Journal officiel
de l'Union européenne

FR
Série L

2025/532

2.7.2025

RÈGLEMENT DÉLÉGUÉ (UE) 2025/532 DE LA COMMISSION

du 24 mars 2025

complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant les éléments qu'une entité financière doit déterminer et évaluer lorsqu'elle sous-traite des services TIC qui soutiennent des fonctions critiques ou importantes

(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 30, paragraphe 5, quatrième alinéa,

considérant ce qui suit:

(1) La fourniture de services TIC à des entités financières repose souvent sur une chaîne complexe de sous-traitants de TIC, au sein de laquelle les prestataires tiers de services TIC sont susceptibles de conclure un ou plusieurs accords de sous-traitance avec d'autres prestataires tiers de services TIC. Le recours indirect à des sous-traitants de TIC peut avoir une incidence sur la capacité d'une entité financière à identifier, évaluer et gérer ses risques, notamment les risques liés aux lacunes que présentent les informations fournies par les prestataires tiers de services TIC ainsi qu'à la capacité de cette entité à obtenir des informations auprès des sous-traitants de TIC fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci. À cet égard, lorsque la fourniture de services TIC à des entités financières repose sur une chaîne potentiellement longue ou complexe de sous-traitants de TIC, il est essentiel que ces entités financières identifient toute la chaîne des sous-traitants fournissant des services TIC qui soutiennent des fonctions critiques ou importantes.

(2) Parmi les sous-traitants fournissant des services TIC qui soutiennent des fonctions critiques ou importantes, les entités financières devraient accorder une attention particulière et constante aux sous-traitants sur lesquels reposent de fait les services TIC qui soutiennent des fonctions critiques ou importantes, notamment à tous les sous-traitants qui fournissent des services TIC dont la perturbation nuirait à la sécurité ou à la continuité du service, tels que répertoriés dans le registre d'informations prévu à l'article 28, paragraphe 3, du règlement (UE) 2022/2554.

(3) La taille, la structure et l'organisation interne des entités financières, ainsi que la nature et la complexité de leurs activités, sont très variables. Dans un souci de proportionnalité, les éléments qu'une entité financière doit déterminer et évaluer en cas de sous-traitance de services TIC qui soutiennent des fonctions critiques ou importantes devraient être définis en tenant compte de cette diversité.

(4) Lorsqu'il est autorisé par les entités financières conformément à l'article 30, paragraphe 2, du règlement (UE) 2022/2554, le recours à des services TIC soutenant des fonctions critiques ou importantes sous-traités par les prestataires tiers de services TIC ne peut décharger les organes de direction des entités financières de la responsabilité ultime de la gestion de leurs risques et du respect de leurs obligations législatives et réglementaires. Lorsque la sous-traitance de services TIC qui soutiennent des fonctions critiques ou importantes est autorisée, il est important que les entités financières aient une vision claire et globale des risques associés à cette sous-traitance afin qu'elles soient en mesure de les surveiller, de les gérer et de les atténuer. Elles devraient donc évaluer ces risques avant la sous-traitance de ces services.

(5) Les sous-traitants de TIC intra-groupe qui fournissent des services TIC soutenant des fonctions critiques ou importantes ou des parties significatives de celles-ci, y compris les sous-traitants de TIC intra-groupe qui sont entièrement ou collectivement détenus par des entités financières appartenant au même système de protection institutionnel, devraient être considérés comme des sous-traitants de TIC.

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

(6) Le cas échéant, dans le contexte d'un groupe, l'entreprise mère des entités financières devrait veiller à l'application uniforme et cohérente, au sein du groupe, de la politique de recours à des sous-traitants de TIC fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci.

(7) Il importe de veiller à une gestion exhaustive des risques qui peuvent survenir lors de la sous-traitance de services TIC qui soutiennent des fonctions critiques ou importantes. C'est pourquoi les entités financières devraient suivre les étapes du cycle de vie d'un accord contractuel sur l'utilisation de services TIC qui soutiennent ces fonctions et qui sont fournis par des prestataires tiers de services TIC, y compris pour les accords de sous-traitance. Il est donc nécessaire de fixer des exigences pour les entités financières qui devraient se refléter dans leurs accords contractuels avec des prestataires tiers de services TIC lorsque le recours à la sous-traitance de services TIC qui soutiennent des fonctions critiques ou importantes est autorisé.

