Journal officiel
de l'Union européenne

FR
Série L

2025/295

13.2.2025

RÈGLEMENT DÉLÉGUÉ (UE) 2025/295 DE LA COMMISSION

du 24 octobre 2024

complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'harmonisation des conditions permettant l'exercice des activités de supervision

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 ([1]), et notamment son article 41, paragraphe 2, deuxième alinéa,

considérant ce qui suit:

(1) Le cadre sur la résilience opérationnelle numérique du secteur financier établi par le règlement (UE) 2022/2554 introduit un cadre de supervision de l'Union pour les prestataires tiers de services de technologies de l'information et de la communication (TIC) du secteur financier désignés comme critiques conformément à l'article 31 dudit règlement.

(2) Un prestataire tiers de services TIC qui décide de présenter une demande de désignation volontaire en tant que prestataire critique devrait fournir à l'autorité européenne de surveillance (AES) destinataire toutes les informations nécessaires afin de démontrer son caractère critique, conformément aux principes et critères énoncés dans le règlement (UE) 2022/2554. C'est pourquoi les informations à inclure dans la demande de désignation volontaire devraient être suffisamment détaillées et complètes pour permettre une évaluation claire et complète du caractère critique au titre de l'article 31, paragraphe 11, dudit règlement. L'AES compétente devrait rejeter toute demande incomplète et demander les informations manquantes.

(3) L'identification juridique des prestataires tiers de services TIC relevant du champ d'application de la présente norme technique de réglementation devrait être alignée sur le code d'identification défini dans le règlement d'exécution de la Commission adopté conformément à l'article 28, paragraphe 9, du règlement (UE) 2022/2554.

(4) Dans le cadre du suivi des recommandations formulées par le superviseur principal à l'intention des prestataires tiers critiques de services TIC, ce dernier devrait contrôler le respect des recommandations par lesdits prestataires. Afin d'assurer un suivi efficient et efficace des mesures qui ont été prises ou des solutions qui ont été mises en œuvre par les prestataires tiers critiques de services TIC en ce qui concerne ces recommandations, le superviseur principal devrait pouvoir demander les rapports visés à l'article 35, paragraphe 1, point c), du règlement (UE) 2022/2554, qui devraient être considérés comme des rapports d'avancement intermédiaires et des rapports finaux.

(5) Aux fins de l'évaluation visée à l'article 42, paragraphe 1, du règlement (UE) 2022/2554, selon laquelle le superviseur principal est tenu d'évaluer si les explications fournies par le prestataire tiers critique de services TIC sont suffisantes, la notification au superviseur principal par le prestataire tiers critique de services TIC de son intention de suivre les recommandations reçues devrait être complétée par une description des actions et des mesures qui ont été prises pour atténuer les risques exposés dans les recommandations, ainsi que de leurs délais respectifs. Cette explication devrait prendre la forme d'un plan de mesures correctives.

(6) Étant donné que le superviseur principal est censé évaluer les accords de sous-traitance du prestataire tiers critique de services TIC, un modèle doit être élaboré pour fournir des informations sur ces accords. Le modèle devrait tenir compte du fait que les prestataires tiers critiques de services TIC ont des structures différentes de celles des entités financières.

([1]) JO L 333 du 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Une fois que les recommandations adressées à un prestataire tiers critique de services TIC ont été émises par le superviseur principal et que les autorités compétentes ont informé les entités financières concernées des risques recensés dans ces recommandations, le superviseur principal devrait suivre et évaluer la mise en œuvre, par le prestataire tiers critique de services TIC, des mesures et des solutions visant au respect des recommandations. Les autorités compétentes devraient surveiller et évaluer dans quelle mesure les entités financières sont exposées aux risques recensés dans ces recommandations. Afin de maintenir des conditions de concurrence équitables en accomplissant leurs tâches respectives, en particulier lorsque les risques recensés dans les recommandations sont graves et partagés entre un grand nombre d'entités financières dans plusieurs États membres, tant les autorités compétentes que le superviseur principal devraient s'échanger toutes les constatations pertinentes qui leur sont nécessaires pour s'acquitter des missions qui leur incombent respectivement. L'objectif du partage d'informations est de faire en sorte que le retour d'information du superviseur principal au prestataire tiers critique de services TIC en ce qui concerne les actions et les mesures correctives que ce dernier met en œuvre tienne compte de l'incidence sur les risques pour les entités financières, et que les activités de surveillance exercées par les autorités compétentes soient étayées par l'évaluation effectuée par le superviseur principal.

