COMMISSION
EUROPÉENNE

Bruxelles, le 13.3.2024
C(2024) 1531 final

RÈGLEMENT DÉLÉGUÉ (UE) …/... DE LA COMMISSION

du 13.3.2024

complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant le contenu détaillé de la politique relative aux accords contractuels sur l'utilisation de services TIC soutenant des fonctions critiques ou importantes fournis par des prestataires tiers de services TIC

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE L'ACTE DÉLÉGUÉ

L'article 28, paragraphe 2, du règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier (ci-après le «règlement DORA») exige que «[a]ux fins de leur cadre de gestion du risque lié aux TIC, les entités financières [...] adoptent une stratégie en matière de risques liés aux prestataires tiers de services TIC et la réexaminent régulièrement [...].La stratégie en matière de risques liés aux prestataires tiers de services TIC inclut une politique relative à l'utilisation des services TIC qui soutiennent des fonctions critiques ou importantes fournis par des prestataires tiers de services TIC et s'applique sur une base individuelle et, le cas échéant, sur une base sous-consolidée et consolidée. [...]»

Conformément à l'article 28, paragraphe 10, du règlement DORA, les AES, agissant par l'intermédiaire du comité mixte, élaborent des projets de normes techniques de réglementation pour préciser davantage le contenu détaillé de la politique relative aux accords contractuels relatifs à l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes fournis par des prestataires tiers de services TIC.

Transmis à la Commission le 17 janvier 2024, le présent règlement délégué correspond à ce mandat. Il a été tenu compte, lors de son élaboration, des spécifications existantes figurant dans les orientations sur les accords d'externalisation publiées par les autorités européennes de surveillance (ABE, AEMF et AEAPP) et d'autres spécifications pertinentes figurant dans les orientations de l'ABE sur la gestion des risques liés aux TIC et en matière de sécurité.

2. CONSULTATION AVANT L'ADOPTION DE L'ACTE

Dans le cadre du processus d'élaboration des normes techniques de réglementation énoncées dans le présent règlement délégué, les AES ont publié leur projet de normes le 19 juin 2023 pour une période de consultation de trois mois, qui s'est achevée le 11 septembre 2023. Les AES ont reçu 103 réponses de divers acteurs du marché, issus de l'ensemble du secteur financier. Les observations des parties prenantes portaient essentiellement sur les points suivants:

- préciser davantage les normes et envisager de les appliquer de manière proportionnée; revoir la clause de réexamen annuel de la politique appliquée;
- préciser davantage comment seront assurés l'alignement et la cohérence entre les normes proposées et les orientations des AES en matière d'externalisation;
- préciser et limiter le rang des sous-traitants de services TIC couverts par les normes proposées;
- préciser si une différenciation est opérée entre les prestataires de services TIC de l'UE et ceux de pays tiers;
- préciser si une politique à l'échelle du groupe suffit, ou s'il faut prévoir des politiques distinctes par entité/implantation géographique;
- préciser davantage ou supprimer les conditions d'utilisation de certifications;
- tenir compte du faible pouvoir de négociation des entités financières par rapport à certaines des exigences parmi les plus contraignantes;
- préciser davantage certains aspects des plans de sortie;
- exempter les prestataires de services TIC intragroupe de certaines exigences.

À la lumière des commentaires reçus, les AES ont apporté des modifications au projet de normes techniques de réglementation, essentiellement sous les aspects suivants:

- **proportionnalité**: les projets de normes ont été adaptés afin de garantir qu'il est tenu compte des facteurs d'augmentation ou, au contraire, de diminution du risque pour l'application du principe de proportionnalité, et afin de rendre l'article 1er plus clair;
- **diligence raisonnable**: l'article énonçant les exigences applicables en matière de diligence raisonnable a été adapté afin de préciser les pièces justificatives que les entités financières doivent utiliser dans le cadre de la procédure de diligence raisonnable, et d'ajouter qu'elles doivent, si possible, en utiliser plusieurs;
- **clauses contractuelles**: les exigences en matière d'audit, d'information et de droits d'accès ont été modifiées afin de préciser que les entités financières doivent recourir à leur propre fonction d'audit interne ou à un tiers désigné par elles, mais qu'elles peuvent utiliser des certifications délivrées par des tiers et recourir à des audits groupés lorsque cela est approprié.
- **sortie et résiliation des accords contractuels**: l'article a été revu afin de préciser qu'un plan de sortie documenté doit accompagner chaque accord contractuel relatif à l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes. L'article précise également que les tests de ces plans de sortie doivent prendre en compte les interruptions de service imprévues et persistantes.

