'Union, ainsi que de l'industrie, de la société civile, tels que les syndicats, les associations de consommateurs, la communauté des logiciels libres et ouverts et les milieux académiques et de la recherche, et d'autres entités.

(11) Dans ses conclusions adoptées en novembre 2017, le Conseil avait invité la Commission à fournir rapidement une analyse d'impact sur les options possibles pour créer un réseau de centres de compétences en cybersécurité et un centre européen de recherche et de compétences en matière de cybersécurité, et à proposer, pour la mi-2018, l'instrument juridique pertinent pour la création d'un tel réseau et d'un tel centre.

(12) L'Union ne dispose toujours pas de moyens et de capacités technologiques et industriels suffisants pour sécuriser de manière autonome son économie et ses infrastructures critiques et devenir un acteur mondial de premier plan dans le domaine de la cybersécurité. Le niveau de la coordination et de la coopération stratégiques et durables entre les industries, les milieux de la recherche dans le domaine de la cybersécurité et les pouvoirs publics est insuffisant. L'Union pâtit d'un investissement insuffisant et d'un accès limité au savoir-faire, aux qualifications et aux installations en matière de cybersécurité et rares sont les résultats de la recherche et de l'innovation dans le domaine de la cybersécurité dans l'Union qui débouchent sur des solutions commercialisables ou qui sont largement déployés dans l'ensemble de l'économie.

(13) La création du Réseau et du Centre de compétences, ayant pour mandat de mener des actions tant en faveur des technologies industrielles que dans le domaine de la recherche et de l'innovation, est la meilleure façon d'atteindre les objectifs du présent règlement, tout en ayant le plus grand impact au niveau économique, sociétal et environnemental et en préservant les intérêts de l'Union.

(14) Le Centre de compétences devrait être le principal instrument de l'Union pour mettre en commun les investissements dans la recherche, les technologies et le développement industriel en matière de cybersécurité et pour mettre en œuvre les projets et initiatives pertinents, en collaboration avec le Réseau. Le Centre de compétences devrait gérer le soutien financier lié à la cybersécurité au titre du programme-cadre pour la recherche et l'innovation "Horizon Europe", établi par le règlement (UE) 2021/... du Parlement européen et du Conseil[1+], et du programme pour une Europe numérique, établi par le règlement (UE) 2021/... du Parlement européen et du Conseil[2++], et il devrait être ouvert, s'il y a lieu, à d'autres programmes. Cette approche devrait contribuer à créer des synergies et à coordonner l'aide financière liée aux initiatives de l'Union dans le domaine de la recherche et du développement, de l'innovation, des technologies et du développement industriel en matière de cybersécurité, et à éviter les doubles emplois inutiles.

---

1 Règlement (UE) 2021/... du Parlement européen et du Conseil du … portant établissement du programme-cadre pour la recherche et l'innovation "Horizon Europe" et définissant ses règles de participation et de diffusion, et abrogeant les règlements (UE) n° 1290/2013 et (UE) n° 1291/2013 (JO ...).

\+ JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20 et insérer le numéro, la date et la référence JO dans la note de bas de page.

2 Règlement (UE) 2021/... du Parlement européen et du Conseil du … établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240 (JO ...).

++ JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20 et insérer le numéro, la date et la référence JO dans la note de bas de page.

(15) Il importe que le respect des droits fondamentaux et un comportement éthique soient garantis dans les projets de recherche en matière de cybersécurité soutenus par le Centre de compétences.

(16) Le Centre de compétences ne devrait pas exercer de tâches opérationnelles en matière de cybersécurité, telles que celles liées aux centres de réponse aux incidents de sécurité informatique (CSIRT), y compris le suivi et le traitement des incidents de cybersécurité. Toutefois, le Centre de compétences devrait pouvoir faciliter le développement d'infrastructures TIC au service des industries, en particulier des PME, des milieux de la recherche, de la société civile et du secteur public, conformément à la mission et aux objectifs prévus dans le présent règlement. Là où les CSIRT et d'autres parties prenantes cherchent à promouvoir le signalement et la divulgation de vulnérabilités, le Centre de compétences et les membres de la communauté de compétences en matière de cybersécurité (ci-après dénommée "communauté") devraient pouvoir soutenir ces parties prenantes, à leur demande, dans les limites de leurs tâches respectives et en évitant tout double emploi avec l'Agence de l'Union européenne pour la cybersécurité (ENISA), établie par le règlement (UE) 2019/881 du Parlement européen et du Conseil[1].

[1] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

(17) Le Centre de compétences, la communauté et le Réseau sont destinés à tirer parti de l'expérience et de la représentation large des parties prenantes concernées, acquises grâce au partenariat public-privé contractuel en matière de cybersécurité instauré entre la Commission et l'Organisation européenne pour la cybersécurité (ECSO) pour la durée du programme-cadre pour la recherche et l'innovation "Horizon 2020" (2014-2020) établi par le règlement (UE) n° 1291/2013 du Parlement européen et du Conseil[1], et des enseignements tirés de quatre projets pilotes lancés au début de l'année 2019 dans le cadre d'Horizon 2020, à savoir CONCORDIA, ECHO, SPARTA et CyberSec4Europe, ainsi que du projet pilote et de l'action préparatoire sur les audits de logiciels libres et ouverts (EU FOSSA), pour la gestion de la communauté et la représentation de la communauté au sein du Centre de compétences.

(18) Compte tenu de l'ampleur du défi que représente la cybersécurité et des investissements dans les moyens et capacités en matière de cybersécurité consentis dans d'autres parties du monde, l'Union et les États membres devraient être encouragés à accroître leur soutien financier à la recherche, au développement et au déploiement dans ce domaine. Dans le but de réaliser des économies d'échelle et d'atteindre un niveau comparable de protection dans l'ensemble de l'Union, les États membres devraient déployer leurs efforts dans un cadre de l'Union en contribuant activement aux travaux du Centre de compétences et du Réseau.

---

[1] Règlement (UE) n° 1291/2013 du Parlement européen et du Conseil du 11 décembre 2013 portant établissement du programme-cadre pour la recherche et l'innovation "Horizon 2020" (2014-2020) et abrogeant la décision n° 1982/2006/CE (JO L 347 du 20.12.2013, p. 104)**.**

(19) Afin de favoriser la compétitivité de l'Union et la mise en place de normes élevées en matière de cybersécurité au niveau international, le Centre de compétences et la communauté devraient rechercher les échanges avec la communauté internationale sur les évolutions dans le domaine de la cybersécurité, y compris les évolutions des produits et des processus ainsi que des normes et des normes techniques, lorsque cela entre dans le cadre de la mission, des objectifs et des tâches du Centre de compétences. Aux fins du présent règlement, les normes techniques pertinentes pourraient comprendre la création d'applications de référence, y compris celles publiées dans le cadre de licences types ouvertes.

(20) Le siège du Centre de compétences se trouve à Bucarest.

(21) Lorsqu'il élabore son programme de travail annuel (ci-après dénommé "programme de travail annuel"), le Centre de compétences devrait informer la Commission de ses besoins de cofinancement sur la base des contributions prévues par les États membres au titre du cofinancement d'actions conjointes, de manière à ce que la Commission soit à même de prendre en compte la contribution de l'Union correspondante lors de l'élaboration du projet de budget général de l'Union pour l'exercice suivant.

(22) Lorsqu'elle élabore le programme de travail d'Horizon Europe pour les questions liées à la cybersécurité, y compris dans le cadre de son processus de consultation des parties prenantes et spécialement avant l'adoption dudit programme de travail, la Commission devrait prendre en compte la contribution du Centre de compétences et la partager avec le comité du programme Horizon Europe.

(23) Afin de permettre au Centre de compétences de jouer son rôle dans le domaine de la cybersécurité, de faciliter la participation du Réseau et de donner aux États membres un rôle important dans la gouvernance, il convient que le Centre de compétences soit créé sous la forme d'un organisme de l'Union doté de la personnalité juridique auquel le règlement délégué (UE) 2019/715[1] de la Commission doit s'appliquer. Le Centre de compétences devrait exercer un double rôle, consistant à réaliser des tâches spécifiques dans les domaines de l'industrie, des technologies et de la recherche en matière de cybersécurité conformément au présent règlement et à gérer les financements liés à la cybersécurité issus de plusieurs programmes en même temps, notamment d'Horizon Europe et du programme pour une Europe numérique, et éventuellement aussi d'autres programmes de l'Union. Cette gestion devrait s'exercer conformément aux règles applicables à ces programmes. Néanmoins, étant donné que le financement destiné au fonctionnement du Centre de compétences proviendrait principalement d'Horizon Europe et du programme pour une Europe numérique, il est nécessaire que le Centre de compétences soit considéré comme un partenariat aux fins de l'exécution du budget, y compris pendant la phase de programmation.

(24) Du fait de la contribution de l'Union, l'accès aux résultats des activités et des projets du Centre de compétences doit être aussi ouvert que possible et aussi fermé que nécessaire, et le réemploi de ces résultats doit être possible s'il y a lieu.

---

[1] Règlement délégué (UE) 2019/715 de la Commission du 18 décembre 2018 portant règlement financier-cadre des organismes créés en vertu du traité sur le fonctionnement de l'Union européenne et du traité Euratom et visés à l'article 70 du règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil (JO L 122 du 10.5.2019, p. 1).

(25) Le Centre de compétences devrait faciliter et coordonner les travaux du Réseau. Le Réseau devrait être composé d'un centre national de coordination par État membre. Les centres nationaux de coordination qui ont été reconnus par la Commission comme ayant la capacité nécessaire de gérer des fonds pour remplir la mission et les objectifs prévus par le présent règlement devraient bénéficier d'un soutien financier direct de l'Union, y compris de subventions octroyées sans appel à propositions, pour exercer leurs activités liées au présent règlement.

(26) Les centres nationaux de coordination devraient être des entités du secteur public ou des entités avec une participation majoritaire du secteur public, exerçant des fonctions d'administration publique en vertu du droit national, y compris sur délégation, et ils devraient être sélectionnés par les États membres. Il devrait être possible que les fonctions d'un centre national de coordination dans un État membre donné soient exercées par une entité qui remplit d'autres fonctions découlant du droit de l'Union, telles que les fonctions d'une autorité nationale compétente, d'un point de contact unique au sens de la directive (UE) 2016/1148 ou de tout autre règlement de l'Union, ou d'un pôle d'innovation numérique au sens du règlement (UE) 2021/…[+]. D'autres entités du secteur public ou entités exerçant des fonctions d'administration publique dans un État membre devraient pouvoir assister le centre national de coordination de cet État membre dans l'exercice de ses fonctions.

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

(27) Les centres nationaux de coordination devraient avoir les capacités administratives nécessaires, posséder une expertise dans les domaines de l'industrie, des technologies et de la recherche en matière de cybersécurité, ou y avoir accès, et être en mesure d'assurer un dialogue et une coordination efficaces avec l'industrie, le secteur public et les milieux de la recherche.

(28) L'éducation, dans les États membres, devrait refléter l'importance de disposer d'une sensibilisation adéquate au domaine de la cybersécurité et de qualifications adéquates dans ce domaine. À cette fin, en tenant compte du rôle de l'ENISA et sans préjudice des compétences des États membres en matière d'éducation, les centres nationaux de coordination, aux côtés des autorités publiques et des parties prenantes concernées, devraient contribuer à promouvoir et à diffuser des programmes éducatifs en matière de cybersécurité.

(29) Les centres nationaux de coordination devraient pouvoir recevoir des subventions du Centre de compétences afin d'apporter un soutien financier à des tiers sous la forme de subventions. Les coûts directs engagés par les centres nationaux de coordination pour la fourniture et la gestion d'un soutien financier à des tiers devraient être éligibles à un financement au titre des programmes pertinents.

(30) Le Centre de compétences, le Réseau et la communauté devraient contribuer à faire progresser et à diffuser les produits, les services et les processus les plus récents en matière de cybersécurité. Parallèlement, le Centre de compétences et le Réseau devraient promouvoir les capacités en matière de cybersécurité des secteurs du côté de la demande, en particulier en soutenant les développeurs et les opérateurs dans des secteurs tels que les transports, l'énergie, la santé, la finance, l'administration, les télécommunications, l'industrie manufacturière et l'espace, afin d'aider ces développeurs et opérateurs à résoudre leurs problèmes de cybersécurité, par exemple en mettant en œuvre la sécurité dès la conception. Le Centre de compétences et le Réseau devraient également soutenir la normalisation et le déploiement de produits, de services et de processus de cybersécurité, tout en promouvant, dans la mesure du possible, la mise en œuvre du cadre européen de certification de cybersécurité établi par le règlement (UE) 2019/881.

(31) En raison de la rapidité avec laquelle les cybermenaces et la cybersécurité changent, l'Union doit être capable de s'adapter rapidement et en permanence aux nouvelles évolutions dans ce domaine. Le Centre de compétences, le Réseau et la communauté devraient dès lors être suffisamment souples afin de garantir la capacité nécessaire pour réagir à de telles évolutions. Ils devraient favoriser des projets qui aident les entités à être en mesure de renforcer constamment leurs capacités pour accroître leur propre résilience et celle de l'Union.

(32) Le Centre de compétences devrait soutenir la communauté. Le Centre de compétences devrait mettre en œuvre les parties relatives à la cybersécurité d'Horizon Europe et du programme pour une Europe numérique conformément au programme de travail pluriannuel du Centre de compétences (ci-après dénommé "programme de travail pluriannuel"), au programme de travail annuel et au processus de planification stratégique d'Horizon Europe en attribuant des subventions et d'autres formes de financement, essentiellement à la suite d'un appel à propositions concurrentiel. Le Centre de compétences devrait aussi faciliter le transfert d'expertise au sein du Réseau et de la communauté et soutenir les investissements conjoints de l'Union, des États membres ou de l'industrie. Il devrait accorder une attention particulière au soutien des PME dans le domaine de la cybersécurité ainsi qu'aux actions qui contribuent à combler le déficit de compétences.

(33) L'assistance technique à la préparation des projets devrait être apportée de manière totalement objective et transparente, afin de garantir que tous les bénéficiaires potentiels reçoivent les mêmes informations, et devrait éviter les conflits d'intérêts.