(8) Afin de permettre un partage efficace et efficient des informations, les autorités compétentes devraient évaluer, dans le cadre de leurs activités de surveillance, dans quelle mesure les entités financières qu'elles surveillent sont exposées aux risques recensés dans les recommandations. Cette évaluation devrait être effectuée d'une manière proportionnée et fondée sur les risques. Le superviseur principal devrait demander aux autorités compétentes de partager les résultats de cette évaluation dans les cas spécifiques où les risques associés aux recommandations sont graves et partagés entre un grand nombre d'entités financières dans plusieurs États membres. Afin d'utiliser au mieux les ressources des autorités compétentes lorsqu'il demande de fournir les résultats de cette évaluation, le superviseur principal devrait toujours tenir compte du fait que l'objectif de ces demandes est d'évaluer la mise en œuvre des mesures et des solutions des prestataires tiers critiques de services TIC.

(9) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([2]) et a rendu un avis le 22 juillet 2024.

(10) Le présent règlement se fonde sur le projet de normes techniques de réglementation soumis à la Commission par les AES.

(11) Le comité mixte des AES a procédé à des consultations publiques ouvertes sur les projets de normes techniques de réglementation sur lesquels se fonde le présent règlement, analysé les coûts et avantages potentiels qu'ils impliquent et sollicité l'avis du groupe des parties intéressées au secteur bancaire institué en application de l'article 37 du règlement (UE) n° 1093/2010 du Parlement européen et du Conseil ([3]), du groupe des parties intéressées à l'assurance et la réassurance et du groupe des parties intéressées aux pensions professionnelles institués en application de l'article 37 du règlement (UE) n° 1094/2010 du Parlement européen et du Conseil ([4]) et du groupe des parties intéressées au secteur financier institué en application de l'article 37 du règlement (UE) n° 1095/2010 du Parlement européen et du Conseil ([5]),

([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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([3]) Règlement (UE) n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Règlement (UE) n° 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/79/CE de la Commission (JO L 331 du 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Règlement (UE) n° 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/77/CE de la Commission (JO L 331 du 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Informations que doit fournir un prestataire tiers de services TIC dans la demande de désignation volontaire en tant que prestataire critique

1. Le prestataire tiers de services de technologies de l'information et de la communication (TIC) soumet les informations suivantes dans sa demande motivée de désignation volontaire en tant que prestataire critique, en vertu de l'article 31, paragraphe 11, du règlement (UE) 2022/2554, conformément à l'article 31, paragraphe 1, point a), du règlement (UE) 2022/2554:

a) nom de la personne morale;

b) code d'identification de l'entité juridique;

c) nom de la personne de contact et coordonnées du prestataire tiers critique de services TIC;

d) pays dans lequel l'entité juridique a son siège statutaire;

e) description de la structure d'entreprise comprenant au moins des informations sur sa société mère et sur les autres entreprises liées fournissant des services TIC à des entités financières de l'Union. Ces informations comprennent, le cas échéant:

   i) le nom de la personne morale;

   ii) le code d'identification de l'entité juridique;

   iii) le pays dans lequel l'entité juridique a son siège statutaire;