(8) Afin d'atténuer les risques associés à la sous-traitance, il est nécessaire de préciser les conditions dans lesquelles les prestataires tiers de services TIC peuvent recourir à des sous-traitants pour la fourniture de services TIC qui soutiennent des fonctions critiques ou importantes. À cette fin, les accords contractuels de services TIC conclus entre des entités financières et des prestataires tiers de services TIC devraient définir ces conditions, y compris la planification des accords de sous-traitance, les évaluations des risques, la diligence requise et le processus d'approbation des nouveaux accords de sous-traitance de services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci, ou des changements significatifs apportés par le prestataire tiers de services TIC aux accords existants.

(9) Afin que les risques susceptibles de survenir soient identifiés avant qu'une entité financière ne conclue un accord avec un sous-traitant de TIC, le prestataire tiers de services TIC devrait évaluer, de manière appropriée et proportionnée, l'aptitude des sous-traitants potentiels sur la base des accords contractuels de services TIC qu'il a conclus avec l'entité financière. Ces accords contractuels de services TIC devraient donc exiger du prestataire tiers de services TIC, ou de l'entité financière directement, selon le cas, qu'il ou elle évalue les ressources du sous-traitant potentiel, y compris son expertise et le fait qu'il dispose ou non des ressources financières, humaines et techniques appropriées, sa politique de sécurité de l'information et sa structure organisationnelle, y compris la gestion des risques et les contrôles internes qu'il devrait avoir mis en place.

(10) Afin d'atténuer les vulnérabilités et les menaces susceptibles de présenter des risques pour leurs systèmes et opérations de TIC, les entités financières devraient être en mesure de surveiller l'exécution du service TIC et d'être informées de tout changement pertinent au sein de leur chaîne de sous-traitance de TIC lorsque ce changement concerne des fonctions critiques ou importantes.

(11) Afin de permettre aux entités financières d'évaluer les risques associés aux accords de sous-traitance ou aux changements significatifs apportés à ces derniers, les prestataires tiers de services TIC devraient informer les entités financières auxquelles ils fournissent des services TIC de tous les nouveaux accords et de tous les changements bien avant que ceux-ci ne commencent à s'appliquer. Pour la même raison, les entités financières devraient avoir le droit de résilier le contrat qu'elles ont conclu avec un prestataire tiers de services TIC lorsque le résultat de leur évaluation des risques indique que les nouveaux accords ou les changements significatifs apportés à ces derniers présentent un niveau de risque supérieur à leur niveau de tolérance au risque.

(12) Les AES ont procédé à une consultation publique sur le projet de normes techniques de réglementation sur lequel repose le présent règlement, analysé les coûts et les avantages potentiels liés à ce projet, et invité leurs groupes de parties intéressées respectifs établis en application de l'article 37 des règlements (UE) nº 1093/2010 ([2]), (UE) nº 1094/2010 ([3]) et (UE) nº 1095/2010 ([4]) du Parlement européen et du Conseil à donner leur avis.

(13) 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 ([5]) et a rendu un avis le 20 août 2024,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Profil de risque global et complexité

Les entités financières tiennent compte de leur taille et de leur profil de risque global ainsi que de la nature, de l'ampleur et des facteurs d'augmentation ou de diminution de la complexité de leurs services, activités et opérations, y compris des éléments relatifs:

a) au type de services TIC qui soutiennent des fonctions critiques ou importantes couverts par l'accord contractuel entre l'entité financière et le prestataire tiers de services TIC;

b) au type de services TIC couverts par l'accord contractuel entre le prestataire tiers de services TIC et ses sous-traitants;

c) au lieu où exerce le sous-traitant de TIC fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci, ou à la localisation de sa société mère;

d) à la longueur et à la complexité de la chaîne des sous-traitants fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci utilisée par le prestataire tiers de services TIC;

e) à la nature des données partagées avec les sous-traitants de TIC fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci;

f) à la question de savoir si les services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci sont fournis par des sous-traitants situés dans un État membre ou dans un pays tiers, y compris le lieu où les services TIC sont effectivement fournis et le lieu où les données sont effectivement traitées et stockées;

g) à la question de savoir si les sous-traitants de TIC fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci appartiennent au même groupe que l'entité financière bénéficiaire de ces services;

([2]) Règlement (UE) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 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).