3. ÉLÉMENTS JURIDIQUES DE L'ACTE DÉLÉGUÉ

L'article 1er définit les facteurs d'augmentation ou de diminution du risque ou de la complexité dont doit tenir compte la politique d'une entité financière relative à l'utilisation de services TIC fournis par des prestataires tiers de services TIC à l'appui de fonctions critiques ou importantes (ci-après la «politique»).

L'article 2 définit les modalités d'application des règles lorsqu'une entité financière fait partie d'un groupe.

L'article 3 établit les règles relatives aux dispositifs de gouvernance.

L'article 4 précise les exigences que la politique doit fixer pour chaque phase importante du cycle de vie de l'accord contractuel.

L'article 5 dispose que la politique doit exiger des entités financières qu'elles procèdent à une évaluation des risques avant de conclure un accord contractuel avec un prestataire tiers de services TIC.

Aux termes de l'article 6, la politique doit prévoir un processus de sélection et d'évaluation des prestataires tiers potentiels de services TIC, à mettre en œuvre avant la conclusion de tout accord contractuel.

L'article 7 dispose que la politique doit prévoir des mesures pour la détection, la prévention et la gestion des conflits d'intérêts réels ou potentiels découlant du recours à des prestataires tiers de services TIC.

L'article 8 établit des règles sur les modalités de formulation des clauses contractuelles que doit fixer la politique.

L'article 9 établit des règles sur les modalités de suivi des accords contractuels que doit contenir la politique.

Conformément à l’article 10, la politique doit exiger que chaque accord contractuel s'accompagne d’un plan de sortie documenté et que ce plan soit régulièrement réexaminé et testé.

L’article 11 fixe la date d’entrée en vigueur.

RÈGLEMENT DÉLÉGUÉ (UE) …/... DE LA COMMISSION

du 13.3.2024

complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant le contenu détaillé de la politique relative aux accords contractuels sur l'utilisation de services TIC soutenant des fonctions critiques ou importantes fournis par des prestataires tiers de services TIC

(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 28, paragraphe 10, troisième alinéa,

considérant ce qui suit:

(1) Le cadre sur la résilience opérationnelle numérique du secteur financier établi par le règlement (UE) 2022/2554 exige que les entités financières se fixent certains principes clés pour la gestion des risques liés aux prestataires tiers de services TIC, risques qui sont particulièrement importants lorsqu'elles font appel à de tels prestataires tiers pour soutenir leurs fonctions importantes ou critiques.

(2) Les entités financières sont tenues d'adopter, comme partie intégrante de leur cadre de gestion du risque lié aux TIC, une stratégie en matière de risques liés aux prestataires tiers de services TIC, et de réexaminer régulièrement cette stratégie. Conformément à l'article 28, paragraphe 2, du règlement (UE) 2022/2554, cette stratégie doit inclure une politique relative à l'utilisation des services TIC soutenant des fonctions critiques ou importantes qui sont fournis par des prestataires tiers de services TIC. Elle s'applique sur une base individuelle et, le cas échéant, sur une base consolidée et sous-consolidée.

(3) Les entités financières varient considérablement par leur taille, leur structure et leur organisation interne, ainsi que par la nature et la complexité de leurs activités et opérations. Tout en imposant, pour l'élaboration de la politique relative aux accords contractuels sur l'utilisation de services TIC soutenant des fonctions critiques ou importantes qui sont fournis par des prestataires tiers de services TIC, un certain nombre d'exigences réglementaires essentielles qui conviennent pour toutes les entités financières, il est nécessaire de tenir compte de cette diversité et de veiller à ce que les exigences fixées soient appliquées de manière proportionnée.