(34) Le Centre de compétences devrait encourager et soutenir la coopération et la coordination stratégiques à long terme des activités de la communauté, qui associerait un groupe important, ouvert, interdisciplinaire et varié de parties prenantes européennes concernées par les technologies de la cybersécurité. Il convient que la communauté inclue les entités de recherche, les industries et le secteur public. La communauté devrait contribuer aux activités du Centre de compétences, au programme de travail pluriannuel et au programme de travail annuel, notamment par l'intermédiaire du groupe consultatif stratégique. Elle devrait également bénéficier des activités de renforcement des communautés déployées par le Centre de compétences et le Réseau, mais elle ne devrait pas être privilégiée d'une autre manière en ce qui concerne les appels à propositions ou les appels d'offres. La communauté devrait être constituée d'organismes collectifs et d'organisations collectives. Dans le même temps, afin de tirer parti de l'ensemble de l'expertise en matière de cybersécurité dans l'Union, le Centre de compétences et ses organes devraient pouvoir également recourir à l'expertise de personnes physiques en tant qu'experts ad hoc.

(35) Le Centre de compétences devrait coopérer et assurer des synergies avec l'ENISA et devrait recevoir des contributions pertinentes de l'ENISA lorsqu'il détermine les priorités de financement.

(36) Afin de répondre aux besoins tant du côté de l'offre de cybersécurité que du côté de la demande de cybersécurité, la tâche du Centre de compétences consistant à fournir aux industries des connaissances et une assistance technique en matière de cybersécurité devrait porter à la fois sur les produits, processus et services TIC et sur tous les autres produits et processus technologiques dans lesquels la cybersécurité doit être intégrée. Lorsqu'il en fait la demande, le secteur public pourrait également bénéficier du soutien du Centre de compétences.

(37) Afin de créer un environnement de cybersécurité viable, il importe que la sécurité dès la conception soit mise en œuvre en tant que principe dans le processus de développement, de maintenance, d'exploitation et de mise à jour des infrastructures, des produits et des services, notamment en soutenant des méthodes de développement sûres de pointe, des essais de sécurité et des audits de sécurité appropriés, en mettant à disposition, sans tarder, des mises à jour remédiant aux vulnérabilités ou menaces connues et en permettant aux tiers, lorsque c'est possible, de créer et de fournir des mises à jour au-delà de la durée de vie respective de chaque produit. La sécurité dès la conception devrait être assurée sur l'ensemble du cycle de vie des produits, services ou processus TIC, ainsi que grâce à des processus de développement qui évoluent constamment pour réduire le risque de préjudice causé par une utilisation malveillante.

(38) Alors que le Centre de compétences et le Réseau devraient s'efforcer de renforcer les synergies et la coordination entre les sphères civile et de défense en matière de cybersécurité, les projets relevant du présent règlement qui sont financés par Horizon Europe devraient être mis en œuvre conformément au règlement (UE) 2021/…[+], qui prévoit que les activités de recherche et d'innovation menées au titre d'Horizon Europe doivent se concentrer exclusivement sur les applications civiles.

(39) Le présent règlement s'applique essentiellement aux questions civiles, mais les activités des États membres menées au titre du présent règlement peuvent tenir compte des spécificités des États membres lorsque la politique en matière de cybersécurité est menée par des autorités effectuant des tâches à la fois civiles et militaires, devraient rechercher les complémentarités avec les instruments de financement relatifs à la défense et éviter les chevauchements avec ces instruments.

(40) Le présent règlement devrait garantir la responsabilité et la transparence du Centre de compétences et des entreprises qui reçoivent des financements, conformément aux règlements relatifs aux programmes concernés.

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

(41) La mise en œuvre des projets de déploiement, notamment des projets de déploiement liés aux infrastructures et aux capacités déployées au niveau de l'Union ou par le biais d'acquisitions conjointes, pourrait être divisée en différentes phases de mise en œuvre, comme des appels d'offres distincts pour la conception de l'architecture matérielle et logicielle, la production du matériel et des logiciels, et leur exploitation et leur maintenance, mais les entreprises pourraient ne participer qu'à une seule de ces phases et, s'il y a lieu, pourrait exiger des bénéficiaires lors de l'une ou de plusieurs de ces phases qu'ils remplissent certaines conditions en matière de propriété ou de contrôle au niveau européen.

(42) Compte tenu de son expertise en matière de cybersécurité et de son mandat en tant que point de référence pour les conseils et l'expertise en matière de cybersécurité pour les institutions, organes et organismes de l'Union ainsi que pour les parties prenantes concernées de l'Union, et compte tenu des contributions qu'elle a recueillies dans le cadre de ses tâches, l'ENISA devrait jouer un rôle actif dans les activités du Centre de compétences, y compris l'élaboration de la stratégie, en évitant toute duplication de leurs tâches, en particulier grâce à son rôle d'observateur permanent au sein du conseil de direction du Centre de compétences. En ce qui concerne la rédaction de la stratégie, du programme de travail annuel et du programme de travail pluriannuel, le directeur exécutif du Centre de compétences et le conseil de direction devraient tenir compte de tous les avis et contributions stratégiques pertinents fournis par l'ENISA, conformément au règlement intérieur du conseil de direction.

(43) Lorsqu'ils reçoivent une contribution financière du budget général de l'Union, les centres nationaux de coordination et les entités qui font partie de la communauté devraient faire connaître au public le fait que leurs activités respectives sont menées dans le cadre du présent règlement.

(44) Les coûts découlant de la création du Centre de compétences et des activités administratives et de coordination du Centre de compétences devraient être financés par l'Union et par les États membres, au prorata des contributions volontaires des États membres aux actions conjointes. Afin d'éviter un double financement, ces activités ne devraient pas bénéficier simultanément d'une contribution d'autres programmes de l'Union.

(45) Le conseil de direction, qui devrait se composer de représentants des États membres et de la Commission, devrait définir l'orientation générale des activités du Centre de compétences et devrait veiller à ce que celui-ci s'acquitte de ses tâches conformément au présent règlement. Le conseil de direction devrait adopter la stratégie.

(46) Le conseil de direction devrait être investi des pouvoirs nécessaires pour établir le budget du Centre de compétences. Il devrait vérifier l'exécution du budget, adopter les règles financières appropriées et établir des procédures de travail transparentes pour la prise de décisions par le Centre de compétences, y compris pour l'adoption, en tenant compte de la stratégie, du programme de travail annuel et du programme de travail pluriannuel. Le conseil de direction devrait également adopter son règlement intérieur, nommer le directeur exécutif et statuer sur toute prorogation ou cessation du mandat du directeur exécutif.

(47) Le conseil de direction devrait superviser les activités stratégiques et de mise en œuvre du Centre de compétences et veiller à ce que ces activités soient mises en adéquation entre elles. Dans son rapport annuel, le Centre de compétences devrait mettre particulièrement l'accent sur les objectifs stratégiques qu'il a atteints et, si nécessaire, proposer des mesures visant à améliorer encore le niveau de réalisation de ces objectifs stratégiques.

(48) Afin que le Centre de compétences fonctionne de manière appropriée et efficace, la Commission et les États membres devraient veiller à ce que les personnes à nommer au conseil de direction disposent d'une expertise et d'une expérience professionnelles appropriées dans des domaines fonctionnels. La Commission et les États membres devraient s'efforcer de limiter le roulement de leurs représentants respectifs au sein du conseil de direction, afin de garantir la continuité des travaux de ce dernier.

(49) Compte tenu du statut spécifique du Centre de compétences et de sa responsabilité en ce qui concerne la mise en œuvre des fonds de l'Union, en particulier ceux provenant d'Horizon Europe et du programme pour une Europe numérique, la Commission devrait disposer, au sein du conseil de direction, de 26 % du total des voix pour les décisions impliquant des fonds de l'Union, afin de maximiser la valeur ajoutée de l'Union de ces décisions, tout en veillant à la légalité de ces décisions et à leur cohérence avec les priorités de l'Union.

(50) Le bon fonctionnement du Centre de compétences exige que son directeur exécutif soit nommé de manière transparente sur la base du mérite, de ses qualifications et compétences attestées en matière d'administration et de gestion et de son expérience en matière de cybersécurité, et que les fonctions du directeur exécutif soient exercées en toute indépendance.

(51) Le Centre de compétences devrait disposer d'un groupe consultatif stratégique en tant qu'organe consultatif. Le groupe consultatif stratégique devrait fournir des conseils sur la base d'un dialogue régulier entre le Centre de compétences et la communauté, qui devrait être formée des représentants du secteur privé, d'organisations de consommateurs, des milieux académiques et d'autres parties prenantes pertinentes. Le groupe consultatif stratégique devrait se concentrer sur les questions intéressant les parties prenantes et les porter à l'attention du conseil de direction et du directeur exécutif. Les tâches du groupe consultatif stratégique devraient inclure la fourniture de conseils sur la stratégie, le programme de travail annuel et le programme de travail pluriannuel. Il convient que les différentes parties prenantes soient représentées de façon équilibrée au sein du groupe consultatif stratégique, une attention particulière étant accordée à la représentation des PME, afin d'assurer une représentation appropriée des parties prenantes dans les travaux du Centre de compétences.

(52) Les contributions des États membres aux ressources du Centre de compétences pourraient être financières ou en nature. Par exemple, ces contributions financières pourraient consister en une subvention accordée par un État membre à un bénéficiaire situé sur son territoire, qui complète le soutien financier octroyé par l'Union à un projet dans le cadre du programme de travail annuel. Les contributions en nature, quant à elles, interviendraient généralement lorsqu'une entité d'un État membre est elle-même bénéficiaire d'un soutien financier de l'Union. Par exemple, si l'Union subventionne une activité d'un centre national de coordination à un taux de financement de 50 %, les coûts restants de l'activité seraient comptabilisés comme une contribution en nature. Autre exemple, lorsqu'une entité d'un État membre reçoit un soutien financier de l'Union pour la création ou la modernisation d'une infrastructure qui doit être partagée entre les parties prenantes conformément au programme de travail annuel, les coûts non subventionnés y afférents seraient comptabilisés comme des contributions en nature.

(53) Conformément aux dispositions pertinentes du règlement délégué (UE) 2019/715 concernant les conflits d'intérêts, le Centre de compétences devrait disposer de règles en matière de prévention, de détection, de résolution et de gestion des conflits d'intérêts à l'égard de ses membres, organes et membres du personnel, du conseil de direction, ainsi que du groupe consultatif stratégique et de la communauté. Les États membres devraient veiller à la prévention, à la détection et à la résolution des conflits d'intérêts en ce qui concerne les centres nationaux de coordination conformément au droit national. Le Centre de compétences devrait également appliquer les dispositions pertinentes du droit de l'Union en ce qui concerne l'accès du public aux documents prévu par le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil[1]. Le traitement de données à caractère personnel effectué par le Centre de compétences devrait être soumis au règlement (UE) 2018/1725 du Parlement européen et du Conseil[2]. Le Centre de compétences devrait respecter les dispositions du droit de l'Union qui s'appliquent aux institutions de l'Union, et le droit national concernant le traitement des informations, en particulier le traitement des informations non classifiées sensibles et des informations classifiées de l'UE.

---

1 Règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

2 Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

(54) Les intérêts financiers de l'Union et des États membres devraient être protégés par des mesures proportionnées tout au long du cycle des dépenses, notamment par la prévention et la détection des irrégularités et les enquêtes en la matière, le recouvrement des fonds perdus, indûment versés ou mal employés et, s'il y a lieu, l'application de sanctions administratives et financières conformément au règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil[1] (ci-après dénommé "règlement financier").

(55) Le Centre de compétences devrait fonctionner de manière ouverte et transparente. Il devrait fournir en temps utile toutes les informations pertinentes et promouvoir ses activités, notamment des activités d'information et de diffusion à l'intention du grand public. Le règlement intérieur du conseil de direction du Centre de compétences et du groupe consultatif stratégique devrait être mis à la disposition du public.

(56) L'auditeur interne de la Commission devrait exercer à l'égard du Centre de compétences les mêmes pouvoirs que ceux qu'il exerce à l'égard de la Commission.

(57) La Commission, la Cour des comptes et l'Office européen de lutte antifraude devraient avoir accès à toutes les informations nécessaires et aux locaux du Centre de compétences pour mener les audits et les enquêtes concernant les subventions, contrats et accords signés par le Centre de compétences.

---

[1] Règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union, modifiant les règlements (UE) n° 1296/2013, (UE) n° 1301/2013, (UE) n° 1303/2013, (UE) n° 1304/2013, (UE) n° 1309/2013, (UE) n° 1316/2013, (UE) n° 223/2014, (UE) n° 283/2014 et la décision n° 541/2014/UE, et abrogeant le règlement (UE, Euratom) n° 966/2012 (JO L 193 du 30.7.2018, p. 1).

(58) Étant donné que les objectifs du présent règlement, à savoir le renforcement de la compétitivité et des capacités de l'Union, le maintien et le développement des capacités de l'Union dans les domaines de la recherche, des technologies et de l'industrie en matière de cybersécurité, le renforcement de la compétitivité du secteur de la cybersécurité de l'Union et la transformation de la cybersécurité en un avantage concurrentiel pour d'autres industries de l'Union, ne peuvent pas être atteints de manière suffisante par les seuls États membres compte tenu du fait que les ressources existantes sont limitées et dispersées ainsi qu'en raison de l'ampleur des investissements nécessaires, mais peuvent, pour éviter la duplication inutile de ces efforts, contribuer à atteindre une masse critique d'investissements et garantir l'utilisation optimale des fonds publics et la promotion d'un niveau élevé de cybersécurité dans l'ensemble des États membres, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

# CHAPITRE I
# DISPOSITIONS ET PRINCIPES GÉNÉRAUX DU CENTRE DE COMPÉTENCES ET DU RÉSEAU

*Article premier*

*Objet et champ d'application*

1. Le présent règlement établit le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité (ci-après dénommé "Centre de compétences") et le Réseau de centres nationaux de coordination (ci-après dénommé "Réseau"). Le présent règlement fixe les règles applicables à la désignation des centres nationaux de coordination et à la création de la communauté de compétences en matière de cybersécurité (ci-après dénommée "communauté").

2. Le Centre de compétences joue un rôle essentiel dans la mise en œuvre de la partie "Cybersécurité" du programme pour une Europe numérique, en particulier en ce qui concerne les actions se rapportant à l'article 6 du règlement (UE) 2021/…[+], et contribue à la mise en œuvre d'Horizon Europe, en particulier en ce qui concerne l'annexe I, pilier II, section 3.1.3. de la décision (UE) 2021/… du Conseil[1++].