([3]) Règlement (UE) nº 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 nº 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).

([4]) Règlement (UE) nº 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 nº 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).

([5]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

h) à la question de savoir si les sous-traitants de TIC fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci sont agréés, enregistrés ou soumis à une surveillance ou à une supervision par une autorité compétente d'un État membre, ou sont soumis au cadre de supervision prévu au chapitre V, section II, du règlement (UE) 2022/2554;

i) à la question de savoir si les prestataires tiers de services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci sont agréés, enregistrés ou soumis à une surveillance ou à une supervision par une autorité de surveillance d'un pays tiers;

j) à la question de savoir si les services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci sont fournis par un seul sous-traitant d'un prestataire tiers de services TIC ou par un petit nombre d'entre eux;

k) à la question de savoir si la sous-traitance de services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci aurait une incidence sur la transférabilité de ces services TIC à un autre prestataire tiers de services TIC;

l) à l'incidence potentielle des perturbations sur la continuité et la disponibilité des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci fournis par le prestataire tiers de services TIC, lorsque ce dernier fait appel à un sous-traitant fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci.

Article 2

Application à l'échelle d'un groupe

Lorsque le présent règlement s'applique sur une base sous-consolidée ou consolidée, l'entreprise mère qui est chargée de fournir les états financiers consolidés ou sous-consolidés pour le groupe fait en sorte que les conditions de sous-traitance pour l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci, lorsque cette sous-traitance est autorisée en vertu des accords contractuels relatifs à l'utilisation de services TIC, soient mises en œuvre de manière cohérente au sein de toutes les entités financières appartenant au groupe et soient adéquates pour l'application effective du présent règlement à tous les niveaux pertinents.

Article 3

Diligence requise et évaluation des risques en ce qui concerne le recours à des sous-traitants qui soutiennent des fonctions critiques ou importantes

1. Avant de conclure un accord contractuel avec un prestataire tiers de services TIC, une entité financière décide si ce prestataire peut sous-traiter un service TIC qui soutient des fonctions critiques ou importantes ou des parties significatives de celles-ci. L'entité financière ne conclut un tel accord contractuel que si elle a déterminé que toutes les conditions suivantes ont été remplies:

a) les processus de diligence requise à l'égard du prestataire tiers de services TIC garantissent que ce dernier est en mesure de sélectionner et d'évaluer les capacités opérationnelles et financières des sous-traitants de TIC potentiels à fournir des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci, y compris en le soumettant, lorsque l'entité financière l'exige, à des tests de résilience opérationnelle numérique tels que visés au chapitre IV du règlement (UE) 2022/2554;

b) le prestataire tiers de services TIC est en mesure d'identifier tous les sous-traitants fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci, afin de pouvoir notifier ces sous-traitants à l'entité financière et la renseigner à leur sujet, et est en mesure de fournir à l'entité financière toutes les informations qui peuvent être nécessaires à l'évaluation des conditions énoncées au présent article;

c) le prestataire tiers de services TIC fait en sorte que les accords contractuels conclus avec les sous-traitants fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci permettent à l'entité financière de se conformer à ses propres obligations découlant du règlement (UE) 2022/2554 ainsi que de la législation de l'Union et de la législation nationale applicables;

d) le sous-traitant accorde à l'entité financière ainsi qu'aux autorités compétentes et aux autorités de résolution les mêmes droits contractuels d'accès et d'inspection que ceux que leur accorde le prestataire tiers de services TIC;