f) une estimation de la part de marché du prestataire tiers de services TIC dans le secteur financier de l'Union et une estimation de la part de marché par type d'entité financière visée à l'article 2, paragraphe 1, du règlement (UE) 2022/2554 à compter de l'année de présentation de la demande de désignation volontaire en tant que prestataire critique et de l'année précédant cette demande;

g) une description de chaque service TIC fourni à des entités financières de l'Union, y compris:

   i) une description de la nature des activités et du type de services TIC fournis aux entités financières;

   ii) une liste des fonctions des entités financières soutenues par les services TIC fournis, le cas échéant;

   iii) des informations indiquant si les services TIC fournis aux entités financières soutiennent des fonctions critiques ou importantes, le cas échéant;

h) une liste des entités financières qui utilisent les services TIC fournis par le prestataire tiers de services TIC, y compris les informations suivantes pour chacune des entités financières desservies, le cas échéant:

   i) nom de la personne morale;

   ii) code d'identification de l'entité juridique, lorsqu'il est connu du prestataire tiers de services TIC;

   iii) type d'entité financière au sens de l'article 2, paragraphe 1, du règlement (UE) 2022/2554;

   iv) localisation géographique à partir de laquelle les services TIC sont fournis à cette entité juridique spécifique;

i) une liste des prestataires tiers critiques de services TIC figurant dans la dernière liste disponible de ces fournisseurs publiée par les AES conformément à l'article 31, paragraphe 9, du règlement (UE) 2022/2554, qui s'appuient sur les services fournis par le demandeur, le cas échéant;

j) une autoévaluation en ce qui concerne:

   i) le degré de substituabilité pour chaque service TIC fourni par le demandeur, compte tenu des éléments suivants:

      — la part de marché du prestataire tiers de services TIC dans le secteur financier de l'Union,

— le nombre de concurrents pertinents connus par type de services TIC ou groupe de services TIC,

— une description des spécificités relatives aux services TIC proposés, y compris en ce qui concerne toute technologie propriétaire, ou des caractéristiques spécifiques de l'organisation ou de l'activité du prestataire tiers de services TIC;

ii) une connaissance de la disponibilité d'autres prestataires tiers de services TIC à fournir les mêmes services TIC que le prestataire tiers de services TIC soumettant la demande;

k) des informations sur une stratégie commerciale future en ce qui concerne la fourniture de services et d'infrastructures TIC aux entités financières dans l'Union, y compris toute modification prévue du groupe ou de la structure de gestion, l'entrée sur de nouveaux marchés ou l'exercice de nouvelles activités;

l) l'identification des sous-traitants du prestataire tiers de services TIC qui ont été désignés comme prestataires tiers critiques de services TIC;

m) tout autre motif pertinent pour la demande de désignation comme prestataire tiers critique de services TIC.

2. Lorsque le prestataire tiers de services TIC appartient à un groupe, les informations visées au paragraphe 1 sont considérées par rapport aux services TIC fournis par l'ensemble du groupe.

Article 2

Contenu, structure et format des informations devant être soumises, divulguées ou communiquées par les prestataires tiers critiques de services TIC

1. Les prestataires tiers critiques de services TIC fournissent au superviseur principal, à sa demande, toute information nécessaire pour lui permettre d'accomplir ses missions de supervision conformément aux exigences du règlement (UE) 2022/2554.

2. Les informations visées au paragraphe 1 incluent, entre autres:

a) des informations sur les accords et les copies des documents contractuels entre:

i) le prestataire tiers critique de services TIC et les entités financières visées à l'article 2, paragraphe 1, du règlement (UE) 2022/2554;

ii) le prestataire tiers critique de services TIC et ses sous-traitants en vue de saisir la chaîne de valeur technologique des services TIC fournis aux entités financières dans l'Union;

b) des informations sur la structure organisationnelle et la structure de groupe du prestataire tiers critique de services TIC, y compris l'identification de toutes les entités appartenant au même groupe qui fournissent directement ou indirectement des services TIC à des entités financières dans l'Union;