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

[1] Décision (UE) 2021/… du Conseil du … établissant le programme spécifique d'exécution du programme-cadre pour la recherche et l'innovation "Horizon Europe", et abrogeant la décision 2013/743/UE (JO …).

[++] JO: prière d'insérer dans le texte le numéro de la décision figurant dans le document ST 8967/20 et insérer le numéro, la date et la référence JO dans la note de bas de page.

3. Les États membres contribuent collectivement aux travaux du Centre de compétences et du Réseau.

4. Le présent règlement s'entend sans préjudice des compétences des États membres en ce qui concerne la sécurité publique, la défense et la sécurité nationale, et les activités de l'État dans les domaines du droit pénal.

*Article 2*

*Définitions*

Aux fins du présent règlement, on entend par:

1) "cybersécurité", les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces;

2) "réseau et système d'information", un réseau et système d'information au sens de l'article 4, point 1), de la directive (UE) 2016/1148;

3) "produits, services et processus de cybersécurité", les produits, services ou processus TIC, commerciaux et non commerciaux, ayant pour objectif précis de protéger les réseaux et systèmes d'information ou de garantir la confidentialité, l'intégrité et l'accessibilité des données qui sont traitées ou stockées dans des réseaux et des systèmes d'information, ainsi que la cybersécurité des utilisateurs de ces systèmes et des autres personnes exposées aux cybermenaces;

4) "cybermenace", toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes;

5) "action conjointe", une action figurant dans le programme de travail annuel qui reçoit un soutien financier de l'Union au titre d'Horizon Europe, du programme pour une Europe numérique ou d'autres programmes de l'Union, ainsi qu'un soutien financier ou en nature d'un ou de plusieurs États membres, et qui est mise en œuvre au travers de projets faisant intervenir des bénéficiaires établis dans lesdits États membres et qui reçoivent un soutien financier ou en nature desdits États membres;

6) "contribution en nature", les coûts éligibles engagés par les centres nationaux de coordination et d'autres entités publiques dans le cadre de leur participation à des projets financés au titre du présent règlement, lorsque ces coûts ne sont financés ni par une contribution de l'Union ni par des contributions financières d'États membres;

7) "pôle européen d'innovation numérique", un pôle européen d'innovation numérique tel qu'il est défini à l'article 2, point e) du règlement (UE) 2021/…[+];

8) "stratégie", une stratégie globale et durable dans les domaines de l'industrie, des technologies et de la recherche en matière de cybersécurité, qui formule des recommandations stratégiques en vue du développement et de la croissance du secteur européen de la cybersécurité dans les domaines de l'industrie, des technologies et de la recherche et définit les priorités stratégiques pour les activités du Centre de compétences, et qui n'est pas contraignante en ce qui concerne les décisions à adopter relatives aux programmes de travail annuels;

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

9) "assistance technique", une assistance apportée par le Centre de compétences aux centres nationaux de coordination ou à la communauté dans l'exécution de leurs tâches, consistant à fournir des connaissances ou à faciliter l'accès à l'expertise dans le domaine de la recherche, des technologies et de l'industrie en matière de cybersécurité, à favoriser la mise en réseau, à sensibiliser et à promouvoir la coopération, ou l'assistance apportée par le Centre de compétences, en collaboration avec les centres nationaux de coordination, aux parties prenantes en ce qui concerne la préparation de projets en rapport avec la mission du Centre de compétences et du Réseau et les objectifs du Centre de compétences.

*Article 3*

*Mission du Centre de compétences et du Réseau*

1. La mission du Centre de compétences et du Réseau consiste à aider l'Union à:

a) renforcer son leadership et son autonomie stratégique dans le domaine de la cybersécurité en maintenant et développant les moyens et capacités académiques, sociétaux, technologiques, industriels et de recherche de l'Union en matière de cybersécurité nécessaires pour renforcer la confiance et la sécurité, y compris la confidentialité, l'intégrité et l'accessibilité des données, au sein du marché unique numérique;

b) soutenir les moyens, capacités, et compétences technologiques de l'Union en ce qui concerne la résilience et la fiabilité des infrastructures des réseaux et des systèmes d'information, y compris des infrastructures critiques ainsi que du matériel et des logiciels couramment utilisés dans l'Union; et

c) accroître la compétitivité du secteur de la cybersécurité de l'Union au niveau mondial, à garantir des normes de cybersécurité élevées dans l'ensemble de l'Union et à transformer la cybersécurité en un avantage concurrentiel pour d'autres industries de l'Union.

2. Le Centre de compétences et le Réseau s'acquittent de leurs tâches en collaboration avec l'ENISA et la communauté, s'il y a lieu.

3. Le Centre de compétences utilise les ressources financières pertinentes de l'Union de manière à contribuer à la mission énoncée au paragraphe 1, conformément aux actes législatifs établissant les programmes concernés, notamment Horizon Europe et le programme pour une Europe numérique.

*Article 4*

*Objectifs du Centre de compétences*

1. Le Centre de compétences a pour objectif général de promouvoir la recherche, l'innovation et le déploiement dans le domaine de la cybersécurité afin de remplir la mission décrite à l'article 3.

2. Le Centre de compétences poursuit les objectifs spécifiques suivants:

a) renforcer les moyens, les capacités, les connaissances et les infrastructures en matière de cybersécurité au bénéfice des industries, en particulier les PME, des milieux de la recherche, du secteur public et de la société civile en tant que besoin;

b) promouvoir la résilience en matière de cybersécurité, l'adoption de bonnes pratiques en la matière, le principe de la sécurité dès le stade de la conception et la certification de la sécurité des produits et services numériques, d'une façon qui complète les efforts déployés par d'autres entités publiques;

c) contribuer à la mise en place d'un écosystème européen de cybersécurité solide qui réunisse toutes les parties prenantes concernées.

3. Le Centre de compétences met en œuvre les objectifs spécifiques énoncés au paragraphe 2:

a) en établissant des recommandations stratégiques pour ce qui est de la recherche, de l'innovation et du déploiement en matière de cybersécurité conformément au droit de l'Union, et en définissant les priorités stratégiques pour les activités du Centre de compétences;

b) en mettant en œuvre des actions au titre des programmes de financement pertinents de l'Union, conformément aux programmes de travail concernés et aux actes législatifs de l'Union établissant lesdits programmes de financement;

c) en favorisant la coopération et la coordination entre les centres nationaux de coordination, avec la communauté et au sein de celle-ci; et

d) lorsque cela est pertinent, opportun et nécessaire, en acquérant et en exploitant des services et infrastructures TIC pour remplir les tâches énoncées à l'article 5 et conformément aux programmes de travail respectifs visés à l'article 5, paragraphe 3, point b).

*Article 5*

*Tâches du Centre de compétences*

1. Afin de remplir sa mission et ses objectifs, le Centre de compétences est chargé:

   a) de tâches stratégiques; et

   b) de tâches de mise en œuvre.

2. Les tâches stratégiques visées au paragraphe 1, point a), consistent à:

   a) mettre au point la stratégie et en contrôler la mise en œuvre;

   b) par l'entremise de la stratégie et du programme de travail pluriannuel, tout en évitant toute duplication des activités avec l'ENISA et en prenant en compte la nécessité de créer des synergies entre le volet "cybersécurité" et d'autres volets d'Horizon Europe et du programme pour une Europe numérique:

      i) définir des priorités pour les travaux du Centre de compétences concernant:

         1) le renforcement de la recherche et de l'innovation en matière de cybersécurité, couvrant l'intégralité du cycle de l'innovation, et le déploiement de cette recherche et innovation;

2) le développement de moyens, de capacités et d'infrastructures industriels, technologiques et de recherche en matière de cybersécurité;

3) le renforcement des qualifications et compétences en matière de cybersécurité et de technologies dans les secteurs de l'industrie, des technologies et de la recherche, ainsi qu'à tous les niveaux d'enseignement pertinents, en favorisant l'équilibre entre les hommes et les femmes;

4) le déploiement de produits, de services et de processus de cybersécurité;

5) le soutien à l'adoption par le marché de produits, services et processus de cybersécurité contribuant à la mission énoncée à l'article 3;

6) le soutien à l'adoption et à l'intégration de produits, services et processus de pointe en matière de cybersécurité par les pouvoirs publics à leur demande, par les secteurs du côté de la demande et par d'autres utilisateurs:

ii) en soutenant l'industrie de la cybersécurité, en particulier les PME, en vue de renforcer l'excellence, les capacités et la compétitivité de l'Union en matière de cybersécurité, y compris en vue d'établir un lien avec des marchés potentiels et des possibilités de déploiement, et d'attirer les investissements; et

iii) en fournissant un soutien et une assistance technique aux start-up, aux PME, aux microentreprises, aux associations, aux experts individuels et aux projets de technologie civique en matière de cybersécurité;

c) veiller aux synergies entre les institutions, organes et organismes de l'Union concernés, en particulier l'ENISA, et à la coopération avec ceux-ci, tout en évitant toute duplication des activités avec ces institutions, organes et organismes;

d) coordonner les centres nationaux de coordination par l'intermédiaire du Réseau et assurer un échange régulier d'expertise;

e) fournir aux État membre, à leur demande, des conseils d'experts dans les domaines de l'industrie, des technologies et de la recherche en matière de cybersécurité, y compris en ce qui concerne l'acquisition et le déploiement de technologies;

f) faciliter la collaboration et le partage d'expertise entre toutes les parties prenantes concernées, en particulier les membres de la communauté;

g) assister à des conférences, foires et forums nationaux, internationaux et de l'Union en rapport avec la mission, les objectifs et les tâches du Centre de compétences, dans le but de partager des points de vue et d'échanger des bonnes pratiques pertinentes avec d'autres participants;

h) faciliter l'utilisation des résultats des projets de recherche et d'innovation dans des actions liées au développement de produits, services et processus de cybersécurité, tout en cherchant à éviter la fragmentation et les doubles emplois et reproduire les bonnes pratiques en matière de cybersécurité et les bons produits, services et processus de cybersécurité, en particulier ceux mis au point par des PME et ceux utilisant des logiciels ouverts.

3. Les tâches de mise en œuvre visées au paragraphe 1, point b), consistent à:

a) coordonner et gérer les travaux du Réseau et de la communauté en vue de remplir la mission énoncée à l'article 3, en particulier en soutenant les start-up, les PME, les microentreprises, les associations et les projets de technologie civique de l'Union en matière de cybersécurité et en facilitant leur accès à l'expertise, aux financements, aux investissements et aux marchés;

b) établir et mettre en œuvre le programme de travail annuel, conformément à la stratégie et au programme de travail pluriannuel, pour les volets relatifs à la cybersécurité:

i) du programme pour une Europe numérique, en particulier les actions liées à l'article 6 du règlement (UE) 2021/…[+];

ii) des actions conjointes recevant un soutien au titre des dispositions relatives à la cybersécurité d'Horizon Europe, en particulier en ce qui concerne l'annexe I, pilier II, section 3.1.3 de la décision (UE) 2021/…[++], conformément au programme de travail pluriannuel et au processus de planification stratégique d'Horizon Europe; et

iii) d'autres programmes de l'Union lorsque cela est prévu dans les actes législatifs pertinents de l'Union;

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

[++] JO: prière d'insérer dans le texte le numéro de la décision figurant dans le document ST 8967/20.

c) soutenir, le cas échéant, la réalisation de l'objectif spécifique 4 "Compétences numériques avancées" énoncé à l'article 7 du règlement (UE) 2021/…[+], en coopération avec les pôles européens d'innovation numérique;

d) fournir des conseils d'experts dans les domaines de l'industrie, des technologies et de la recherche en matière de cybersécurité à la Commission lorsque celle-ci élabore les projets de programme de travail en vertu de l'article 13 de la décision (UE) 2021/…[++];

e) réaliser ou permettre le déploiement d'infrastructures TIC et faciliter l'acquisition de telles infrastructures, au bénéfice de la société, de l'industrie et du secteur public, à la demande des États membres, des milieux de la recherche et des opérateurs de services essentiels, grâce entre autres à des contributions des États membres et à des financements de l'Union pour des actions conjointes, conformément à la stratégie, au programme de travail pluriannuel et au programme de travail annuel;

f) sensibiliser à la mission du Centre de compétences et du Réseau ainsi qu'aux objectifs et aux tâches du Centre de compétences;

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

[++] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 8967/20.

g) sans préjudice de la nature civile des projets à financer au titre d'Horizon Europe, et conformément aux règlements (UE) 2021/…[+] et (UE) 2021/…[++], renforcer les synergies et la coordination entre les sphères civiles et de défense de la cybersécurité en facilitant l'échange:

i) de connaissances et d'informations en ce qui concerne les technologies et applications à double usage;

ii) de résultats, d'exigences et de bonnes pratiques; et

iii) d'informations en ce qui concerne les priorités des programmes pertinents de l'Union.

4. Le Centre de compétences exerce les tâches énoncées au paragraphe 1 en étroite coopération avec le Réseau.

5. Conformément à l'article 6 du règlement (UE) 2021/…[+] et sous réserve d'une convention de contribution au sens de l'article 2, point 18, du règlement financier, le Centre de compétences peut se voir confier la mise en œuvre des volets relatifs à la cybersécurité d'Horizon Europe qui ne sont pas cofinancées par les États membres, en particulier en ce qui concerne l'annexe I, pilier II, section 3.1.3, de la décision (UE) 2021/…[+++].

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

[++] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

[+++] JO: prière d'insérer dans le texte le numéro de la décision figurant dans le document ST 8967/20.

*Article 6*

*Désignation des centres nationaux de coordination*

1. Au plus tard le … [six mois après la date d'entrée en vigueur du présent règlement], chaque État membre désigne une entité qui remplit les critères fixés au paragraphe 5 pour agir comme son centre national de coordination aux fins du présent règlement. Chaque État membre notifie sans tarder la désignation de cette entité au conseil de direction. Cette entité peut être une entité déjà établie dans ledit État membre.

   Le délai énoncé au premier alinéa du présent paragraphe est prolongé de la période au cours de laquelle la Commission doit rendre l'avis visé au paragraphe 2.