(4) Dans le cas d'entités financières faisant partie d'un groupe, il devrait incomber à l'entreprise mère chargée de fournir les états financiers consolidés ou sous-consolidés

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

du groupe de veiller à ce que la politique soit appliquée de manière uniforme et cohérente au sein du groupe.

(5) Dans le cadre de l'application de la politique, les prestataires de services TIC intragroupe, y compris ceux qui sont entièrement ou collectivement détenus par des entités financières relevant du même système de protection institutionnel, devraient être considérés comme des prestataires tiers de services TIC. Les risques posés par les prestataires de services TIC intragroupe peuvent certes être différents, mais les exigences qui leur sont applicables en vertu du règlement (UE) 2022/2554 sont les mêmes. De même, lorsqu'il existe une chaîne de prestataires tiers de services TIC, la politique devrait s'appliquer aux sous-traitants qui fournissent aux prestataires tiers de services TIC des services TIC soutenant des fonctions critiques ou importantes ou des parties importantes de celles-ci.

(6) La responsabilité ultime, incombant à l'organe de direction, de la gestion du risque lié aux TIC d'une entité financière, constitue un principe fondamental qui s'applique aussi au recours à des prestataires tiers de services TIC. Cette responsabilité devrait se traduire plus avant par l'implication constante de l'organe de direction dans le contrôle et le suivi de la gestion du risque lié aux TIC, y compris dans l'adoption et le réexamen, au moins une fois par an, de la politique.

(7) Afin de garantir un reporting approprié à l'organe de direction, la politique devrait préciser et énoncer clairement les responsabilités internes en matière d'approbation, de gestion, de contrôle et de documentation des accords contractuels sur l'utilisation de services TIC soutenant des fonctions critiques ou importantes qui sont fournis par des prestataires tiers de services TIC (ci-après les «accords contractuels»), y compris les services TIC fournis en vertu des accords contractuels visés à l'article 28, paragraphe 1, point a), du règlement (UE) 2022/2554.

(8) Afin de tenir compte de tous les risques qui peuvent être liés à l'achat contractuel de services TIC à l'appui d'une fonction critique ou importante, la structure de la politique devrait suivre toutes les étapes de chaque phase importante du cycle de vie des accords contractuels conclus avec des prestataires tiers.

(9) Afin d'atténuer les risques identifiés, la politique devrait préciser les modalités de planification des accords contractuels, notamment en ce qui concerne l'évaluation des risques, la diligence raisonnable et la procédure d'approbation de nouveaux accords contractuels ou de modifications importantes d'accords contractuels existants. Aux fins de la gestion des risques susceptibles de survenir avant la conclusion d'un accord contractuel avec un prestataire tiers de services TIC, la politique devrait prévoir un processus approprié et proportionné pour la sélection des prestataires tiers de services TIC potentiels et l'évaluation de leur adéquation, et imposer à l'entité financière de tenir compte d'une liste non exhaustive d'éléments que ces prestataires tiers devraient avoir mis en place. Cette liste devrait couvrir la réputation commerciale des prestataires tiers, leurs ressources financières, humaines et techniques, la sécurité des informations en leur sein, leur structure organisationnelle, y compris leur gestion des risques, et les contrôles internes qu'ils appliquent.

(10) Afin de garantir une bonne gestion des risques dans le cadre de la fourniture par des prestataires tiers de services TIC soutenant des fonctions critiques ou importantes, la politique devrait contenir des informations sur la mise en œuvre, le suivi et la gestion des accords contractuels, y compris au niveau consolidé et sous-consolidé, s'il y a lieu. Cela inclut des exigences concernant les clauses contractuelles relatives aux obligations mutuelles de l'entité financière et du prestataire tiers de services TIC,

lesquelles devraient être énoncées par écrit. Afin de garantir une surveillance efficace et de favoriser la résilience en cas de changements dans le modèle d'entreprise ou l'environnement des entreprises, la politique devrait garantir le droit des entités financières, ou de tiers désignés par elles, et des autorités compétentes de procéder à des inspections et d'accéder à des informations, et elle devrait également préciser les stratégies de sortie et les processus de résiliation des accords contractuels.