c) des informations sur les principaux actionnaires, y compris leur structure et leur répartition géographique, des entités suivantes:

i) les entités qui détiennent, seules ou conjointement avec leurs entités liées, 25 % ou plus du capital ou des droits de vote du prestataire tiers critique de services TIC;

ii) les entités qui ont le droit de nommer ou de révoquer la majorité des membres de l'organe d'administration, de direction ou de surveillance du prestataire tiers critique de services TIC;

iii) les entités qui contrôlent, en vertu d'un accord, la majorité des droits de vote des actionnaires ou des membres du prestataire tiers critique de services TIC;

d) des informations sur la part de marché du prestataire tiers critique de services TIC par type de services, sur les marchés pertinents où il exerce ses activités;

e) des informations sur les dispositifs de gouvernance interne du prestataire tiers critique de services TIC, y compris la structure avec les lignes de responsabilité en matière de gouvernance et les règles d'imputabilité;

f) le procès-verbal de la réunion de l'organe de direction du prestataire tiers critique de services TIC et de tout autre comité interne compétent, qui ont trait, de quelque manière que ce soit, aux activités et aux risques concernant les services TIC qui soutiennent des fonctions d'entités financières au sein de l'Union;

g) des informations sur la sécurité des TIC du prestataire tiers critique de services TIC, y compris les stratégies, objectifs, politiques, procédures, protocoles, processus, mesures de contrôle visant à protéger les données sensibles, contrôles d'accès, pratiques de chiffrement et plans de réponse en cas d'incident pertinents, et des informations sur le respect de toutes les réglementations et de toutes les normes nationales et internationales pertinentes, le cas échéant;

h) des informations sur les mesures techniques et organisationnelles visant à garantir la protection et la confidentialité des données, y compris les données à caractère personnel et non personnel, les mesures de contrôle mises en œuvre pour protéger les données sensibles, les contrôles d'accès, les pratiques de chiffrement et les plans de réponse en cas de violation de données; en ce qui concerne le traitement de données à caractère personnel, le prestataire tiers de services TIC est soumis à la législation de pays tiers, y compris aux demandes d'accès des gouvernements de pays tiers, à la liste des pays tiers et aux lois applicables;

i) des informations sur les mécanismes que le prestataire tiers critique de services TIC propose aux entités financières de l'Union pour la portabilité des données, la portabilité des applications et l'interopérabilité;

j) des informations sur la localisation des centres de données et des centres de production de TIC utilisés aux fins de la fourniture de services aux entités financières, y compris une liste de tous les locaux et installations pertinents du prestataire tiers critique de services TIC, y compris en dehors de l'Union;

k) des informations sur la fourniture de services par un prestataire tiers critique de services TIC de pays tiers, y compris des informations sur les dispositions juridiques pertinentes applicables aux données à caractère personnel et à caractère non personnel traitées par le prestataire tiers de services TIC;

l) des informations sur les mesures prises pour faire face aux risques découlant de la fourniture de services TIC par un prestataire tiers critique de services TIC et ses sous-traitants de pays tiers;

m) des informations sur le cadre de gestion du risque et le cadre de gestion des incidents, notamment les politiques, procédures, outils, mécanismes et modalités de gouvernance du prestataire tiers critique de services TIC et de ses sous-traitants, y compris la liste et la description des incidents majeurs ayant des effets directs ou indirects sur les entités financières au sein de l'Union, y compris les détails pertinents permettant de déterminer l'importance de l'incident pour les entités financières et d'évaluer les éventuelles incidences transfrontières;

n) des informations sur le cadre de gestion des changements, y compris les politiques, procédures et contrôles du prestataire tiers critique de services TIC et de ses sous-traitants;

o) des informations sur le cadre global de réponse et de rétablissement du prestataire tiers critique de services TIC, y compris les plans de continuité des activités et les accords et procédures connexes, la politique de cycle de vie du développement des logiciels, les plans de réponse et de rétablissement et les modalités et procédures connexes, les modalités et procédures des politiques de sauvegarde;