2. À tout moment, un État membre peut demander à la Commission un avis quant à savoir si l'entité que l'État membre a désignée ou a l'intention de désigner pour agir comme son centre national de coordination, dispose de la capacité nécessaire pour gérer des fonds de manière à remplir la mission et les objectifs fixés dans le présent règlement. La Commission rend son avis à l'intention dudit État membre dans un délai de trois mois à compter de la demande de l'État membre.

3. Sur la base de la notification de la désignation d'une entité à laquelle a procédé un État membre conformément au paragraphe 1, le conseil de direction inscrit cette entité en tant que centre national de coordination au plus tard trois mois après la notification. Le Centre de compétences publie la liste des centres nationaux de coordination désignés.

4. Un État membre peut désigner à tout moment une nouvelle entité pour agir comme son centre national de coordination aux fins du présent règlement. Les paragraphes 1, 2 et 3 s'appliquent à la désignation de toute nouvelle entité.

5. Le centre national de coordination est une entité du secteur public ou une entité majoritairement détenue par l'État membre qui exerce des fonctions d'administration publique en vertu du droit national, y compris par voie de délégation, et ayant la capacité d'aider le Centre de compétences et le Réseau à remplir la mission qui leur est confiée à l'article 3 du présent règlement. Il possède ou a un accès à l'expertise dans les domaines des technologies et de la recherche en matière de cybersécurité. Il est en mesure d'assurer un dialogue et une coordination efficaces avec l'industrie, le secteur public, les milieux académiques et de la recherche et les citoyens, ainsi qu'avec les autorités désignées conformément à la directive (UE) 2016/1148.

6. À tout moment, un centre national de coordination peut demander à ce qu'il soit reconnu comme disposant de la capacité nécessaire pour gérer des fonds de manière à remplir la mission et les objectifs fixés dans le présent règlement, conformément aux règlements (UE) 2021/…[+] and (UE) 2021/…[++]. Dans un délai de trois mois à compter d'une telle demande, la Commission évalue si ce centre national de coordination dispose d'une telle capacité et rend une décision.

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

[++] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

Lorsque la Commission a rendu un avis favorable à l'intention d'un État membre conformément à la procédure prévue au paragraphe 2 du présent article, ledit avis est réputé constituer une décision reconnaissant que l'entité concernée dispose de la capacité nécessaire aux fins du présent paragraphe.

Au plus tard le ... [deux mois à compter de la date d'entrée en vigueur du présent règlement], après consultation du conseil de direction, la Commission émet des lignes directrices concernant l'évaluation visée au premier alinéa, précisant notamment les conditions de reconnaissance et les modalités d'élaboration des avis et des évaluations.

Avant de rendre l'avis visé au paragraphe 2 et la décision visée au premier alinéa du présent paragraphe, la Commission tient compte de toute information et documentation fournies par le centre national de coordination demandeur.

Toute décision de ne pas reconnaître qu'un centre national de coordination dispose de la capacité nécessaire pour gérer des fonds de manière à remplir la mission et les objectifs fixés dans le présent règlement est dûment motivée et précise les exigences que le centre national de coordination demandeur n'a pas encore remplies qui justifient la décision de refuser la reconnaissance. Tout centre national de coordination dont la demande de reconnaissance a été rejetée peut à tout moment présenter à nouveau sa demande en l'accompagnant d'informations complémentaires.

Les États membres informent la Commission en cas de changements concernant le centre national de coordination, tels que sa composition, sa forme juridique ou d'autres aspects pertinents ayant une incidence sur sa capacité à gérer les fonds de manière à remplir la mission et les objectifs fixés dans le présent règlement. Lorsqu'elle reçoit de telles informations, la Commission peut réexaminer sa décision d'accorder ou de refuser la reconnaissance du centre national de coordination comme disposant de la capacité nécessaires pour gérer des fonds en conséquence.

7. Le Réseau se compose de tous les centres nationaux de coordination dont la désignation a été notifiée au conseil de direction par les États membres.

*Article 7*

*Tâches des centres nationaux de coordination*

1. Les centres nationaux de coordination s'acquittent des tâches suivantes:

a) faire office de points de contact au niveau national pour la communauté afin d'aider le Centre de compétences à remplir sa mission et ses objectifs, en particulier, à coordonner la communauté au moyen d'une coordination entre ses membres dans leur État membre;

b) fournir une expertise et contribuer activement aux tâches stratégiques énoncées à l'article 5, paragraphe 2, en tenant compte des défis pertinents au niveau national et régional en matière de cybersécurité dans les différents secteurs;

c) promouvoir, encourager et favoriser la participation de la société civile, de l'industrie, en particulier des start-up et des PME, des milieux académiques et de la recherche ainsi que d'autres parties prenantes au niveau national à des projets transfrontières et à des actions en matière de cybersécurité financés par des programmes de l'Union pertinents;

d) fournir une assistance technique aux parties prenantes en les aidant dans leur phase de candidature pour les projets gérés par le Centre de compétences en rapport avec sa mission et ses objectifs, et dans le plein respect des règles de bonne gestion financière, notamment en matière de conflits d'intérêts;

e) s'efforcer de créer des synergies avec les activités pertinentes au niveau national, régional et local, telles que les politiques nationales en matière de recherche, de développement et d'innovation dans le domaine de la cybersécurité, en particulier les politiques énoncées dans les stratégies nationales de cybersécurité;

f) mettre en œuvre des actions spécifiques pour lesquelles des subventions ont été accordées par le Centre de compétences, y compris par la fourniture d'un soutien financier à des tiers conformément à l'article 204 du règlement financier, dans les conditions spécifiées dans les conventions de subvention concernées;

g) sans préjudice des compétences des États membres en matière d'éducation et en tenant compte des tâches pertinentes de l'ENISA, nouer un dialogue avec les autorités nationales en ce qui concerne d'éventuelles contributions à la promotion et à la diffusion de programmes éducatifs en matière de cybersécurité;

h) promouvoir et diffuser les résultats pertinents des travaux du Réseau, de la communauté et du Centre de compétences au niveau national, régional ou local;

i) évaluer les demandes présentées par des entités établies dans le même État membre que le centre national de coordination en vue de faire partie de la communauté;

j) prôner et faciliter la participation des entités concernées aux activités résultant du Centre de compétences, du Réseau et de la communauté, et assurer un suivi, le cas échéant, du niveau de participation à la recherche, au développement et au déploiement en matière de cybersécurité et du montant du soutien financier public qui y est accordé.

2. Aux fins du paragraphe 1, point f), du présent article, le soutien financier à des tiers peut être fourni sous l'une des formes de contribution de l'Union spécifiées à l'article 125 du règlement financier, y compris sous la forme de montants forfaitaires.

3. Sur la base d'une décision rendue conformément à l'article 6, paragraphe 6, du présent règlement, les centres nationaux de coordination peuvent recevoir une subvention de l'Union conformément à l'article 195, premier alinéa, point d), du règlement financier pour l'exécution des tâches définies dans le présent article.

4. Les centres nationaux de coordination coopèrent, le cas échéant, par l'intermédiaire du Réseau.

*Article 8*

*La communauté de compétences en matière de cybersécurité*

1. La communauté contribue à la mission du Centre de compétences et du Réseau telle qu'elle énoncée à l'article 3, et améliore, partage et diffuse l'expertise en matière de cybersécurité dans toute l'Union.

2. La communauté se compose, d'une part, de l'industrie, y compris de PME, d'institutions académiques et de recherche, d'autres associations concernées de la société civile ainsi que, selon les besoins, d'organismes européens de normalisation pertinents, d'entités publiques et d'autres entités traitant de questions de cybersécurité de nature opérationnelle et technique et, le cas échéant, de parties prenantes de secteurs qui ont un intérêt dans le domaine de la cybersécurité et sont confrontés à des défis en la matière. La communauté réunit les principales parties prenantes en ce qui concerne les capacités technologiques, industrielles, académiques et de recherche en matière de cybersécurité dans l'Union. Elle associe les centres nationaux de coordination, les pôles européens d'innovation numérique, le cas échéant, ainsi que les institutions, organes et organismes de l'Union disposant de l'expertise nécessaire, tels que l'ENISA.

3. Seules les entités établies dans les États membres sont enregistrées en tant que membres de la communauté. Elles démontrent qu'elles sont à même de contribuer à la mission et qu'elles possèdent une expertise en matière de cybersécurité dans au moins l'un des domaines suivants:

   a) milieux académiques, recherche ou innovation;

   b) développement industriel ou de produits;

c) formation et éducation;

d) sécurité de l'information ou opérations de réaction en cas d'incident;

e) éthique;

f) normalisation et spécifications formelles et techniques.

4. Le Centre de compétences enregistre les entités, à leur demande, en tant que membres de la communauté après une évaluation effectuée par le centre national de coordination de l'État membre dans lequel lesdites entités sont établies, destinée à confirmer que ces entités remplissent les critères énoncés au paragraphe 3 du présent article. Cette évaluation tient également compte de toute évaluation nationale pertinente fondée sur des motifs de sécurité effectuée par les autorités nationales compétentes. Cet enregistrement n'est pas limité dans le temps, mais peut être révoqué à tout moment par le Centre de compétences si le centre national de coordination concerné estime que l'entité en question ne remplit plus les critères énoncés au paragraphe 3 du présent article ou qu'elle relève de l'article 136 du règlement financier, ou pour des raisons de sécurité justifiées. Lorsque l'appartenance à la communauté est révoquée pour des raisons de sécurité, la décision de révocation est proportionnée et motivée. Les centres nationaux de coordination visent à parvenir à une représentation équilibrée des parties prenantes au sein de la communauté et encouragent activement la participation, en particulier des PME.

5. Les centres nationaux de coordination sont encouragés à coopérer par l'intermédiaire du Réseau afin d'harmoniser la manière dont ils appliquent les critères énoncés au paragraphe 3 ainsi que les procédures d'évaluation et d'enregistrement des entités visées au paragraphe 4.

6. Le Centre de compétences enregistre les institutions, organes et organismes de l'Union concernés en tant que membres de la communauté, après avoir procédé à une évaluation destinée à confirmer que l'institution, l'organe ou l'organisme de l'Union satisfait aux critères énoncés au paragraphe 3 du présent article. Cet enregistrement n'est pas limité dans le temps, mais peut être révoqué à tout moment par le Centre de compétences si ce dernier estime que l'institution, l'organe ou l'organisme de l'Union en question ne remplit plus les critères énoncés au paragraphe 3 du présent article ou relève de l'article 136 du règlement financier.

7. Les représentants des institutions, organes et organismes de l'Union peuvent participer aux travaux de la communauté.

8. Une entité enregistrée en tant que membre de la communauté désigne ses représentants afin d'assurer un dialogue efficace. Ces représentants possèdent une expertise dans le domaine de la recherche, des technologies ou de l'industrie en matière de cybersécurité. Les exigences peuvent être précisées davantage par le conseil de direction, sans limiter indûment les entités dans la désignation de leurs représentants.

9. La communauté fournit au directeur exécutif et au conseil de direction, par l'intermédiaire de ses groupes de travail, et en particulier du groupe consultatif stratégique, des conseils stratégiques sur la stratégie, le programme de travail annuel et le programme de travail pluriannuel conformément au règlement intérieur du conseil de direction.

*Article 9*

*Tâches des membres de la communauté*

Les membres de la communauté:

a) aident le Centre de compétences à remplir sa mission et ses objectifs et, à cette fin, travaillent en étroite collaboration avec le Centre de compétences et les centres nationaux de coordination;

b) le cas échéant, participent aux activités formelles ou informelles ainsi qu'aux groupes de travail visés à l'article 13, paragraphe 3, point n), pour exercer les activités spécifiques prévues dans le programme de travail annuel; et

c) le cas échéant, aident le Centre de compétences et les centres nationaux de coordination à promouvoir des projets spécifiques.

*Article 10*

*Coopération entre le Centre de compétences et les autres institutions, organes et organismes de l'Union, et les organisations internationales*

1. Aux fins d'assurer la cohérence et la complémentarité, tout en évitant la duplication des efforts, le Centre de compétences coopère avec les institutions, organes et organismes de l'Union concernés, dont l'ENISA, le Service européen pour l'action extérieure, la direction générale du Centre commun de recherche de la Commission, l'Agence exécutive européenne pour la recherche, l'Agence exécutive pour le Conseil européen de la recherche et l'agence exécutive européenne pour la santé et le numérique, instituées par la décision d'exécution (UE) 2021/173 de la Commission[1], les pôles européens d'innovation numérique concernés, le Centre européen de lutte contre la cybercriminalité au sein de l'Agence de l'Union européenne pour la coopération des services répressifs établie par le règlement (UE) 2016/794 du Parlement européen et du Conseil[2], l'Agence européenne de défense pour ce qui est des tâches énoncées à l'article 5 du présent règlement, et d'autres entités pertinentes de l'Union. Le Centre de compétences peut également coopérer avec des organisations internationales, s'il y a lieu.

---

1 Décision d'exécution (UE) 2021/173 de la Commission du 12 février 2021 instituant l'Agence exécutive européenne pour le climat, les infrastructures et l'environnement, l'Agence exécutive européenne pour la santé et le numérique, l'Agence exécutive européenne pour la recherche, l'Agence exécutive pour le Conseil européen de l'innovation et les PME, l'Agence exécutive du Conseil européen de la recherche et l'Agence exécutive européenne pour l'éducation et la culture, et abrogeant les décisions d'exécution 2013/801/UE, 2013/771/UE, 2013/778/UE, 2013/779/UE, 2013/776/UE et 2013/770/UE (JO L 50 du 15.2.2021, p. 9).

2 Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

2. La coopération visée au paragraphe 1 du présent article peut s'inscrire dans le cadre d'arrangements de travail. Ces arrangements sont soumis à l'approbation du conseil de direction. Tout partage d'informations classifiées s'effectue dans le cadre d'arrangements administratifs conclus conformément à l'article 36, paragraphe 3.

# CHAPITRE II
# ORGANISATION DU CENTRE DE COMPÉTENCES

*Article 11*

*Composition et structure*

1. Les membres du Centre de compétences sont l'Union, représentée par la Commission, et les États membres.

2. La structure du Centre de compétences assure la réalisation des objectifs énoncés à l'article 4 et des tâches définies à l'article 5 et comprend:

   a) un conseil de direction;

   b) un directeur exécutif;

   c) un groupe consultatif stratégique.