(11) Dans la mesure où des données à caractère personnel sont traitées par des prestataires tiers de services TIC, la politique et les accords contractuels sont sans préjudice des obligations prévues par le règlement (UE) 2016/679 et devraient les compléter, par exemple par la mise en place d'un contrat écrit prévoyant les modalités de traitement des données à caractère personnel, l'obligation de garantir la sécurité de ce traitement et tous les autres éléments requis par ledit règlement.

(12) Le comité mixte des autorités européennes de surveillance visé à l'article 54 du règlement (UE) nº 1093/2010 du Parlement européen et du Conseil[2], à l'article 54 du règlement (UE) nº 1094/2010 du Parlement européen et du Conseil[3] et à l'article 54 du règlement (UE) nº 1095/2010 du Parlement européen et du Conseil[4] a procédé à des consultations publiques ouvertes sur le projet de normes techniques de réglementation sur lequel se fonde le présent règlement, analysé les coûts et avantages potentiels des normes proposées et sollicité l'avis du groupe des parties intéressées au secteur bancaire institué par l'article 37 du règlement (UE) nº 1093/2010, du groupe des parties intéressées à l'assurance et la réassurance et du groupe des parties intéressées aux pensions professionnelles institués par l'article 37 du règlement (UE) nº 1094/2010, ainsi que du groupe des parties intéressées au secteur financier institué par l'article 37 du règlement (UE) nº 1095/2010,

(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 24 janvier 2024,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier
Profil de risque global et complexité

La politique relative à l'utilisation de services TIC soutenant des fonctions critiques ou importantes qui sont fournis par des prestataires tiers de services TIC (ci-après la «politique»)

---

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).

tient compte de la taille et du profil de risque global de l'entité financière, ainsi que de la nature, de l'échelle et des facteurs d'augmentation ou de diminution de la complexité de ses services, activités et opérations, y compris des éléments suivants:

(a) le type de services TIC inclus dans chaque accord contractuel sur l'utilisation de services TIC soutenant des fonctions critiques ou importantes (ci-après l'«accord contractuel») conclu entre l'entité financière et un prestataire tiers de services TIC;

(b) la situation géographique du prestataire tiers de services TIC ou celle de son entreprise mère;

(c) si les services TIC soutenant des fonctions critiques ou importantes sont fournis par un prestataire tiers de services TIC situé dans un État membre ou dans un pays tiers, compte tenu également du lieu à partir duquel les services TIC sont fournis et du lieu où les données sont traitées et stockées;

(d) la nature des données partagées avec le prestataire tiers de services TIC;

(e) si le prestataire tiers de services TIC fait partie du même groupe que l'entité financière à laquelle les services sont fournis;

(f) le recours à des prestataires tiers de services TIC qui sont agréés, immatriculés ou soumis à la surveillance ou à la supervision d'une autorité compétente d'un État membre ou qui sont assujettis au cadre de supervision prévu au chapitre V, section II, du règlement (UE) 2022/2554, et le recours à des prestataires tiers de services TIC qui ne le sont pas;

(g) le recours à des prestataires tiers de services TIC qui sont agréés, immatriculés ou soumis à la surveillance ou à la supervision d'une autorité compétente d'un pays tiers, et le recours à des prestataires tiers de services TIC qui ne le sont pas;

(h) si la fourniture des services TIC soutenant des fonctions critiques ou importantes est concentrée chez un seul prestataire tiers de services TIC ou un petit nombre de tels prestataires;

(i) la transférabilité des services TIC soutenant des fonctions critiques ou importantes à un autre prestataire tiers de services TIC, y compris du fait de spécificités technologiques;

(j) l'impact potentiel de perturbations dans la fourniture des services TIC soutenant des fonctions critiques ou importantes sur la continuité des activités de l'entité financière et sur la disponibilité de ses services.

Article 2
Application à l'échelle d'un groupe

Lorsque le présent règlement s'applique sur une base consolidée ou sous-consolidée, l'entreprise mère chargée de fournir les états financiers consolidés ou sous-consolidés pour le groupe veille à ce que la politique soit mise en œuvre de manière cohérente dans toutes les entités financières faisant partie du groupe et à ce qu'elle soit adaptée à l'application effective du présent règlement à tous les niveaux pertinents du groupe.