p) des informations sur le suivi des performances, le suivi de la sécurité et le suivi des incidents, ainsi que des informations sur les mécanismes de déclaration liés à la performance des services, aux incidents et au respect des accords de niveau de service et des objectifs de niveau de service convenus, ou d'accords similaires conclus entre des prestataires tiers critiques de services TIC et des entités financières dans l'Union;

q) des informations sur le cadre de gestion, par un prestataire tiers de services TIC, du prestataire tiers critique de services TIC, notamment les stratégies, politiques, procédures, processus et contrôles, y compris des détails sur la diligence requise et l'évaluation des risques effectuée par le prestataire tiers critique de services TIC sur ses sous-traitants avant de conclure un accord avec eux, ainsi que le suivi de la relation couvrant tous les risques pertinents en matière de TIC et de contrepartie;

r) des extractions des systèmes de suivi et d'analyse du prestataire tiers critique de services TIC et de ses sous-traitants, couvrant, sans toutefois s'y limiter, le suivi du réseau, des serveurs, des applications et de la sécurité, l'analyse des vulnérabilités, la gestion des journaux, le suivi des performances, la gestion des incidents et les mesures liées aux objectifs de fiabilité, tels que les objectifs de niveau de service;

s) des extractions de tout système ou application de production, de préproduction et de test utilisé(e) par le prestataire tiers critique de services TIC et ses sous-traitants pour fournir directement ou indirectement des services à des entités financières dans l'Union;

t) les rapports d'audit de conformité et les rapports d'audit disponibles, ainsi que toute constatation d'audit pertinente, y compris les audits réalisés par les autorités nationales dans l'Union et en dehors de l'Union lorsque des accords de coopération avec les autorités compétentes prévoient un tel échange d'informations, ou les certifications obtenues par le prestataire tiers critique de services TIC ou ses sous-traitants, y compris les rapports d'auditeurs internes et externes, les certifications ou les évaluations de la conformité avec les normes sectorielles. Cela comprend des informations sur tout type de test indépendant disponible de la résilience des systèmes TIC du prestataire tiers critique de services TIC, y compris tout type de test d'intrusion fondé sur la menace effectué par le prestataire tiers de services TIC;

u) des informations sur toute évaluation effectuée par le prestataire tiers critique de services TIC à sa demande ou en son nom, concernant le caractère approprié et l'intégrité des personnes occupant des postes clés au sein du prestataire tiers critique de services TIC;

v) des informations sur tout plan de mesures correctives visant à donner suite aux recommandations visées à l'article 3, et les informations pertinentes connexes permettant de confirmer la mise en œuvre des solutions;

w) des informations sur les programmes de formation des salariés et les programmes de sensibilisation à la sécurité disponibles, y compris, le cas échéant, des informations sur les investissements, les ressources et les méthodes du prestataire tiers critique de services TIC pour former son personnel à traiter des données financières sensibles et à maintenir des niveaux élevés de sécurité;

x) des informations sur les activités du prestataire tiers critique de services TIC et les états financiers, y compris des informations sur le budget et les ressources liées aux TIC et à la sécurité.

Article 3

Informations communiquées par des prestataires tiers critiques de services TIC après la formulation de recommandations

1. Le prestataire tiers critique de services TIC fournit au superviseur principal un rapport contenant un plan de mesures correctives concernant les recommandations et les solutions que le prestataire tiers critique de services TIC prévoit de mettre en œuvre afin d'atténuer les risques recensés dans les recommandations visées à l'article 35, paragraphe 1, point d), du règlement (UE) 2022/2254. Le rapport est conforme au calendrier fixé par le superviseur principal pour chaque recommandation.