## SECTION I
## CONSEIL DE DIRECTION

*Article 12*

*Composition du conseil de direction*

1. Le conseil de direction se compose d'un représentant de chaque État membre et de deux représentants de la Commission qui agissent au nom de l'Union.

2. Chaque membre du conseil de direction dispose d'un suppléant. Ce suppléant représente le membre en cas d'absence du membre.

3. Les membres du conseil de direction nommés par les États membres et leurs suppléants font partie du personnel du secteur public dans leur État membre respectif et sont désignés sur la base de leurs connaissances dans les domaines de la recherche, des technologies et de l'industrie en matière de cybersécurité, de leur capacité à assurer la coordination des actions et prises de position avec leur centre national de coordination respectif, ou de leurs qualifications pertinentes en matière de gestion, d'administration et de budget. La Commission nomme ses membres du conseil de direction et leurs suppléants sur la base de leurs connaissances dans le domaine de la cybersécurité, des technologies, ou de leurs qualifications pertinentes en matière de gestion, d'administration et de budget, et de leur capacité à assurer la coordination, les synergies et, dans la mesure du possible, la mise en œuvre d'initiatives conjointes entre les différentes politiques sectorielles ou horizontales de l'Union touchant à la cybersécurité. La Commission et les États membres s'efforcent de limiter le roulement de leurs représentants au sein du conseil de direction, afin de garantir la continuité des travaux de celui-ci. La Commission et les États membres visent à atteindre une représentation équilibrée entre hommes et femmes au sein du conseil de direction.

4. Le mandat des membres du conseil de direction et de leurs suppléants a une durée de quatre ans. Ce mandat est renouvelable.

5. Les membres du conseil de direction veillent à la sauvegarde de la mission, des objectifs, de l'identité et de l'autonomie du Centre de compétences et à la cohérence entre cette mission et ces objectifs, en toute indépendance et transparence.

6. Le conseil de direction peut inviter des observateurs, y compris des représentants d'institutions, d'organes et organismes compétents de l'Union, et les membres de la communauté, à prendre part à ses réunions, s'il y a lieu.

7. Un représentant de l'ENISA est un observateur permanent au sein du conseil de direction. Le conseil de direction peut inviter un représentant du groupe consultatif stratégique à participer à ses réunions.

8. Le directeur exécutif participe aux réunions du conseil de direction mais ne dispose pas de droit de vote.

*Article 13*

*Tâches du conseil de direction*

1. Le conseil de direction a la responsabilité globale de l'orientation stratégique et du fonctionnement du Centre de compétences, supervise la mise en œuvre de ses activités et est responsable de toute tâche qui n'est pas spécifiquement assignée au directeur exécutif.

2. Le conseil de direction arrête son règlement intérieur. Ce règlement intérieur contient des procédures spécifiques visant à détecter et prévenir les conflits d'intérêts et à garantir la confidentialité de toutes les informations sensibles.

3. Le conseil de direction prend les décisions stratégiques nécessaires, en particulier concernant:

a) la mise au point et l'adoption de la stratégie, et le suivi de sa mise en œuvre;

b) en tenant compte des priorités stratégiques de l'Union et de la stratégie, l'adoption du programme de travail pluriannuel comportant les priorités communes dans les domaines de l'industrie, des technologies et de la recherche, qui s'appuient sur les besoins répertoriés par les États membres en coopération avec la communauté et qui nécessitent une concentration du soutien financier de l'Union, en ce compris les technologies et domaines essentiels pour le développement des capacités propres de l'Union en matière de cybersécurité;

c) l'adoption du programme de travail annuel pour la mise en œuvre des fonds de l'Union concernés, notamment les parties relatives à la cybersécurité d'Horizon Europe, dans la mesure où ils sont cofinancés de manière volontaire par les États membres, et du programme pour une Europe numérique, conformément au programme de travail pluriannuel du Centre de compétences et au processus de planification stratégique d'Horizon Europe;

d) l'adoption des comptes annuels, du bilan et du rapport d'activité annuel du Centre de compétences, sur la base d'une proposition du directeur exécutif;

e) l'adoption des règles financières spécifiques du Centre de compétences conformément à l'article 70 du règlement financier;

f) dans le cadre du programme de travail annuel, l'affectation de fonds du budget de l'Union à des thèmes pour des actions conjointes entre l'Union et des États membres;

g) dans le cadre du programme de travail annuel et conformément aux décisions visées au point f) du présent alinéa, ainsi que dans le respect des règlements (UE) 2021/…[+] et (UE) 2021/…[++], la description des actions conjointes visées au point f) du présent alinéa, et la définition des conditions applicables à leur mise en œuvre;

h) l'adoption d'une procédure de nomination du directeur exécutif, la nomination et la révocation du directeur exécutif, la prorogation de son mandat, la formulation d'orientations à l'intention du directeur exécutif et le suivi des du travail accompli par celui-ci;

i) l'adoption de lignes directrices pour l'évaluation et l'enregistrement des entités en tant que membres de la communauté;

j) l'adoption des arrangements de travail visés à l'article 10, paragraphe 2;

k) la nomination du comptable;

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

[++] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

l) l'adoption du budget annuel du Centre de compétences, y compris le tableau des effectifs correspondant indiquant le nombre de postes temporaires par groupe de fonctions et par grade, ainsi que le nombre d'agents contractuels et d'experts nationaux détachés, exprimés en équivalents temps plein;

m) l'adoption de règles de transparence applicables au Centre de compétences et de règles en matière de prévention et de gestion des conflits d'intérêts, y compris en ce qui concerne les membres du conseil de direction, conformément à l'article 42 du règlement délégué (UE) 2019/715;

n) la création de groupes de travail au sein de la communauté, en tenant compte, le cas échéant, des conseils fournis par le groupe consultatif stratégique;

o) la nomination des membres du groupe consultatif stratégique;

p) l'adoption de règles relatives au remboursement des frais pour les membres du groupe consultatif stratégique;

q) la mise en place d'un mécanisme de suivi afin de veiller à ce que la mise en œuvre des fonds respectifs gérés par le Centre de compétences ait lieu conformément à la stratégie, à la mission et au programme de travail pluriannuel ainsi qu'aux règles des programmes qui sont la source des financements concernés;

r) la garantie d'un dialogue régulier avec la communauté et l'établissement d'un mécanisme de coopération efficace avec celle-ci;

s) l'établissement de la politique de communication du Centre de compétences sur la base d'une recommandation du directeur exécutif;

t) s'il y a lieu, l'établissement des modalités d'application du statut des fonctionnaires de l'Union européenne et du régime applicable aux autres agents de l'Union, fixés par le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil[1] (ci-après dénommés "statut" et "régime"), conformément à l'article 30, paragraphe 3 du présent règlement;

u) s'il y a lieu, l'établissement des règles applicables au détachement d'experts nationaux auprès du Centre de compétences et à l'emploi de stagiaires, conformément à l'article 31, paragraphe 2;

v) l'adoption de règles de sécurité pour le Centre de compétences;

w) l'adoption d'une stratégie de lutte contre la fraude et la corruption qui est proportionnée aux risques de fraude et de corruption, ainsi que l'adoption de mesures globales, conformément à la législation applicable de l'Union, pour la protection des personnes qui signalent des violations du droit de l'Union, en tenant compte de l'analyse coût-bénéfice des mesures à mettre en œuvre;

[1] JO L 56 du 4.3.1968, p. 1.

x) si nécessaire, l'adoption de la méthode de calcul des contributions financières et en nature volontaires des États membres contributeurs conformément aux règlements (UE) 2021/…[+] et (UE) 2021/…[++], ou à tout autre législation applicable;

y) dans le cadre du programme de travail annuel et du programme de travail pluriannuel, la garantie d'une cohérence et de synergies avec les parties du programme pour une Europe numérique et d'Horizon Europe qui ne sont pas gérés par le Centre de compétences, ainsi qu'avec d'autres programmes de l'Union;

z) l'adoption du rapport annuel relatif à la mise en œuvre des objectifs et priorités stratégiques du Centre de compétences, en l'accompagnant, si nécessaire, d'une recommandation en vue d'une meilleure réalisation de ces objectifs et priorités.

Dans la mesure où le programme de travail annuel comprend des actions conjointes, il contient des informations sur les contributions volontaires des États membres aux actions conjointes. S'il y a lieu, des propositions, en particulier la proposition de programme de travail annuel, évaluent la nécessité d'appliquer les règles de sécurité énoncées à l'article 33 du présent règlement, y compris la procédure d'autoévaluation de la sécurité conformément à l'article 20 du règlement (UE) 2021/…[+].

4. En ce qui concerne les décisions énoncées au paragraphe 3, points a), b) et c), le directeur exécutif et le conseil de direction prennent en considération tout conseil et toute contribution stratégiques pertinents fournis par l'ENISA, conformément au règlement intérieur du conseil de direction.

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

[++] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

5. Il incombe au conseil de direction de veiller au suivi adéquat des recommandations figurant dans le rapport de mise en œuvre et l'évaluation visés à l'article 38, paragraphes 2 et 4.

*Article 14*

*Président et réunions du conseil de direction*

1. Le conseil de direction élit un président et un vice-président parmi ses membres, chacun pour une période de trois ans. Le mandat du président et du vice-président peut être prorogé une fois, sur décision du conseil de direction. Cependant, si le président ou le vice-président perd sa qualité de membre du conseil de direction à un moment quelconque de son mandat, ledit mandat expire automatiquement à ce moment. Le vice-président remplace le président d'office lorsque celui-ci n'est pas en mesure d'assumer ses fonctions. Le président participe au vote.

2. Le conseil de direction tient des réunions ordinaires au moins trois fois par an. Il peut tenir des réunions extraordinaires à la demande de la Commission, à la demande d'un tiers de tous ses membres, à la demande du président, ou à la demande du directeur exécutif dans l'accomplissement de ses tâches.

3. Le directeur exécutif prend part aux délibérations du conseil de direction, à moins que le conseil de direction n'en décide autrement, mais il n'a pas de droit de vote.

4. Le conseil de direction peut inviter d'autres personnes à assister à ses réunions en qualité d'observateurs, au cas par cas.

5. Le président peut inviter des représentants de la communauté à participer aux réunions du conseil de direction, mais ils n'ont pas de droit de vote.

6. Les membres du conseil de direction et leurs suppléants peuvent être assistés par des conseillers ou des experts lors des réunions, sous réserve du règlement intérieur du conseil de direction.

7. Le Centre de compétences assure le secrétariat du conseil de direction.

*Article 15*

*Règles de vote du conseil de direction*

1. Le conseil de direction adopte une approche consensuelle lors des discussions menées en son sein. Un vote est organisé si les membres du conseil de direction ne parviennent pas à un consensus.

2. Si le conseil de direction ne parvient pas à un consensus sur une question, il adopte ses décisions à la majorité d'au moins 75 % des votes de l'ensemble de ses membres, les représentants de la Commission constituant un seul membre à cette fin. Un membre absent du conseil de direction peut déléguer son droit de vote à son suppléant ou, en l'absence de celui-ci, à un autre membre. Aucun membre du conseil de direction ne peut représenter plus d'un autre membre.

3. Les décisions du conseil de direction sur les actions conjointes et leur gestion visées à l'article 13, paragraphe 3, points f) et g), sont prises comme suit:

a) les décisions visant à allouer des fonds du budget de l'Union à des actions conjointes conformément à l'article 13, paragraphe 3, point f), et les décisions visant à intégrer ces actions conjointes dans le programme de travail annuel sont prises conformément au paragraphe 2 du présent article;

b) les décisions ayant trait à la description des actions conjointes et déterminant les conditions applicables à leur mise en œuvre visées à l'article 13, paragraphe 3, point g), sont prises par les États membres participants et par la Commission, les droits de vote des membres étant cependant proportionnels à leurs contributions respectives à cette action conjointe, calculées conformément à la méthode adoptée en vertu de l'article 13, paragraphe 3, point x).

4. Pour les décisions prises en vertu de l'article 13, paragraphe 3, points b), c), d), e), f), k), l), p), q), t), u), w), x) et y), la Commission dispose de 26 % du total des voix au sein du conseil de direction.

5. Pour les décisions autres que celles visées au paragraphe 3, point b), et au paragraphe 4, chaque État membre et l'Union disposent d'une voix. Le vote de l'Union est exprimé conjointement par les deux représentants de la Commission.

6. Le président participe au vote.

## SECTION II
## DIRECTEUR EXÉCUTIF

*Article 16*

*Nomination, révocation et prorogation du mandat du directeur exécutif*

1. Le directeur exécutif est une personne ayant une expertise et jouissant d'une solide réputation dans les domaines d'activité du Centre de compétences.

2. Le directeur exécutif est engagé en tant qu'agent temporaire du Centre de compétences conformément à l'article 2, point a), du régime.

3. Le directeur exécutif est nommé par le conseil de direction à partir d'une liste de candidats proposés par la Commission à la suite d'une procédure de sélection ouverte, transparente et non discriminatoire.

4. Aux fins de la conclusion du contrat du directeur exécutif, le Centre de compétences est représenté par le président du conseil de direction.

5. Le mandat du directeur exécutif est de quatre ans. Avant la fin de cette période, la Commission procède à une évaluation qui tient compte de l'évaluation du travail accompli par le directeur exécutif et des tâches et défis futurs du Centre de compétences.

6. Le conseil de direction, statuant sur proposition de la Commission tenant compte de l'évaluation visée au paragraphe 5, peut proroger une fois le mandat du directeur exécutif, pour une durée n'excédant pas quatre ans.

7. Un directeur exécutif dont le mandat a été prorogé ne peut pas participer à une nouvelle procédure de sélection pour le même poste.

8. Le directeur exécutif n'est démis de ses fonctions que sur décision du conseil de direction, statuant sur proposition de la Commission ou d'au moins 50 % des États membres.

*Article 17*

*Tâches du directeur exécutif*

1. Le directeur exécutif est chargé du fonctionnement et de la gestion quotidienne du Centre de compétences, dont il est le représentant légal. Il rend compte au conseil de direction et exerce ses fonctions en toute indépendance, dans les limites des pouvoirs qui lui sont dévolus. Le directeur exécutif s'appuie sur le personnel du Centre de compétences.