Article 3
Dispositifs de gouvernance

1. L'organe de direction réexamine la politique au moins une fois par an et l'actualise si nécessaire. Les modifications apportées à la politique sont mises en œuvre en temps

utile, et dès que possible, dans le cadre des accords contractuels concernés. L'entité financière documente le calendrier prévu pour la mise en œuvre.

2. La politique établit ou fait référence à une méthode permettant de déterminer quels services TIC soutiennent des fonctions critiques ou importantes. La politique précise également quand cette évaluation doit être effectuée et réexaminée.

3. La politique attribue clairement les responsabilités internes en matière d'approbation, de gestion, de contrôle et de documentation des accords contractuels concernés et garantit le maintien, au sein de l'entité financière, des compétences, de l'expérience et des connaissances nécessaires à une supervision effective de ces accords, y compris des services TIC fournis conformément à ceux-ci.

4. Sans préjudice de la responsabilité finale de l'entité financière de superviser effectivement les accords contractuels conclus, la politique exige une évaluation du prestataire tiers de services TIC attestant qu'il dispose de ressources suffisantes pour garantir que l'entité financière respecte toutes les exigences légales et réglementaires lui incombant quant aux services TIC qui lui sont fournis à l'appui de fonctions critiques ou importantes.

5. La politique indique clairement à quel rôle ou à quel membre de la direction générale incombe la responsabilité de suivre le respect des accords contractuels conclus. La politique précise comment s'exerce la coopération entre ce rôle ou ce membre de la direction générale et les fonctions de contrôle, à moins qu'il n'en fasse partie, et elle indique les lignes hiérarchiques à respecter pour faire rapport à l'organe de direction, notamment la nature des informations et les documents à lui fournir. Elle précise également la fréquence ce reporting.

6. La politique garantit la cohérence des accords contractuels avec les éléments suivants:

   (a) le cadre de gestion du risque lié aux TIC prévu par l'article 6 du règlement (UE) 2022/2554;

   (b) la politique de sécurité de l'information prévue par l'article 9, paragraphe 4, du règlement (UE) 2022/2554:

   (c) la politique de continuité des activités de TIC prévue par l'article 11 du règlement (UE) 2022/2554;

   (d) les exigences en matière de déclaration des incidents liés aux TIC prévues par l'article 19 du règlement (UE) 2022/2554.

7. La politique exige que les services TIC fournis par des prestataires tiers de services TIC à l'appui de fonctions critiques ou importantes fassent l'objet d'un examen indépendant et soient inclus dans le plan d'audit.

8. La politique précise explicitement que les accords contractuels:

   (a) ne dispensent pas l'entité financière, ni son organe de direction, des obligations réglementaires de l'entité financière et de ses responsabilités à l'égard de ses clients;

   (b) ne doivent pas empêcher la surveillance effective de l'entité financière et ne doivent enfreindre aucune restriction de services ou d'activités imposée par les autorités de surveillance;

(c) doivent imposer aux prestataires tiers de services TIC de coopérer avec les autorités compétentes;

(d) doivent exiger que l'entité financière, ses auditeurs et les autorités compétentes aient effectivement accès aux données et aux locaux en lien avec l'utilisation de services TIC soutenant des fonctions critiques ou importantes.

Article 4

Principales phases du cycle de vie pour l'adoption et l'utilisation d'accords contractuels

La politique précise les exigences, notamment les règles, les responsabilités et les processus, à respecter à chacune des phases principales du cycle de vie d'un accord contractuel, ces exigences couvrant au moins les éléments suivants:

(a) les responsabilités de l'organe de direction, y compris sa participation, en tant que de besoin, au processus décisionnel relatif à l'utilisation de services TIC fournis par des prestataires tiers de services TIC pour soutenir des fonctions critiques ou importantes;

(b) la planification des accords contractuels, y compris l'évaluation des risques, la diligence raisonnable prévue aux articles 5 et 6 et la procédure d'approbation des nouveaux accords contractuels ou des modifications importantes d'accords contractuels existants prévue à l'article 8, paragraphe 4;

(c) le rôle des unités opérationnelles, des contrôles internes et d'autres unités pertinentes dans l'exécution des accords contractuels;

(d) la mise en œuvre, le suivi et la gestion, conformément aux articles 7, 8 et 9, des accords contractuels, y compris, s'il y a lieu, aux niveaux consolidé et sous-consolidé;

(e) la documentation et la tenue de registres, compte tenu des exigences définies à l'article 28, paragraphe 3, du règlement (UE) 2022/2554 en ce qui concerne le registre d'informations;

(f) les stratégies de sortie et les processus de résiliation prévus à l'article 10.