2. Afin de permettre le suivi de la mise en œuvre des mesures prises ou des solutions mises en œuvre par le prestataire tiers critique de services TIC en ce qui concerne les recommandations reçues, le prestataire tiers critique de services TIC partage avec le superviseur principal, sur demande:

a) les rapports d'avancement intermédiaires et les documents justificatifs connexes précisant l'état d'avancement de la mise en œuvre des mesures et solutions énoncées dans le rapport fourni par le prestataire tiers critique de services TIC au superviseur principal dans le délai défini par ce dernier;

b) les rapports finaux et les documents justificatifs connexes précisant les mesures prises ou les solutions mises en œuvre par le prestataire tiers critique de services TIC afin d'atténuer les risques recensés dans les recommandations reçues.

Article 4

Structure et format des informations fournies par les prestataires tiers critiques de services TIC

1. Le prestataire tiers critique de services TIC fournit les informations demandées au superviseur principal par l'intermédiaire des canaux électroniques sécurisés dédiés indiqués par le superviseur principal dans sa demande et sous la forme définie par le superviseur principal.

2. Lorsqu'ils fournissent des informations au superviseur principal, les prestataires tiers critiques de services TIC:

a) suivent la structure indiquée par le superviseur principal dans sa demande d'informations;

b) localisent clairement l'élément d'information pertinent dans la documentation soumise.

3. Les informations soumises, divulguées ou communiquées au superviseur principal par le prestataire tiers critique de services TIC sont rédigées dans une langue usuelle dans la sphère financière internationale.

Article 5

Modèle pour la fourniture d'informations sur les accords de sous-traitance

Un prestataire tiers critique de services TIC qui est tenu de partager des informations sur les accords de sous-traitance fournit ces informations au superviseur principal conformément au modèle figurant en annexe.

Article 6

Évaluation par les autorités compétentes des risques traités dans les recommandations du superviseur principal

1. Dans le cadre de sa surveillance des entités financières, l'autorité compétente évalue l'incidence sur les entités financières des mesures prises par le prestataire tiers critique de services TIC sur la base des recommandations du superviseur principal conformément au principe de proportionnalité.

2. Lorsqu'elle procède à l'évaluation visée au paragraphe 1, l'autorité compétente tient compte de l'ensemble des éléments suivants:

a) l'adéquation et la cohérence des mesures correctives mises en œuvre par les entités financières pour atténuer les risques recensés dans les recommandations;

b) l'évaluation effectuée par le superviseur principal du respect, par le prestataire tiers critique de services TIC, des mesures et solutions figurant dans le rapport lorsque ce respect a une incidence sur l'exposition des entités financières relevant de la compétence de ce prestataire aux risques recensés dans les recommandations;

c) l'avis de toute autre autorité compétente qui a été consultée conformément à l'article 42, paragraphe 5, du règlement (UE) 2022/2554;

d) la question de savoir si le superviseur principal a considéré que les mesures et solutions mises en œuvre par le prestataire tiers critique de services TIC étaient adéquates pour atténuer l'exposition des entités financières relevant de la compétence de ce prestataire aux risques recensés dans les recommandations.

3. À la demande du superviseur principal, l'autorité compétente fournit dans un délai raisonnable les résultats de l'évaluation visée au paragraphe 1. Lorsqu'il demande les résultats de cette évaluation, le superviseur principal tient compte du principe de proportionnalité et de l'ampleur des risques associés aux recommandations, y compris les incidences transfrontières de ces risques lorsqu'ils ont une incidence sur des entités financières opérant dans plus d'un État membre.

4. Le cas échéant, l'autorité compétente demande aux entités financières de fournir toute information nécessaire à la réalisation de l'évaluation visée au paragraphe 1.