2. Le directeur exécutif exerce au moins les tâches suivantes de manière indépendante:

   a) mettre en œuvre les décisions adoptées par le conseil de direction;

b) assister le conseil de direction dans ses travaux, assurer le secrétariat des réunions du conseil de direction et fournir toutes les informations nécessaires à l'exercice des fonctions du conseil de direction;

c) après consultation du conseil de direction et de la Commission, et prenant en compte la contribution des centres nationaux de coordination et de la communauté, préparer et soumettre au conseil de direction pour adoption la stratégie ainsi que, conformément à la stratégie, le projet de programme de travail pluriannuel et le projet de programme de travail annuel du Centre de compétences, y compris le contenu des appels à propositions, des appels à manifestation d'intérêt et des appels d'offres nécessaires à la mise en œuvre du programme de travail annuel et les estimations de dépenses correspondantes, comme le proposent les États membres et la Commission;

d) préparer et soumettre le projet de budget annuel pour adoption au conseil de direction, y compris le tableau des effectifs correspondant visé à l'article 13, paragraphe 3, point l), indiquant le nombre de postes temporaires dans chaque grade et chaque groupe de fonctions et le nombre d'agents contractuels et d'experts nationaux détachés, exprimés en équivalents temps plein;

e) mettre en œuvre le programme de travail annuel et le programme de travail pluriannuel et en rendre compte au conseil de direction;

f) élaborer le projet de rapport d'activité annuel du Centre de compétences, y compris les informations sur les dépenses correspondantes et la mise en œuvre de la stratégie et du programme de travail pluriannuel; si nécessaire, ce rapport s'accompagne de propositions visant à améliorer encore la réalisation des objectifs et priorités stratégiques ou à les reformuler;

g) assurer la mise en œuvre de procédures efficaces de suivi et d'évaluation du travail accompli par le Centre de compétences;

h) préparer un plan d'action donnant suite aux conclusions du rapport de mise en œuvre et de l'évaluation visés à l'article 38, paragraphes 2 et 4, et présenter des rapports tous les deux ans au Parlement européen et à la Commission sur les progrès accomplis;

i) préparer et conclure des accords avec les centres nationaux de coordination;

j) assumer la responsabilité des questions administratives, financières et de personnel, y compris de l'exécution du budget du Centre de compétences, en tenant dûment compte des conseils reçus de la fonction d'audit interne, conformément aux décisions visées à l'article 13, paragraphe 3, points e), l), t), u), v) et w);

k) approuver et gérer le lancement des appels à propositions, conformément au programme de travail annuel, et gérer les conventions et les décisions de subvention qui en découlent;

l) approuver la liste des actions sélectionnées en vue d'un financement sur la base d'un classement établi par un groupe d'experts indépendants;

m) approuver et gérer le lancement des appels d'offres, conformément au programme de travail annuel, et gérer les contrats en qui découlent;

n) approuver les offres sélectionnées en vue d'un financement;

o) soumettre les projets de comptes annuels et de bilan à la fonction d'audit interne concernée et, par la suite, au conseil de direction;

p) s'assurer de la bonne exécution des évaluations des risques et de la gestion des risques;

q) signer les conventions, décisions et contrats de subvention individuels;

r) signer les contrats de passation de marché;

s) préparer un plan d'action donnant suite aux conclusions des rapports d'audit internes ou externes, ainsi qu'aux enquêtes de l'Office européen de lutte antifraude (OLAF) institué par la décision 1999/352/CE, CECA, Euratom de la Commission[1], et présenter des rapports semestriels à la Commission et des rapports réguliers au conseil de direction sur les progrès accomplis;

t) préparer un projet de règles financières applicables au Centre de compétences;

[1] Décision 1999/352/CE, CECA, Euratom de la Commission du 28 avril 1999 instituant l'Office européen de lutte antifraude (OLAF) (JO L 136 du 31.5.1999, p. 20).

u) mettre en place un système de contrôle interne efficace et efficient et en assurer le fonctionnement, et signaler au conseil de direction tout changement important qui y serait apporté;

v) assurer une communication efficace avec les institutions de l'Union et rendre compte, lorsqu'il y est invité, au Parlement européen et au Conseil;

w) prendre toute autre mesure nécessaire pour évaluer la réalisation par le Centre de compétences de sa mission et de ses objectifs;

x) exécuter toutes les autres tâches qui lui sont confiées ou déléguées par le conseil de direction.

## SECTION III
## GROUPE CONSULTATIF STRATÉGIQUE

*Article 18*

*Composition du groupe consultatif stratégique*

1. Le groupe consultatif stratégique se compose de 20 membres au maximum. Les membres sont nommés par le conseil de direction, statuant sur proposition du directeur exécutif, parmi les représentants des membres de la communauté autres que les représentants des institutions, organes et organismes de l'Union. Seuls les représentants de membres qui ne sont pas contrôlés par un pays tiers ou par une entité établie dans un pays tiers sont éligibles. La nomination se fait selon une procédure ouverte, transparente et non discriminatoire. Le conseil de direction vise à ce que la composition du groupe consultatif stratégique représente la communauté de façon équilibrée en ce qui concerne les entités scientifiques, industrielles et de la société civile, les secteurs du côté de la demande et de l'offre, les grandes entreprises et les PME, ainsi qu'au regard de la provenance géographique et de l'équilibre entre les hommes et les femmes. Il vise également à atteindre un équilibre intrasectoriel, en ayant égard à la cohésion de l'Union et de tous les États membres dans le domaine de la recherche, de l'industrie et de la technologie en matière de cybersécurité. Le groupe consultatif stratégique est composé de manière à permettre un dialogue global, continu et permanent entre la communauté et le Centre de compétences.

2. Les membres du groupe consultatif stratégique possèdent une expertise en ce qui concerne la recherche, le développement industriel, l'offre, la mise en œuvre ou le déploiement de services ou produits professionnels en matière de cybersécurité. Les exigences relatives à cette expertise sont précisées davantage par le conseil de direction.

3. Les procédures relatives à la nomination des membres du groupe consultatif stratégique par le conseil de direction et au fonctionnement du groupe consultatif stratégique sont précisées dans le règlement intérieur du conseil de direction et sont rendues publiques.

4. La durée du mandat des membres du groupe consultatif stratégique est de deux ans. Ce mandat est renouvelable une fois.

5. Des représentants de la Commission et d'autres institutions, organes et organismes de l'Union, en particulier l'ENISA, peuvent être invités par le groupe consultatif stratégique à prendre part à ses travaux et à les appuyer. Le groupe consultatif stratégique peut inviter, le cas échéant, au cas par cas, d'autres représentants de la communauté en qualité d'observateurs, de conseillers ou d'experts, afin de prendre en compte la dynamique des évolutions dans le domaine de la cybersécurité. Les membres du conseil de direction peuvent participer en qualité d'observateurs aux réunions du groupe consultatif stratégique.

*Article 19*

*Fonctionnement du groupe consultatif stratégique*

1. Le groupe consultatif stratégique se réunit au moins trois fois par an.

2. Le groupe consultatif stratégique fournit des conseils au conseil de direction sur la création de groupes de travail au sein de la communauté, conformément à l'article 13, paragraphe 3, point n), sur des questions spécifiques pertinentes pour les travaux du Centre de compétences, lorsque ces questions sont en lien direct avec les tâches et domaines de compétence énoncés à l'article 20. Lorsque cela est nécessaire, ces groupes de travail font l'objet d'une coordination d'ensemble par un ou de plusieurs membres du groupe consultatif stratégique.

3. Le groupe consultatif stratégique élit son président à la majorité simple de ses membres.

4. Le secrétariat du groupe consultatif stratégique est assuré par le directeur exécutif et le personnel du Centre de compétences, en utilisant les ressources existantes, en tenant dûment compte de la charge de travail globale du Centre de compétences. Les ressources affectées au soutien du groupe consultatif stratégique sont indiquées dans le projet de budget annuel.

5. Le groupe consultatif stratégique adopte son règlement intérieur à la majorité simple de ses membres.

*Article 20*

*Tâches du groupe consultatif stratégique*

Le groupe consultatif stratégique conseille régulièrement le Centre de compétences sur l'exécution de ses activités et assure la communication avec la communauté et les autres parties prenantes concernées. Le groupe consultatif stratégique est également chargé des tâches suivantes:

a) en tenant compte des contributions de la communauté et des groupes de travail visés à l'article 13, paragraphe 3, point n), le cas échéant, fournir au directeur exécutif et au conseil de direction des conseils et des avis stratégiques, et les actualiser en permanence, en ce qui concerne la stratégie, le programme de travail annuel et le programme de travail pluriannuel, dans les délais fixés par le conseil de direction;

b) conseiller le conseil de direction quant à la création de groupes de travail au sein de la communauté conformément à l'article 13, paragraphe 3, point n), sur des questions spécifiques pertinentes pour les travaux du Centre de compétences;

c) sous réserve de l'approbation du conseil de direction, décider de la tenue de consultations publiques ouvertes à toutes les parties prenantes publiques et privées ayant un intérêt dans le domaine de la cybersécurité, afin de recueillir des contributions pour les conseils stratégiques visés au point a), et organiser de telles consultations.

# CHAPITRE III
# DISPOSITIONS FINANCIÈRES

*Article 21*

*Contributions financières de l'Union et des États membres*

1. Le Centre de compétences est financé par l'Union, tandis que les actions conjointes sont financées par l'Union et par des contributions volontaires des États membres.

2. Les coûts administratifs et les frais de fonctionnement des actions conjointes sont pris en charge par l'Union et par les États membres contribuant aux actions conjointes, conformément aux règlements (UE) 2021/…[+] et (UE) 2021/…[++].

3. La contribution de l'Union au Centre de compétences pour couvrir les coûts administratifs et les frais de fonctionnement comprend les éléments suivants:

   a) jusqu'à 1 649 566 000 EUR provenant du programme pour une Europe numérique, dont jusqu'à 32 000 000 EUR pour les coûts administratifs;

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

[++] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

b) un montant provenant d'Horizon Europe, y compris pour les coûts administratifs, pour les actions conjointes, lequel est égal au montant apporté à titre de contribution par les États membres en vertu du paragraphe 7 du présent article mais ne dépasse pas le montant déterminé dans le cadre du processus de planification stratégique d'Horizon Europe devant être mis en œuvre en vertu de l'article 6, paragraphe 6, du règlement (EU) 2021/…[+], dans le programme de travail pluriannuel ou dans le programme de travail annuel;

c) un montant provenant des autres programmes de l'Union pertinents, dans la mesure où cela est nécessaire à la mise en œuvre des tâches ou à la réalisation des objectifs du Centre de compétences, sous réserve des décisions prises conformément aux actes juridiques de l'Union établissant ces programmes.

4. La contribution maximale de l'Union est prélevée sur les crédits du budget général de l'Union alloués au programme pour une Europe numérique, au programme spécifique d'exécution d'Horizon Europe, établi par la décision (UE) 2021/…[++], et aux autres programmes et projets relevant du Centre de compétences ou du Réseau.

5. Le Centre de compétences met en œuvre les actions en matière de cybersécurité du programme pour une Europe numérique et d'Horizon Europe conformément à l'article 62, paragraphe 1, premier alinéa, point c) iv), du règlement financier.

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

[++] JO: prière d'insérer dans le texte le numéro de la décision figurant dans le document ST 8967/20.

6. Les contributions provenant de programmes de l'Union autres que ceux visés aux paragraphes 3 et 4 qui s'inscrivent dans le cadre du cofinancement de l'Union en faveur d'un programme mis en œuvre par l'un des États membres ne sont pas prises en compte dans le calcul de la contribution financière maximale de l'Union visée dans lesdits paragraphes.

7. Les États membres participent aux actions conjointes sur une base volontaire au moyen de contributions financières et/ou en nature volontaires. Si un État membre participe à une action conjointe, sa contribution financière couvre les coûts administratifs au prorata de sa contribution à ladite action conjointe. Les coûts administratifs des actions conjointes sont couverts par des contributions financières. Les frais de fonctionnement des actions conjointes peuvent être couverts par des contributions financières ou en nature, comme le prévoient Horizon Europe et le programme pour une Europe numérique. Les contributions de chaque État membre peuvent prendre la forme d'un soutien apporté par cet État membre dans le cadre d'une action conjointe à des bénéficiaires établis dans ledit État membre. Les contributions en nature des États membres se composent des coûts éligibles engagés par les centres nationaux de coordination et autres entités publiques lorsqu'ils participent à des projets financés au titre du présent règlement, déduction faite d'une éventuelle contribution de l'Union à ces coûts. Dans le cas de projets financés au titre d'Horizon Europe, les coûts éligibles sont calculés conformément à l'article 36 du règlement (UE) 2021/…[+]. Dans le cas de projets financés au titre du programme pour une Europe numérique, les coûts éligibles sont calculés conformément au règlement financier.

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

Le montant envisagé pour les contributions volontaires totales des États membres aux actions conjointes relevant d'Horizon Europe, y compris les contributions financières pour les coûts administratifs, est déterminé de façon à être pris en compte dans le processus de planification stratégique d'Horizon Europe devant être mis en œuvre en vertu de l'article 6, paragraphe 6, du règlement (UE) 2021/…[+], avec la participation du conseil de direction. En ce qui concerne les actions relevant du programme pour une Europe numérique, nonobstant l'article 15 du règlement (UE) 2021/…[++], les États membres peuvent apporter une contribution aux coûts du Centre de compétences qui sont cofinancés au titre du programme pour une Europe numérique, qui est inférieure aux montants spécifiés au paragraphe 3, point a), du présent article.

8. Le cofinancement national par les États membres d'actions soutenues par des programmes de l'Union autres qu'Horizon Europe et le programme pour une Europe numérique est considéré comme constituant des contributions nationales des États membres dans la mesure où ces contributions font partie d'actions conjointes et figurent dans le programme de travail du Centre de compétences.

9. Aux fins de l'évaluation des contributions visées au paragraphe 3 du présent article et à l'article 22, paragraphe 2, point b), les coûts sont déterminés conformément aux pratiques habituelles des États membres concernés en matière de comptabilité analytique, aux normes comptables applicables de l'État membre concerné, ainsi qu'aux normes comptables internationales et aux normes internationales d'information financière applicables. Les coûts sont certifiés par un auditeur externe indépendant désigné par l'État membre concerné. La méthode d'évaluation peut être vérifiée par le Centre de compétences en cas de doute quant à la certification.