e) sans préjudice de la responsabilité ultime de l'entité financière de se conformer à ses obligations légales et réglementaires, le prestataire tiers de services TIC dispose lui-même des capacités, de l'expertise et des ressources financières, humaines et techniques suffisantes pour surveiller les risques liés aux TIC au niveau des sous-traitants, notamment en appliquant des normes appropriées en matière de sécurité de l'information et en disposant d'une structure organisationnelle appropriée, d'une gestion des risques et de contrôles internes ainsi que de notifications et de réponses en cas d'incident;

f) l'entité financière dispose des capacités, de l'expertise et des ressources financières, humaines et techniques suffisantes pour surveiller les risques liés aux TIC concernant le service TIC qui soutient des fonctions critiques ou importantes ou des parties significatives de celles-ci et qui a été sous-traité par le prestataire tiers, notamment en appliquant des normes appropriées en matière de sécurité de l'information et en disposant d'une structure organisationnelle appropriée, d'une gestion des risques, de réponses apportées en cas d'incident, d'une gestion de la continuité des activités ainsi que de contrôles internes;

g) l'entité financière a évalué l'incidence d'une éventuelle défaillance d'un sous-traitant fournissant des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci sur la résilience opérationnelle numérique et la solidité financière de l'entité financière;

h) l'entité financière a évalué les risques associés à la localisation des sous-traitants potentiels en ce qui concerne les services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci fournis par le prestataire tiers de services TIC;

i) l'entité financière a évalué les risques de concentration de TIC au niveau de l'entité conformément à l'article 29 du règlement (UE) 2022/2554;

j) l'entité financière a évalué s'il existait des obstacles à l'exercice de droits d'accès, d'inspection et d'audit par les autorités compétentes, les autorités de résolution ou l'entité financière, y compris par les personnes qu'elles désignent.

2. Les entités financières qui font appel à des prestataires tiers de services TIC qui sous-traitent des services TIC soutenant des fonctions critiques ou importantes ou des parties significatives de celles-ci effectuent périodiquement l'évaluation des risques visée au paragraphe 1, points f) à j), à l'aune d'éventuels changements dans leur environnement d'entreprise, y compris les changements dans les fonctions «métiers» s'appuyant sur les TIC, ainsi que dans leurs évaluations des risques, y compris les menaces liées aux TIC, les risques de concentration des TIC et les risques géopolitiques.

3. Le fait de se reposer sur les résultats de l'évaluation des risques effectuée par leurs prestataires tiers de services TIC à l'égard de leurs sous-traitants aux fins du respect des obligations énoncées dans le présent article ne limite en rien la responsabilité ultime des entités financières de respecter leurs obligations légales et réglementaires découlant du règlement (UE) 2022/2554.

Article 4

Conditions de sous-traitance des services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci

1. L'accord contractuel conclu entre l'entité financière et le prestataire tiers de services TIC détermine, parmi les services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci, ceux qui peuvent faire l'objet d'une sous-traitance, et dans quelles conditions. Ce contrat précise:

a) que le prestataire tiers de services TIC est responsable de la fourniture des services fournis par les sous-traitants;

b) que le prestataire tiers de services TIC est tenu de surveiller tous les services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci et qui ont été sous-traités, afin de veiller au respect permanent de ses obligations contractuelles envers l'entité financière;

c) les obligations de suivi et de déclaration incombant au prestataire tiers de services TIC à l'égard de l'entité financière en ce qui concerne les sous-traitants qui fournissent des services TIC soutenant des fonctions critiques ou importantes ou des parties significatives de celles-ci;

d) que le prestataire tiers de services TIC doit évaluer tous les risques associés au lieu d'établissement des sous-traitants actuels ou potentiels qui fournissent un service TIC soutenant des fonctions critiques ou importantes ou des parties significatives de celles-ci, ainsi qu'à leur société mère et au lieu où le service TIC concerné est fourni;

e) Le lieu de traitement et de stockage des données par le sous-traitant, le cas échéant;

f) que le prestataire tiers de services TIC doit préciser, dans son contrat avec ses sous-traitants, les obligations de suivi et de déclaration incombant à ces sous-traitants à son égard et, s'il en a été convenu ainsi, à l'égard de l'entité financière;