Article 7

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 24 octobre 2024.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

MODÈLE POUR LE PARTAGE D'INFORMATIONS SUR LES ACCORDS DE SOUS-TRAITANCE

Catégorie d'information	Éléments d'information clés
Informations générales	— Nom du prestataire tiers critique de services TIC. — Code d'identification du prestataire tiers critique de services TIC. — Nom de la personne de contact et coordonnées du prestataire tiers critique de services TIC. — Date de présentation du modèle.
Vue d'ensemble des accords de sous-traitance	— Cartographie des accords de sous-traitance, y compris une brève description de l'objet et de la portée des relations de sous-traitance (notamment une indication du niveau de criticité ou de l'importance des accords de sous-traitance pour le prestataire tiers critique de services TIC). — Spécification et description des types de services TIC sous-traités et de leur importance par rapport aux services TIC fournis à des entités financières, conformément aux normes techniques d'exécution adoptées en vertu de l'article 28, paragraphe 9, du règlement (UE) 2022/2554. — Pour préciser les types de services TIC, veuillez vous référer à la liste figurant à l'annexe IV des normes techniques d'exécution adoptées en vertu de l'article 28, paragraphe 9, du règlement (UE) 2022/2554.
Informations relatives aux sous-traitants	— Nom et coordonnées de l'entité juridique (y compris le code d'identification) de chaque sous-traitant. — Coordonnées des membres du personnel responsables de chacune des relations de sous-traitance dans la structure de gestion du prestataire tiers critique de services TIC. — Vue d'ensemble, pour chaque sous-traitant, de l'expertise, de l'expérience et des qualifications liées aux services TIC visés par le contrat.
Description des services fournis par les sous-traitants	— Description détaillée des services TIC spécifiques fournis par chaque sous-traitant. — Délimitation des responsabilités et des tâches attribuées aux sous-traitants en détaillant les différents rôles aux différentes étapes des processus TIC. — Informations sur le niveau d'accès des sous-traitants à des données à caractère personnel ou autrement sensibles ou à des systèmes sensibles concernant les services TIC fournis à des entités financières. — Informations sur les sites à partir desquels les services des sous-traitants sont fournis et sur les mesures prises pour faire face aux risques découlant des services fournis en dehors de l'Union.
Gouvernance et supervision de la sous-traitance	— Description du cadre contractuel et de gouvernance en place pour gérer les relations de sous-traitance, y compris les clauses limitant l'utilisation de données sensibles. — Explication des processus de sélection, d'engagement et de suivi des sous-traitants. — Vue d'ensemble des indicateurs de performance, des accords et des objectifs de niveau de service, ainsi que des indicateurs de performance clés utilisés pour évaluer les performances et le suivi de la fiabilité du sous-traitant.
Gestion des risques et conformité	— Évaluation des profils de risque du sous-traitant et de l'incidence potentielle sur les services TIC fournis aux entités financières. — Explication des mesures d'atténuation des risques mises en œuvre pour faire face aux risques liés à la sous-traitance. — Précisions sur le respect par le sous-traitant de la réglementation applicable, y compris en ce qui concerne la protection des données et les normes du secteur.

Catégorie d'information	Éléments d'information clés
Continuité des activités et plans d'urgence	— Vue d'ensemble des plans de continuité des activités et de réponse et de rétablissement du sous-traitant. — Description des modalités mises en place pour assurer la continuité du service en cas de perturbations ou de résiliation par le sous-traitant. — Fréquence des tests des plans de continuité des activités ainsi que des plans de réponse et de rétablissement effectués par les sous-traitants, dates des derniers tests au cours des trois dernières années, et spécification si le prestataire tiers critique de services TIC a participé à ces tests.
Notification	— Description des mécanismes de déclaration et de la fréquence de notification entre le prestataire tiers critique de services TIC et ses sous-traitants.
Gestion des incidents et des corrections	— Description des procédures de traitement des incidents, infractions ou non-conformités liés au sous-traitant.
Certifications et audits	— Informations sur toute certification, tout audit indépendant ou toute évaluation concernant des sous-traitants pour valider leurs contrôles de sécurité, leurs normes de qualité ou leur conformité réglementaire. — Date et fréquence des audits des sous-traitants menés par le prestataire tiers critique de services TIC.