Article 5

Évaluation ex ante des risques

1. La politique exige que les besoins métiers de l'entité financière soient définis avant la conclusion de tout accord contractuel.

2. La politique exige qu'une évaluation des risques soit effectuée au niveau de l'entité financière et, s'il y a lieu, aux niveaux consolidé et sous-consolidé, avant la conclusion de tout accord contractuel.

L'évaluation des risques tient compte de toutes les exigences pertinentes énoncées dans le règlement (UE) 2022/2554 et dans la législation sectorielle de l'Union applicable. Elle tient compte, en particulier, des incidences que peut avoir sur l'entité financière la fourniture de services TIC soutenant des fonctions critiques ou importantes par des prestataires tiers de tels services, et de tous les risques liés à cette fourniture, qui incluent:

(a) les risques opérationnels;

(b) les risques juridiques;

(c) les risques liés aux TIC;

(d) les risques réputationnels;

(e) les risques liés à la protection de données confidentielles ou à caractère personnel;

(f) les risques liés à la disponibilité des données;

(g) les risques liés au lieu où les données sont traitées et stockées;

(h) les risques liés à la situation géographique du prestataire tiers de services TIC;

(i) les risques de concentration de TIC au niveau de l'entité.

Article 6
Diligence raisonnable

1. La politique définit un processus approprié et proportionné de sélection et d'évaluation des prestataires tiers potentiels de services TIC, en tenant compte de leur appartenance ou non au groupe, et exige qu'avant de conclure un accord contractuel, l'entité financière vérifie si le prestataire tiers de services TIC:

(a) dispose d'une réputation, de capacités, d'une expertise, de ressources financières, humaines et techniques et de normes de sécurité de l'information suffisantes, ainsi que d'une structure organisationnelle, d'une gestion des risques et de contrôles internes appropriés et, s'il y a lieu, du ou des agréments ou immatriculations requis pour fournir de manière fiable et professionnelle les services TIC destinés à soutenir la fonction critique ou importante concernée;

(b) est capable de suivre les évolutions technologiques pertinentes et d'identifier et de mettre en œuvre, le cas échéant, les pratiques de pointe en matière de sécurité des TIC, afin d'obtenir un cadre solide et performant de résilience opérationnelle numérique;

(c) recourt ou a l'intention de recourir à des sous-traitants de services TIC pour fournir les services TIC destinés à soutenir des fonctions critiques ou importantes ou des parties importantes de celles-ci;

(d) est situé dans un pays tiers, ou traite ou stocke les données dans un pays tiers et, dans ce cas, si cette pratique augmente le niveau des risques opérationnels ou réputationnels ou le risque d'être affecté par des mesures restrictives, y compris par des embargos et des sanctions, pouvant avoir un impact sur la capacité du prestataire tiers de services TIC à fournir les services TIC visés, ou la capacité de l'entité financière à bénéficier de ces derniers;

(e) consent à la conclusion d'accords contractuels garantissant qu'il est effectivement possible que des audits soient effectués en son sein, y compris sur place, par l'entité financière elle-même, par des tiers désignés à cet effet et par les autorités compétentes;

(f) agit de manière éthique et socialement responsable, respecte les droits de l'homme et les droits de l'enfant, y compris l'interdiction du travail des enfants, et les principes applicables en matière de protection de l'environnement, et garantit des conditions de travail appropriées.

2. La politique précise le niveau d'assurance requis en ce qui concerne l'efficacité du cadre de gestion des risques liés aux prestataires tiers de services TIC pour les

services TIC que fournit un prestataire tiers de tels services à l'appui de fonctions critiques ou importantes. La politique exige que le processus de diligence raisonnable comprenne une vérification de l'existence, chez le prestataire tiers de services TIC, de mesures d'atténuation des risques et de continuité des activités, et de la manière dont leur fonctionnement en son sein est garanti.

3. La politique définit le processus de diligence raisonnable à appliquer pour sélectionner et évaluer les prestataires tiers potentiels de services TIC et indique quels éléments, parmi les suivants, doivent être utilisés pour le niveau d'assurance requis en ce qui concerne les performances d'un prestataire tiers de services TIC:

   (a) audits ou évaluations indépendantes effectués par l'entité financière elle-même ou pour son compte;

   (b) utilisation de rapports d'audit indépendants établis à la demande du prestataire tiers de services TIC;

   (c) utilisation de rapports d'audit établis par la fonction d'audit interne du prestataire tiers de services TIC;

   (d) utilisation de certifications de tiers appropriées;

   (e) utilisation d'autres informations pertinentes dont dispose l'entité financière ou d'autres informations fournies par le prestataire tiers de services TIC.

4. Les entités financières veillent à ce que les performances du prestataire tiers de services TIC soient soumises à un niveau d'assurance approprié, tenant compte des éléments énumérés au paragraphe 3, points a) à e). S'il y a lieu, plusieurs des éléments énumérés sous ces points sont utilisés.

Article 7
Conflits d'intérêts

1. La politique précise les mesures appropriées de détection, de prévention et de gestion des conflits d'intérêts réels ou potentiels découlant du recours à des prestataires tiers de services TIC qui doivent être prises avant la conclusion de tout accord contractuel en la matière, et elle prévoit un suivi permanent de ces conflits d'intérêts.

2. Lorsque des services TIC soutenant des fonctions critiques ou importantes sont fournis par des prestataires de services TIC intragroupe, la politique précise que les décisions relatives aux conditions, y compris financières, régissant ces services doivent être prises de manière objective.

Article 8
Clauses contractuelles

1. La politique précise que les accords contractuels doivent être écrits et inclure tous les éléments visés à l'article 30, paragraphes 2 et 3, du règlement (UE) 2022/2554. La politique inclut aussi des éléments portant sur les exigences visées à l'article 1er, paragraphe 1, point a), du règlement (UE) 2022/2554 et, le cas échéant, sur d'autres dispositions pertinentes du droit de l'Union et du droit national.

2. La politique précise que les accords contractuels doivent prévoir le droit pour l'entité financière d'accéder à des informations, de procéder à des inspections et des audits, et d'effectuer des tests portant sur les TIC. À cette fin, la politique exige que l'entité financière utilise les méthodes suivantes, sans préjudice de sa responsabilité ultime:

(a) son propre audit interne ou un audit effectué par un tiers désigné;

(b) lorsque cela est approprié, des audits groupés et des tests groupés de TIC, y compris des tests de pénétration fondés sur la menace, organisés conjointement avec d'autres entités financières ou entreprises contractantes qui utilisent des services TIC du même prestataire tiers de services TIC, et effectués par ces entités financières ou entreprises contractantes ou par un tiers désigné par elles;

(c) lorsque cela est approprié, des certifications délivrées par des tiers;

(d) lorsque cela est approprié, des rapports d'audit internes ou de tiers fournis par le prestataire tiers de services TIC

3. L'entité financière ne peut indéfiniment s'appuyer uniquement sur les certifications visées au paragraphe 2, point c), ou sur les rapports d'audit visés au point d) du même paragraphe. La politique n'autorise l'utilisation des méthodes visées au paragraphe 2, points c) et d), que lorsque l'entité financière:

(a) est convaincue par le plan d'audit du prestataire tiers de services TIC pour les accords contractuels concernés;

(b) s'assure que les certifications ou rapports d'audit couvrent les systèmes et contrôles clés indiqués par elle, et veille au respect des exigences réglementaires applicables;

(c) évalue en permanence et de manière approfondie le contenu des certifications ou des rapports d'audit et vérifie que ces rapports ou certifications ne sont pas obsolètes;

(d) veille à ce que les systèmes et contrôles clés soient couverts par les futures versions des certifications ou rapports d'audit;

(e) est convaincue des aptitudes du tiers qui délivre la certification ou effectue l'audit;

(f) a la conviction que les certifications sont délivrées, et les audits effectués, dans le respect de normes professionnelles pertinentes largement reconnues, et qu'ils comportent un test de l'efficacité opérationnelle des contrôles clés mis en place;

(g) a le droit contractuel de demander, à une fréquence raisonnable et légitime du point de vue de la gestion des risques, que les certifications ou rapports d'audit soient modifiés de manière à englober d'autres systèmes et contrôles pertinents;

(h) a le droit contractuel d'effectuer à sa discrétion des audits individuels et groupés relatifs aux accords contractuels, et d'exercer ce droit selon la fréquence convenue.

4. La politique garantit que toute modification importante apportée à un accord contractuel sera formalisée dans un document écrit, daté et signé par toutes les parties, et elle précise la procédure de reconduction des accords contractuels.

Article 9
Suivi des accords contractuels

1. La politique exige que les accords contractuels précisent les mesures et les indicateurs clés qui doivent permettre de suivre en permanence les performances des

prestataires tiers de services TIC, notamment les mesures de contrôle du respect des exigences relatives à la confidentialité, la disponibilité, l'intégrité et l'authenticité des données et des informations, ainsi que le respect, par ces prestataires, des politiques et procédures de l'entité financière en la matière. La politique précise aussi les mesures qui s'appliquent en cas de manquement à des accords sur le niveau de service, y compris, le cas échéant, les pénalités contractuelles applicables.

2. La politique précise comment l'entité financière doit évaluer si les prestataires tiers de services TIC auxquels il est fait appel pour des services TIC soutenant des fonctions critiques ou importantes respectent des normes de performance et de qualité appropriées correspondant à l'accord contractuel et à ses propres politiques. La politique garantit en particulier:

   (a) que les prestataires tiers de services TIC fourniront à l'entité financière des rapports appropriés sur leurs activités et services, notamment des rapports périodiques, des rapports d'incidents, des rapports sur les services fournis, des rapports sur la sécurité des TIC et des rapports sur les mesures et tests de continuité des activités;

   (b) que les performances des prestataires tiers de services TIC seront évaluées à l'aide d'indicateurs de performance clés, d'indicateurs de contrôle clés, d'audits, d'auto-certifications et d'examens indépendants conformes au cadre de gestion des risques liés aux TIC de l'entité financière;

   (c) que les prestataires tiers de services TIC communiqueront à l'entité financière toute autre information pertinente;

   (d) que les incidents liés aux TIC et les incidents opérationnels ou liés à la sécurité des paiements seront notifiés à l'entité financière lorsque cela est approprié;

   (e) qu'un examen indépendant et des audits indépendants seront effectués pour vérifier le respect des exigences et politiques légales et réglementaires.

3. La politique précise que l'évaluation visée au paragraphe 2 doit être documentée et ses résultats utilisés pour actualiser l'évaluation des risques de l'entité financière prévue par l'article 6.

4. La politique définit les mesures appropriées que l'entité financière doit prendre si elle constate, chez des prestataires tiers de services TIC, des lacunes, notamment des incidents liés aux TIC et des incidents opérationnels ou liés à la sécurité des paiements, dans la prestation de services TIC soutenant des fonctions critiques ou importantes ou dans le respect d'accords contractuels ou d'exigences légales. Elle précise aussi comment il convient de suivre la mise en œuvre de ces mesures afin qu'elles soient effectivement respectées dans un délai déterminé, tenant compte de l'importance des lacunes constatées.

Article 10
Sortie et résiliation d'accords contractuels

La politique exige que chaque accord contractuel s'accompagne d'un plan de sortie documenté et que ce plan soit régulièrement réexaminé et testé. Il est tenu compte, lors de l'établissement de ce plan de sortie, des éléments suivants:

(a) interruptions de service imprévues et persistantes;

(b) prestation de services défaillante ou inadaptée;

(c) résiliation imprévue de l'accord contractuel.

Le plan de sortie est réaliste, applicable, fondé sur des scénarios plausibles et des hypothèses raisonnables et comporte un calendrier prévisionnel de mise en œuvre compatible avec les conditions de sortie et de résiliation définies dans l'accord contractuel.

Article 11
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 13.3.2024

Par la Commission
La présidente
Ursula VON DER LEYEN