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

[++] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

10. Si l'un des États membres se trouve en situation de défaut d'exécution de ses engagements en matière de contribution financière ou en nature aux actions conjointes, le directeur exécutif notifie cette situation par écrit à l'État membre concerné et fixe un délai raisonnable dans lequel il doit être remédié à cette situation. S'il n'est pas remédié à la situation dans ce délai, le directeur exécutif convoque une réunion du conseil de direction pour décider si le droit de vote de l'État membre participant défaillant doit être révoqué ou si d'autres mesures doivent être prises jusqu'à ce que cet État membre ait rempli ses obligations. Le droit de vote de l'État membre défaillant concernant les actions conjointes est suspendu jusqu'à ce qu'il soit remédié au défaut d'exécution de ses engagements.

11. La Commission peut supprimer la contribution financière de l'Union aux actions conjointes, réduire proportionnellement ou suspendre cette contribution si les États membres contributeurs ne contribuent pas ou n'apportent que partiellement ou tardivement les contributions visées au paragraphe 3, point b). La suppression, la réduction ou la suspension de la contribution financière de l'Union par la Commission est proportionnelle, quant au montant et à la durée, au défaut de contribution, ou à la contribution partielle ou tardive de l'État membre.

12. Les États membres contributeurs communiquent au conseil de direction, au plus tard le 31 janvier de chaque année, la valeur des contributions visées au paragraphe 7 pour l'action conjointe avec l'Union versées au cours de l'exercice précédent.

*Article 22*

*Coûts et ressources du Centre de compétences*

1. Les coûts administratifs du Centre de compétences sont en principe couverts par des contributions financières de l'Union versées sur une base annuelle. Des contributions financières supplémentaires sont versées par les États membres contributeurs proportionnellement à leurs contributions volontaires aux actions conjointes. Si une partie de la contribution aux coûts administratifs n'est pas utilisée, elle peut être mise à disposition pour couvrir les frais de fonctionnement du Centre de compétences.

2. Les frais de fonctionnement du Centre de compétences sont couverts par:

   a) la contribution financière de l'Union;

   b) les contributions volontaires, financières ou en nature, des États membres contributeurs en cas d'actions conjointes.

3. Les ressources du Centre de compétences inscrites à son budget proviennent des contributions suivantes:

   a) les contributions financières de l'Union aux frais de fonctionnement et aux coûts administratifs;

   b) les contributions financières volontaires des États membres contributeurs aux coûts administratifs en cas d'actions conjointes;

   c) les contributions financières volontaires des États membres contributeurs aux frais de fonctionnement en cas d'actions conjointes;

d) toute recette générée par le Centre de compétences;

e) toutes autres contributions financières, ressources ou recettes.

4. Les intérêts produits par les contributions versées au Centre de compétences par les États membres contributeurs sont considérés comme une recette du Centre de compétences.

5. Toutes les ressources du Centre de compétences et ses activités sont utilisées aux fins de la réalisation de ses objectifs.

6. Le Centre de compétences est propriétaire de tous les actifs qu'il génère ou qui lui sont transférés aux fins de la réalisation de ses objectifs. Sans préjudice des règles applicables du programme de financement concerné, il est décidé de la propriété des actifs générés ou acquis dans le cadre d'actions conjointes conformément à l'article 15, paragraphe 3, point b).

7. Sauf en cas de liquidation du Centre de compétences, l'excédent éventuel de recettes sur les dépenses restent la propriété du Centre de compétences et ne sont pas versés aux membres contributeurs du Centre de compétences.

8 Le Centre de compétences coopère étroitement avec les autres institutions, organes et organismes de l'Union, compte dûment tenu de leurs mandats respectifs et sans dupliquer les mécanismes de coopération existants, afin de profiter des synergies avec ces institutions, organes et organismes et, si c'est possible et approprié, de réduire les coûts administratifs.

*Article 23*

*Engagements financiers*

Les engagements financiers du Centre de compétences n'excèdent pas le montant des ressources financières disponibles ou inscrites à son budget par ses membres.

*Article 24*

*Exercice budgétaire*

L'exercice budgétaire commence le 1er janvier et s'achève le 31 décembre.

*Article 25*

*Établissement du budget*

1. Chaque année, le directeur exécutif établit un projet d'état prévisionnel des recettes et des dépenses du Centre de compétences pour l'exercice budgétaire suivant et le transmet au conseil de direction avec le projet de tableau des effectifs visé à l'article 13, paragraphe 3, point l). Les recettes et les dépenses sont en équilibre. Les dépenses du Centre de compétences comprennent les dépenses de personnel, d'administration, d'infrastructure et de fonctionnement. Les dépenses administratives sont réduites au minimum, y compris au moyen d'un redéploiement de personnel ou de postes.

2. Le conseil de direction établit chaque année, sur la base du projet d'état prévisionnel des recettes et des dépenses visé au paragraphe 1, un état prévisionnel des recettes et des dépenses du Centre de compétences pour l'exercice budgétaire suivant.

3. Le conseil de direction transmet à la Commission, au plus tard le 31 janvier de chaque année, l'état prévisionnel visé au paragraphe 2 du présent article, qui fait partie du projet de document de programmation unique visé à l'article 32, paragraphe 1, du règlement délégué (UE) 2019/715.

4. Sur la base de l'état prévisionnel visé au paragraphe 2 du présent article, la Commission inscrit dans le projet de budget de l'Union les prévisions qu'elle estime nécessaires en ce qui concerne le tableau des effectifs visé à l'article 13, paragraphe 3, point l), du présent règlement, et le montant de la contribution à la charge du budget général, et le soumet au Parlement européen et au Conseil conformément aux articles 313 et 314 du traité sur le fonctionnement de l'Union européenne.

5. Le Parlement européen et le Conseil autorisent les crédits pour la contribution destinée au Centre de compétences.

6. Le Parlement européen et le Conseil adoptent le tableau des effectifs visé à l'article 13, paragraphe 3, point l).

7. En même temps que le programme de travail annuel et le programme de travail pluriannuel, le conseil de direction adopte le budget du Centre de compétences. Ce budget devient définitif après l'adoption définitive du budget général de l'Union. S'il y a lieu, le conseil de direction adapte le budget et le programme de travail annuel du Centre de compétences en fonction du budget général de l'Union.

*Article 26*

*Présentation des comptes du Centre de compétences et décharge*

La présentation des comptes provisoires et définitifs du Centre de compétences ainsi que la décharge respectent les règles et le calendrier du règlement financier et des règles financières du Centre de compétences.

*Article 27*

*Rapports opérationnels et financiers*

1. Le directeur exécutif présente chaque année au conseil de direction un rapport sur l'exécution de ses tâches conformément aux règles financières du Centre de compétences.

2. Dans un délai de deux mois à compter de la fin de chaque exercice budgétaire, le directeur exécutif soumet au conseil de direction, pour approbation, un rapport d'activité annuel sur les progrès accomplis par le Centre de compétences au cours de l'année civile précédente, en ce qui concerne notamment le programme de travail annuel adopté pour l'année en question et la réalisation de ses objectifs et priorités stratégiques. Ce rapport comprend des informations sur les points suivants:

a) les actions opérationnelles qui ont été réalisées, ainsi que les dépenses correspondantes;

b) les actions proposées, avec une ventilation par type de participants, y compris les PME, et par État membre;

c) les actions sélectionnées en vue d'un financement, avec une ventilation par type de participants, y compris les PME, et par État membre, indiquant les contributions versées par le Centre de compétences aux différents participants et aux différentes actions;

d) la réalisation de la mission et des objectifs fixés dans le présent règlement et des propositions concernant d'autres initiatives nécessaires pour remplir ladite mission et lesdits objectifs;

e) la cohérence des tâches de mise en œuvre avec la stratégie et le programme de travail pluriannuel.

3. Une fois approuvé par le conseil de direction, le rapport d'activité annuel est rendu public.

*Article 28*

*Règles financières*

Le Centre de compétences adopte ses règles financières spécifiques conformément à l'article 70 du règlement financier.

*Article 29*

*Protection des intérêts financiers de l'Union*

1. Le Centre de compétences prend les mesures appropriées pour garantir la protection des intérêts financiers de l'Union lors de la mise en œuvre d'actions financées au titre du présent règlement, par l'application de mesures préventives contre la fraude, la corruption et toute autre activité illégale, par des contrôles réguliers et efficaces et, si des irrégularités sont décelées, par le recouvrement des montants indûment versés et, s'il y a lieu, par des sanctions administratives effectives, proportionnées et dissuasives.

2. Le Centre de compétences accorde au personnel de la Commission et aux autres personnes autorisées par celle-ci, ainsi qu'à la Cour des comptes, l'accès aux sites et locaux du Centre de compétences, ainsi qu'à toutes les informations, y compris sous forme électronique, qui sont nécessaires pour mener leurs audits.

3. L'OLAF peut mener des enquêtes, y compris des contrôles et vérifications sur place, conformément aux dispositions et procédures prévues par le règlement (Euratom, CE) n° 2185/96 du Conseil[1] et le règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil[2] en vue d'établir l'existence éventuelle d'une fraude, d'un acte de corruption ou de toute autre activité illégale portant atteinte aux intérêts financiers de l'Union, dans le cadre d'une convention de subvention ou d'un contrat bénéficiant d'un financement direct ou indirect au titre du présent règlement.

4. Sans préjudice des paragraphes 1, 2 et 3, les contrats et les conventions de subvention résultant de la mise en œuvre du présent règlement contiennent des dispositions habilitant expressément la Commission, le Centre de compétences, la Cour des comptes et l'OLAF à procéder à ces audits et enquêtes conformément à leurs compétences respectives. Lorsque la mise en œuvre d'une action est externalisée ou sous-traitée, en tout ou partie, ou lorsqu'elle nécessite l'attribution d'un marché ou un soutien financier à un tiers, le contrat ou la convention de subvention prévoit l'obligation, pour le contractant ou le bénéficiaire, d'imposer à tout tiers concerné l'acceptation explicite desdits pouvoirs de la Commission, du Centre de compétences, de la Cour des comptes et de l'OLAF.

---

[1] Règlement (Euratom, CE) n° 2185/96 du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités (JO L 292 du 15.11.1996, p. 2).

[2] Règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil du 11 septembre 2013 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) et abrogeant le règlement (CE) n° 1073/1999 du Parlement européen et du Conseil et le règlement (Euratom) n° 1074/1999 du Conseil (JO L 248 du 18.9.2013, p. 1).

# CHAPITRE IV
# PERSONNEL DU CENTRE DE COMPÉTENCES

*Article 30*

*Personnel*

1. Le statut et le régime, ainsi que les règles adoptées conjointement par les institutions de l'Union aux fins de l'application du statut et du régime, s'appliquent au personnel du Centre de compétences.

2. Le conseil de direction exerce, à l'égard du personnel du Centre de compétences, les pouvoirs conférés par le statut à l'autorité investie du pouvoir de nomination et les pouvoirs conférés par le régime à l'autorité habilitée à conclure les contrats d'engagement (ci-après dénommés "pouvoirs de l'autorité investie du pouvoir de nomination").

3. Le conseil de direction adopte, conformément à l'article 110 du statut, une décision fondée sur l'article 2, paragraphe 1, du statut et sur l'article 6 du régime, déléguant au directeur exécutif les pouvoirs correspondants de l'autorité investie du pouvoir de nomination et définissant les conditions dans lesquelles cette délégation peut être suspendue. Le directeur exécutif est autorisé à subdéléguer ces pouvoirs.

4. Lorsque des circonstances exceptionnelles l'exigent, le conseil de direction peut, par la voie d'une décision, suspendre temporairement la délégation des pouvoirs de l'autorité investie du pouvoir de nomination au directeur exécutif et toute subdélégation de ces pouvoirs par ce dernier. Dans ce cas, le conseil de direction exerce lui-même les pouvoirs de l'autorité investie du pouvoir de nomination ou les délègue à l'un de ses membres ou à un membre du personnel du Centre de compétences autre que le directeur exécutif.

5. Le conseil de direction arrête les règles d'exécution du statut et du régime conformément à l'article 110 du statut.

6. Les ressources en personnel sont déterminés par le tableau des effectifs visé à l'article 13, paragraphe 3, point l), lequel indique le nombre d'emplois temporaires par groupe de fonctions et par grade et le nombre d'agents contractuels exprimés en équivalents temps plein, conformément au budget annuel du Centre de compétences.

7. Les besoins en ressources humaines du Centre de compétences sont rencontrés en premier lieu par un redéploiement de membres du personnel ou de postes des institutions, organes et organismes de l'Union, et par des ressources humaines supplémentaires par voie de recrutement. Le personnel du Centre de compétences peut se composer d'agents temporaires et d'agents contractuels.

8. Toutes les dépenses de personnel sont à la charge du Centre de compétences.

*Article 31*

*Experts nationaux détachés et autre personnel*

1. Le Centre de compétences peut recourir à des experts nationaux détachés ou à d'autres membres du personnel qui ne sont pas employés par le Centre de compétences.

2. Le conseil de direction adopte une décision fixant les règles applicables au détachement d'experts nationaux auprès du Centre de compétences, en accord avec la Commission.

*Article 32*

*Privilèges et immunités*

Le protocole n° 7 sur les privilèges et immunités de l'Union européenne annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne s'applique au Centre de compétences et à son personnel.

# CHAPITRE V
# DISPOSITIONS COMMUNES

*Article 33*

*Règles de sécurité*

1. L'article 12 du règlement (UE) 2021/…[+] s'applique à la participation à toutes les actions financées par le Centre de compétences.

2. Les règles de sécurité spécifiques suivantes s'appliquent aux actions financées au titre d'Horizon Europe:

   a) aux fins de l'article 38, paragraphe 1, du règlement (UE) 2021/…[++], lorsque le programme de travail annuel le prévoit, l'octroi de licences non exclusives peut être limité à des tiers qui sont établis ou réputés établis dans un État membre et qui sont contrôlés par ledit État membre ou par des ressortissants de cet État membre;

   b) aux fins de l'article 40, paragraphe 4, premier alinéa, point b), du règlement (UE) 2021/…[++], le transfert ou l'octroi d'une licence à une entité juridique établie dans un pays associé ou établie dans l'Union, mais contrôlée depuis des pays tiers, constituent également des motifs d'objection aux transferts de propriété des résultats ou à l'octroi d'une licence exclusive en ce qui concerne les résultats;

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

[++] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

c) aux fins de l'article 41, paragraphe 7, premier alinéa, point a), du règlement (UE) 2021/…[+], lorsque le programme de travail annuel le prévoit, l'octroi de droits d'accès, tels qu'ils sont définis à l'article 2, point 9), dudit règlement, peut être réservé uniquement à une entité juridique qui est établie ou réputée établie dans un État membre et qui est contrôlée par ledit État membre ou par des ressortissants de cet État membre.

*Article 34*

*Transparence*

1. Le Centre de compétences exerce ses activités dans la plus grande transparence.

2. Le Centre de compétences veille à ce que le public et toute partie intéressée reçoivent, en temps utile, des informations suffisantes, objectives, fiables et facilement accessibles, notamment en ce qui concerne les résultats de ses travaux. Il rend également publiques les déclarations d'intérêt faites conformément à l'article 43. Ces exigences s'appliquent également aux centres nationaux de coordination, à la communauté et au groupe consultatif stratégique conformément au droit applicable.

3. Le conseil de direction, statuant sur proposition du directeur exécutif, peut autoriser des parties intéressées à participer en tant qu'observateurs à certaines activités du Centre de compétences.

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

4. Le Centre de compétences fixe dans le règlement intérieur de son conseil de direction et dans le règlement intérieur du groupe consultatif stratégique les modalités pratiques de mise en œuvre des règles de transparence visées aux paragraphes 1 et 2 du présent article. En ce qui concerne les actions financées au titre d'Horizon Europe, ces règles et modalités tiennent compte du règlement (UE) 2021/…[+].

*Article 35*

*Équilibre entre les hommes et les femmes*

Dans le cadre de la mise en œuvre du présent règlement, lorsqu'ils désignent des candidats ou proposent des représentants, la Commission, les États membres et les autres parties prenantes institutionnelles et privées choisissent des représentants parmi plusieurs candidats, dans la mesure du possible, et dans le but d'assurer un équilibre entre les hommes et les femmes.

*Article 36*

*Règles de sécurité en matière de protection des informations classifiées et des informations sensibles non classifiées*

1. Après approbation par la Commission, le conseil de direction adopte les règles de sécurité du Centre de compétences. Ces règles de sécurité appliquent les principes et les règles de sécurité fixés dans les décisions (UE, Euratom) 2015/443[1] et 2015/444[2] de la Commission.

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

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

[2] Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53).

2. Les membres du conseil de direction, le directeur exécutif, les experts externes participant aux groupes de travail ad hoc et les membres du personnel du Centre de compétences se conforment aux exigences de confidentialité prévues à l'article 339 du traité sur le fonctionnement de l'Union européenne, même après la cessation de leurs fonctions.

3. Le Centre de compétences peut prendre les mesures nécessaires pour faciliter l'échange d'informations utiles à l'exécution de ses tâches, avec la Commission et les États membres et, s'il y a lieu, les institutions, organes et organismes de l'Union concernés. Tout arrangement administratif conclu à cette fin concernant le partage d'informations classifiées de l'Union européenne (ICUE) ou, en l'absence d'un tel arrangement, toute communication ad hoc exceptionnelle d'ICUE sont préalablement approuvés par la Commission.

*Article 37*

*Accès aux documents*

1. Le règlement (CE) n° 1049/2001 s'applique aux documents détenus par le Centre de compétences.

2. Le conseil de direction adopte les modalités de mise en œuvre du règlement (CE) n° 1049/2001 au plus tard le … [six mois après la date d'entrée en vigueur du présent règlement].

3. Les décisions prises par le Centre de compétences en vertu de l'article 8 du règlement (CE) n° 1049/2001 peuvent faire l'objet d'une plainte auprès du médiateur au titre de l'article 228 du traité sur le fonctionnement de l'Union européenne ou d'un recours devant la Cour de justice de l'Union européenne au titre de l'article 263 du traité sur le fonctionnement de l'Union européenne.

*Article 38*

*Suivi, évaluation et réexamen*

1. Le Centre de compétences veille à ce que ses activités, y compris celles qui sont gérées par l'intermédiaire des centres nationaux de coordination et du Réseau, fassent l'objet d'un suivi continu et systématique et d'une évaluation périodique. Le Centre de compétences veille à ce que les données nécessaires au suivi de la mise en œuvre et des résultats des programmes de financement de l'Union visés à l'article 4, paragraphe 3, point b), soient collectées de manière efficace et effective et en temps utile, et impose aux destinataires de fonds de l'Union et aux États membres des obligations de déclaration proportionnées. Les conclusions de ladite évaluation sont rendues publiques.

2. Dès qu'elle dispose d'informations suffisantes sur la mise en œuvre du présent règlement, et en tout état de cause au plus tard 30 mois après la date prévue à l'article 46, paragraphe 4, la Commission élabore un rapport de mise en œuvre sur les activités du Centre de compétences, en prenant en compte les contributions préliminaires du conseil de direction, des centres nationaux de coordination et de la communauté. La Commission soumet ce rapport de mise en œuvre au Parlement européen et au Conseil au plus tard le 30 juin 2024. Le Centre de compétences et les États membres fournissent à la Commission les informations nécessaires à l'élaboration de ce rapport.

3. Le rapport de mise en œuvre visé au paragraphe 2 comporte une évaluation:

a) des capacités de travail du Centre de compétences au regard de sa mission, de ses objectifs, de son mandat et de ses tâches, ainsi que de la coopération et de la coordination avec les parties prenantes, en particulier les centres nationaux de coordination, la communauté et l'ENISA;

b) des résultats obtenus par le Centre de compétences, eu égard à sa mission, à ses objectifs, à son mandat et à ses tâches, et en particulier de l'efficacité du Centre de compétences en ce qui concerne la coordination des fonds de l'Union et la mise en commun de l'expertise;

c) de la cohérence des tâches de mise en œuvre avec la stratégie et le programme de travail pluriannuel;

d) de la coordination et de la coopération du Centre de compétences avec le comité du programme d'Horizon Europe et le comité du programme pour une Europe numérique, en particulier en vue d'accroître la cohérence et les synergies avec le programme de travail annuel, le programme de travail pluriannuel, la stratégie, Horizon Europe et le programme pour une Europe numérique;

e) des actions conjointes.

4. Après avoir présenté le rapport de mise en œuvre visé au paragraphe 2 du présent article, la Commission procède à une évaluation du Centre de compétences, en prenant en compte les contributions préliminaires du conseil de direction, des centres nationaux de coordination et de la communauté. Cette évaluation renvoie, au besoin, aux évaluations visées au paragraphe 3 du présent article, ou les actualise, et est réalisée avant l'expiration de la période indiquée à l'article 47, paragraphe 1, de manière à déterminer en temps utile s'il convient de prolonger la durée du mandat du Centre de compétences au-delà de cette période. Cette évaluation analyse les aspects juridiques et administratifs du mandat du Centre de compétences et les possibilités de créer des synergies et d'éviter la fragmentation avec d'autres institutions, organes et organismes de l'Union.

   Si la Commission estime que le maintien du Centre de compétences est justifié au regard de sa mission, de ses objectifs, de son mandat et de ses tâches, elle peut présenter une proposition législative visant à prolonger la durée du mandat du Centre de compétences énoncée à l'article 47.

5. Sur la base des conclusions du rapport de mise en œuvre visé au paragraphe 2, la Commission peut prendre des mesures appropriées.

6. Le suivi, l'évaluation, la suppression progressive et le renouvellement de la contribution au titre d'Horizon Europe ont lieu conformément aux articles 10, 50 et 52 du règlement (UE) 2021/…[+], et aux modalités d'exécution convenues.

7. Le suivi et l'évaluation de la contribution au titre du programme pour une Europe numérique ainsi que les rapports établis à ce sujet sont réalisés conformément aux articles 24 et 25 du règlement (UE) 2021/…[++].

8. En cas de liquidation du Centre de compétences, la Commission procède à une évaluation finale du Centre de compétences dans les six mois à compter de sa liquidation et, en tout état de cause, au plus tard deux ans après le déclenchement de la procédure de liquidation visée à l'article 47. Les résultats de cette évaluation finale sont présentés au Parlement européen et au Conseil.

*Article 39*

*Personnalité juridique du Centre de compétences*

1. Le Centre de compétences est doté de la personnalité juridique.

---

[+] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 7064/20.

[++] JO: prière d'insérer dans le texte le numéro du règlement figurant dans le document ST 6789/20.

2. Dans chaque État membre, le Centre de compétences jouit de la capacité juridique la plus large reconnue aux personnes morales par le droit de cet État. Il peut notamment acquérir ou aliéner des biens mobiliers et immobiliers et ester en justice.

*Article 40*

*Responsabilité du Centre de compétences*

1. La responsabilité contractuelle du Centre de compétences est régie par le droit applicable à la convention, à la décision ou au contrat en question.

2. En matière de responsabilité non contractuelle, le Centre de compétences doit réparer les dommages causés par son personnel dans l'exercice de ses fonctions, conformément aux principes généraux communs aux législations des États membres.

3. Tout paiement effectué par le Centre de compétences relativement à la responsabilité visée aux paragraphes 1 et 2, ainsi que les frais et dépenses exposés en relation avec celle-ci, sont considérés comme des dépenses du Centre de compétences et sont couverts par ses ressources.

4. Le Centre de compétences répond seul de ses obligations.

*Article 41*

*Compétence de la Cour de justice de l'Union européenne et droit applicable*

1. La Cour de justice de l'Union européenne est compétente:

   a) pour statuer en vertu de clauses compromissoires contenues dans les décisions adoptées par le Centre de compétences ou dans les conventions ou contrats conclus par celui-ci;

   b) pour les litiges concernant la réparation des dommages causés par le personnel du Centre de compétences dans l'exercice de ses fonctions;

   c) pour tout litige entre le Centre de compétences et son personnel dans les limites et dans les conditions prévues par le statut.

2. Le droit de l'État membre où se trouve le siège du Centre de compétences est applicable à toute matière non couverte par le présent règlement ou par d'autres actes juridiques de l'Union.

*Article 42*

*Responsabilité de l'Union et des États membres et assurances*

1. La responsabilité financière de l'Union et des États membres en ce qui concerne les dettes du Centre de compétences est limitée à la contribution qu'ils ont déjà versée pour couvrir les coûts administratifs.

2. Le Centre de compétences contracte et maintient en vigueur les assurances nécessaires.

*Article 43*

*Conflits d'intérêts*

Le conseil de direction adopte des règles en matière de prévention, de détection et de résolution des conflits d'intérêts qui s'appliquent à ses membres, à ses organes et à son personnel, y compris au directeur exécutif. Ces règles contiennent des dispositions visant à éviter tout conflit d'intérêts impliquant des représentants des membres siégeant au conseil de direction ainsi qu'au groupe consultatif stratégique, conformément au règlement financier, y compris des dispositions relatives à d'éventuelles déclarations d'intérêts. Les centres nationaux de coordination sont soumis au droit national en ce qui concerne les conflits d'intérêts.

*Article 44*

*Protection des données à caractère personnel*

1. Les opérations de traitement de données à caractère personnel effectuées par le Centre de compétences sont soumises au règlement (UE) 2018/1725.

2. Le conseil de direction adopte les dispositions d'application visées à l'article 45, paragraphe 3, du règlement (UE) 2018/1725. Le conseil de direction peut adopter des mesures supplémentaires nécessaires à l'application dudit règlement par le Centre de compétences.

*Article 45*

*Soutien apporté par l'État membre d'accueil*

Un accord administratif peut être conclu entre le Centre de compétences et l'État membre d'accueil où se trouve son siège en ce qui concerne les privilèges et immunités et les autres formes de soutien à fournir par cet État membre au Centre de compétences.

# CHAPITRE VI
# DISPOSITIONS FINALES

*Article 46*

*Mesures initiales*

1. La Commission est chargée de la création et de l'exploitation initiale du Centre de compétences jusqu'à ce que celui-ci dispose de la capacité opérationnelle pour exécuter son propre budget. La Commission prend, conformément au droit de l'Union, toutes les mesures nécessaires avec la participation des organes compétents du Centre de compétences.

2. Aux fins du paragraphe 1 du présent article, la Commission peut désigner un directeur exécutif par intérim jusqu'à ce que le directeur exécutif prenne ses fonctions après avoir été nommé par le conseil de direction conformément à l'article 16. Le directeur exécutif par intérim exerce les fonctions du directeur exécutif et peut être assisté par un nombre limité de membres du personnel de la Commission. La Commission peut détacher, à titre provisoire, un nombre limité de membres de son personnel au Centre de compétences.

3. Le directeur exécutif par intérim peut autoriser tous les paiements couverts par les crédits prévus au budget annuel du Centre de compétences après que celui-ci a été adopté par le conseil de direction, et peut conclure des conventions et des contrats, y compris des contrats d'engagement, et adopter des décisions, après l'adoption du tableau des effectifs visé à l'article 13, paragraphe 3, point l).

4. Le directeur exécutif par intérim détermine, d'un commun accord avec le directeur exécutif et sous réserve de l'approbation du conseil de direction, la date à partir de laquelle le Centre de compétences aura la capacité d'exécuter son propre budget. À compter de cette date, la Commission s'abstient de procéder à des engagements et d'exécuter des paiements pour les activités du Centre de compétences.

*Article 47*

*Durée*

1. Le Centre de compétences est établi pour la période du … [date d'entrée en vigueur du présent règlement] au 31 décembre 2029.

2. Sauf prorogation du mandat du Centre de compétences conformément à l'article 38, paragraphe 4, la procédure de liquidation est déclenchée automatiquement au terme de la période visée au paragraphe 1 du présent article.

3. Pour les besoins de la procédure de liquidation du Centre de compétences, le conseil de direction nomme un ou plusieurs liquidateurs, qui se conforment aux décisions du conseil de direction.

4. Lors de la liquidation du Centre de compétences, ses actifs sont utilisés pour couvrir ses dettes et les dépenses liées à sa liquidation. Tout excédent est réparti entre l'Union et les États membres contributeurs, au prorata de leur contribution financière au Centre de compétences. Tout excédent de ce type attribué à l'Union est reversé au budget de l'Union.

*Article 48*

*Entrée en vigueur*

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

| | |
|---|---|
| *Par le Parlement européen* | *Par le Conseil* |
| *Le président* | *Le président* |