g) que le prestataire tiers de services TIC doit, tout au long de la chaîne de sous-traitance, assurer la continuité des services TIC qui soutiennent des fonctions critiques ou importantes en cas de non-respect par un sous-traitant TIC de ses obligations contractuelles;

h) que l'accord contractuel entre le prestataire tiers de services TIC et ses sous-traitants contient les exigences relatives aux plans d'urgence visés à l'article 30, paragraphe 3, point c), du règlement (UE) 2022/2554 et précise les niveaux de service que les sous-traitants TIC doivent atteindre en ce qui concerne ces plans;

i) que l'accord contractuel entre le prestataire tiers de services TIC et ses sous-traitants énonce les normes de sécurité des TIC et toute exigence supplémentaire en matière de sécurité visées à l'article 30, paragraphe 3, point c), du règlement (UE) 2022/2554;

j) que le sous-traitant doit accorder à l'entité financière, aux autorités compétentes et aux autorités de résolution concernées les mêmes droits d'accès, d'inspection et d'audit que ceux visés à l'article 30, paragraphe 3, point e), du règlement (UE) 2022/2554;

k) que le prestataire tiers de services TIC doit notifier à l'entité financière tout changement significatif apporté aux accords de sous-traitance;

l) que l'entité financière a le droit de résilier le contrat avec le prestataire tiers de services TIC lorsque soit les conditions énoncées à l'article 6 du présent règlement soit les conditions énumérées à l'article 28, paragraphe 7, du règlement (UE) 2022/2554 sont remplies.

2. Les changements qu'il est nécessaire, pour se conformer au présent règlement, d'apporter aux accords contractuels entre l'entité financière et les prestataires tiers de services TIC fournissant un service TIC qui soutient des fonctions critiques ou importantes ou des parties significatives de celles-ci sont mis en œuvre en temps utile et dès que possible. L'entité financière documente le calendrier prévu pour la mise en œuvre.

Article 5

Changements significatifs apportés aux accords de sous-traitance de services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci

1. L'accord contractuel prévoit que le prestataire tiers de services TIC informe l'entité financière de tout changement significatif qu'il est prévu d'apporter à ses accords de sous-traitance en temps utile pour permettre à l'entité financière d'évaluer:

a) l'incidence sur les risques auxquels elle est ou pourrait être exposée;

b) si de tels changements significatifs sont susceptibles de compromettre la capacité du prestataire tiers de services TIC à respecter ses obligations contractuelles à l'égard de l'entité financière.

2. L'accord contractuel prévoit un délai de préavis raisonnable dans lequel l'entité financière doit approuver les changements ou s'y opposer.

3. Le prestataire tiers de services TIC ne met en œuvre les changements significatifs apportés à ses accords de sous-traitance qu'après que l'entité financière a approuvé ces changements ou si elle ne s'y est pas opposée avant la fin du délai de préavis.

4. Lorsque l'entité financière estime que les changements significatifs visés au paragraphe 1 dépassent son niveau de tolérance au risque, elle doit, avant la fin du délai de préavis:

a) en informer le prestataire tiers de services TIC;

b) s'opposer aux changements et demander leur modification avant leur mise en œuvre.

Article 6

Résiliation du contrat entre l'entité financière et le prestataire tiers de services TIC

L'entité financière a le droit de prévoir, dans l'accord contractuel avec le prestataire tiers de services TIC, la résiliation de cet accord dans chacun des cas suivants:

a) l'entité financière s'est opposée aux changements significatifs apportés aux accords de sous-traitance de services TIC qui soutiennent des fonctions critiques ou importantes et a demandé la modification de ces accords, mais le prestataire tiers de services TIC les a néanmoins mis en œuvre;

b) le prestataire tiers de services TIC a mis en œuvre des changements significatifs des accords de sous-traitance de services TIC qui soutiennent des fonctions critiques ou importantes ou des parties significatives de celles-ci avant la fin de la période de préavis sans l'approbation de l'entité financière;

c) le prestataire tiers de services TIC a sous-traité un service TIC qui soutient des fonctions critiques ou importantes ou des parties significatives de celles-ci dont la sous-traitance n'est pas explicitement autorisée par le contrat entre l'entité financière et le prestataire tiers de services TIC.

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 mars 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN