

RÈGLEMENT SUR LA RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE (UE) 2022/2554 (« DORA »)

DISPOSITIONS CONTRACTUELLES

SUPPLÉMENT 1 – Services de TIC non critiques

Le règlement sur la résilience opérationnelle numérique (UE) 2022/2554 (« DORA ») est une loi de l'UE qui est entrée en vigueur le 16 janvier 2024 et qui s'appliquera à compter du 17 janvier 2025. DORA affectera les services de TIC dont Tower Research Capital B.V. (TRCE BV) bénéficie. Si vous, en tant que fournisseur (le « fournisseur »), fournissez au groupe dans lequel TRCE BV repose des « services TIC » (comme définis dans le DORA) qui ne prennent pas en charge des « fonctions critiques ou importantes » (comme définies dans le DORA), à moins d'en avoir convenu séparément par écrit avec vous, ce supplément s'appliquera. Ce supplément (le « supplément ») vise uniquement à inclure les modalités contractuelles mandatées par le DORA dans l'entente (l'« entente ») que vous avez convenue directement avec TRCE BV ou que vous avez acceptée auprès d'une société affiliée de TRCE BV (ci-après appelée « Tower » ou votre « client »), mais qui profite à TRCE BV. Toutes les autres dispositions contractuelles de l'entente demeurent inchangées. En cas de conflit entre les modalités de l'entente et celles du présent supplément, les modalités de ce supplément ont préséance. À moins que vous n'avisiez Tower autrement par écrit, en continuant de fournir des services à Tower, vous êtes réputé avoir accepté les modalités du présent supplément.

Les termes non définis dans le présent supplément ont le sens qui leur est donné dans le DORA ou dans l'entente.

PAR CONSÉQUENT, les parties conviennent de compléter l'entente avec les dispositions suivantes pour être en vigueur, sauf indication contraire, le 1^{er} janvier 2025 :

1. Descriptions des services et surveillance du rendement

1.1. Les parties conviennent que :

- a) l'entente définit les fonctions, les services et les niveaux de service (les « services ») qui seront fournis par le fournisseur au client;
- b) les services seront fournis à l'échelle mondiale et les données du client seront traitées à l'échelle mondiale et stockées dans divers endroits, notamment l'Union européenne, le Royaume-Uni et les États-Unis d'Amérique. Le fournisseur doit aviser le client s'il envisage des changements d'emplacement pour les services ou si les données seront traitées ou stockées ailleurs.

1.2. Le fournisseur accepte les exigences suivantes :

- a) le fournisseur doit assurer la protection, la disponibilité, l'authenticité, l'intégrité et la confidentialité des données personnelles et non personnelles du client, conformément à toutes les lois et réglementations applicables (y compris les lois et règlements sur la confidentialité des données) et aux conditions de l'entente;

- b) en cas d'insolvabilité, de résolution ou d'interruption des activités commerciales du fournisseur, ou en cas de résiliation de l'entente, le fournisseur veillera à ce que tous les renseignements personnels et non personnels du client soient accessibles, récupérés et retournés par le fournisseur, dans un format facilement accessible;
- c) lorsqu'un incident lié aux TIC se produit, en lien avec le service fourni au client, le fournisseur s'engage à fournir toute l'assistance raisonnable au client, sans frais supplémentaires ou à un coût déterminé à l'avance;
- d) si le client est soumis à toute enquête ou intervention par ses autorités compétentes ou des autorités de résolution, le fournisseur s'engage par les présentes à collaborer pleinement avec les autorités compétentes ou les autorités de résolution du client, y compris les personnes désignées par le client; et
- e) le fournisseur se conformera à toute demande raisonnable de participation aux programmes de sensibilisation à la sécurité des TIC du client et à la formation sur la résilience opérationnelle numérique, le cas échéant.

2. Résiliation

2.1. Nonobstant les dispositions de résiliation contenues dans l'entente, le client peut résilier l'entente pertinente en vigueur immédiatement dans l'une des circonstances suivantes :

- a) en cas de violation importante par le fournisseur de toute loi ou réglementation applicable ou en cas de violation importante des modalités de l'entente;
- b) dans le cas où certaines circonstances ont été repérées par la surveillance du risque de tiers et où ces circonstances sont jugées aptes à modifier l'exécution des fonctions fournies par le fournisseur dans les ententes et le présent supplément, y compris les changements importants qui pourraient avoir une incidence sur l'entente avec le fournisseur ou sur la situation du fournisseur;
- c) des faiblesses démontrées par le fournisseur relativement à sa gestion globale des risques liés aux TIC et, en particulier, à sa façon d'assurer la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, qu'elles soient personnelles ou autrement sensibles ou non personnelles; ou
- d) lorsque l'autorité compétente ne peut plus superviser le client de manière efficace en raison des conditions ou des circonstances liées à l'entente contractuelle ou à l'entente.

2.2. Lorsque le client est mandaté par une autorité compétente ou une autorité de résolution de résilier une entente, cette entente peut être résiliée par le client sur préavis écrit de 90 jours, à moins qu'une période de préavis plus courte ne s'applique ou soit exigée par une autorité compétente ou une autorité de règlement.

3. Divers

3.1. L'entente, ses amendements, ses annexes et le présent supplément constituent l'intégralité de l'entente entre les parties.

3.2. Les lois régissant l'entente régissent également les modalités complétées par le présent supplément et les tribunaux précisés dans l'entente ont également compétence sur les modalités complétées par le présent supplément.

3.3. Chaque partie assume ses propres coûts et responsabilités relativement au présent supplément et à sa mise en œuvre.

RÈGLEMENT SUR LA RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE (UE) 2022/2554 (« DORA ») DISPOSITIONS CONTRACTUELLES

SUPPLÉMENT 2 – Services de TIC critiques

Le règlement sur la résilience opérationnelle numérique (UE) 2022/2554 (« **DORA** ») est une loi de l'UE qui est entrée en vigueur le 16 janvier 2024 et qui s'appliquera à compter du 17 janvier 2025. DORA affectera les services de TIC dont Tower Research Capital B.V. (**TRCE BV**) bénéficie. Si vous, en tant que fournisseur (le « **fournisseur** »), fournissez au groupe dans lequel TRCE BV repose des « services TIC » (comme définis dans le DORA) qui prennent en charge des « fonctions critiques ou importantes » (comme définies dans le DORA), à moins d'en avoir convenu séparément par écrit avec vous, ce supplément s'appliquera. Ce supplément (le « **supplément** ») vise uniquement à inclure les modalités contractuelles mandatées par le DORA dans l'entente (l'« **entente** ») que vous avez convenue directement avec TRCE BV ou que vous avez acceptée auprès d'une société affiliée de TRCE BV (ci-après appelée « **Tower** » ou votre « **client** »), mais qui profite à TRCE BV. Toutes les autres dispositions contractuelles de l'entente demeurent inchangées. En cas de conflit entre les modalités de l'entente et celles du présent supplément, les modalités de ce supplément ont préséance. À moins que vous n'avisiez Tower autrement par écrit, en continuant de fournir des services à Tower, vous êtes réputé avoir accepté les modalités du présent supplément.

Les termes non définis dans le présent supplément ont le sens qui leur est donné dans le DORA ou dans l'entente.

PAR CONSÉQUENT, les parties conviennent de compléter l'entente avec les dispositions suivantes pour être en vigueur, sauf indication contraire, le 1^{er} janvier 2025 :

Descriptions des services et surveillance du rendement

1.1. Les parties conviennent que :

1.1.1. l'entente définit les fonctions, les services et les niveaux de service (les « **services** ») qui seront fournis par le fournisseur au client;

1.1.2. la sous-traitance est autorisée. Les conditions de la sous-traitance sont énoncées ci-dessous;

1.1.3. les services seront fournis à l'échelle mondiale et les données du client seront traitées à l'échelle mondiale et stockées dans divers endroits, notamment l'Union européenne, le Royaume-Uni et les États-Unis d'Amérique;

1.1.4. les niveaux de service et les objectifs de rendement actuels sont reflétés dans l'entente.

1.2. Le fournisseur s'engage par les présentes à :

- 1.2.1. aviser le client s'il envisage des changements d'emplacement pour les services ou si les données seront traitées ou stockées ailleurs;
- 1.2.2. aviser le client de tout développement qui pourrait avoir une incidence importante sur la capacité du fournisseur à fournir les services de manière efficace conformément aux niveaux de service convenus;
- 1.2.3. si les niveaux de service convenus ne sont pas respectés, prendre les mesures correctives appropriées selon les instructions du client, sans délai excessif.

2. Sous-traitance

2.1. Pour chaque service sous-traité admissible, le fournisseur a accepté ce qui suit et s'y engage :

- 2.1.1. être responsable de la prestation des services fournis par les sous-traitants;
- 2.1.2. surveiller tous les services sous-traités pour s'assurer que ses obligations contractuelles sont respectées en permanence;
- 2.1.3. surveiller le rendement de tous les sous-traitants et transmettre périodiquement les résultats d'une telle surveillance au client;
- 2.1.4. évaluer tous les risques associés à l'emplacement des sous-traitants actuels ou potentiels et de leur société mère, ainsi que l'emplacement de la prestation du service et l'emplacement des données traitées ou stockées par le sous-traitant, le cas échéant;
- 2.1.5. préciser dans son entente contractuelle écrite avec le sous-traitant les obligations de surveillance et de déclaration du sous-traitant envers le fournisseur, et lorsque convenu, envers le client;
- 2.1.6. s'assurer de la continuité des services sous-traités dans l'ensemble de la chaîne de sous-traitants en cas de défaut par un sous-traitant de respecter ses obligations contractuelles, et il doit avoir conclu une entente contractuelle avec le sous-traitant selon laquelle le sous-traitant met en œuvre des plans opérationnels d'urgence au moins à la norme définie par la réglementation européenne et cette entente doit définir les niveaux de service à respecter par le sous-traitant relativement à ces plans;
- 2.1.7. dans son entente contractuelle écrite avec le sous-traitant, il énonce les normes de sécurité des TIC et toute exigence de sécurité supplémentaire, le cas échéant, qui doivent être respectées par les sous-traitants conformément à la réglementation européenne pertinente;
- 2.1.8. s'assurer que le sous-traitant est tenu d'accorder au client et aux autorités compétentes et pertinentes en matière de résolution les mêmes droits d'accès, d'inspection et de vérification accordés au client et aux autorités compétentes et pertinentes en matière de résolution par le fournisseur; et
- 2.1.9. aviser le client des changements importants apportés aux ententes de sous-traitance.

2.2. Lorsque le fournisseur est autorisé à sous-traiter le contrat, il en informera le client dès que possible de la chaîne de sous-traitance des TIC et s'assurera qu'elle demeure à jour au fil du temps.

2.3. Le fournisseur doit surveiller les risques liés au rendement et aux TIC présentés par tout sous-traitant et faire rapport périodiquement au client de ces risques. Ces rapports doivent comprendre la divulgation des renseignements sur les indicateurs de rendement clés, le cas échéant, au client.

2.4. Le fournisseur signalera au client, au moyen d'un avis écrit, tout changement important apporté à ses ententes de sous-traitance dans les 60 jours suivant la prise de connaissance de ces

changements. Le fournisseur convient que les modifications importantes apportées à la sous-traitance ne peuvent être mises en œuvre qu'après réception du consentement ou d'aucune objection à ces modifications de la part du client.

2.5. Si le client, à la suite de son évaluation des risques internes des modifications importantes proposées à la sous-traitance qui lui sont communiquées conformément à l'article 2.4 ci-dessus, détermine que les modifications proposées ne sont pas acceptables, le client peut s'opposer aux modifications et demander des modifications aux modifications proposées, et le fournisseur accepte de prendre des mesures raisonnables pour mettre en œuvre ces modifications avec le sous-traitant et, dans la mesure où il ne peut pas le faire, il mettra fin à l'entente de sous-traitance.

3. Protection et résilience

3.1. Le fournisseur assurera la protection, la disponibilité, l'authenticité, l'intégrité et la confidentialité des données personnelles et non personnelles du client, conformément à toutes les lois et réglementations applicables sur la confidentialité des données.

3.2. Le fournisseur déclare et garantit qu'il a ou qu'il s'engage à mettre en œuvre et à mettre à l'essai des plans opérationnels d'urgence et qu'il a mis en place des mesures, des outils et des politiques de sécurité des TIC à un niveau approprié pour permettre au client de fonctionner dans le cadre réglementaire.

3.3. En cas d'insolvabilité, de résolution ou d'interruption des activités commerciales du fournisseur, ou en cas de résiliation de l'entente, le fournisseur veillera à ce que tous les renseignements personnels et non personnels du client soient accessibles, récupérés et retournés par le fournisseur, dans un format facilement accessible.

3.4. Lorsqu'un incident lié aux TIC se produit, en lien avec le service fourni au client, le fournisseur s'engage à fournir une assistance au client, sans frais supplémentaires ou à un coût déterminé à l'avance.

3.5. Lorsque le client est tenu d'effectuer un test d'intrusion de menace, le fournisseur participera et collaborera pleinement à ces tests sur avis raisonnable au fournisseur.

3.6. Le fournisseur doit se conformer à toute demande raisonnable de participation aux programmes de sensibilisation à la sécurité des TIC du client et à la formation sur la résilience opérationnelle numérique, le cas échéant.

4. Droits de surveillance et de vérification

4.1. Le fournisseur autorise le client à surveiller le rendement du fournisseur sur une base continue, et accepte ce qui suit et s'y engage :

4.1.1. accorder des droits d'accès, d'inspection et de vérification sans restriction au client ou à une autorité compétente (y compris un superviseur principal) ou à un tiers raisonnablement nommé par le client, une autorité compétente ou un superviseur principal;

4.1.2. fournir à toute personne mentionnée ci-dessus le droit de faire des copies de la documentation pertinente dans ses locaux, si elle est essentielle aux activités du fournisseur;

4.1.3. convenir avec le client d'autres niveaux d'assurance si d'autres clients des droits du fournisseur sont affectés; et

4.1.4. collaborer pleinement dans le cadre des inspections et des vérifications sur place effectuées par les autorités compétentes, le superviseur principal, le client ou un tiers désigné.

4.2. Les parties s'engagent à agir de bonne foi dans l'octroi et l'exercice des droits prévus à l'article 5.1 ci-dessus.

4.3. Le client doit fournir un avis raisonnable avant d'effectuer une vérification ou une inspection et doit effectuer sa vérification dans les heures normales d'ouverture.

4.4. L'exercice efficace de ces droits ne peut être entravé ou limité par d'autres ententes contractuelles ou politiques de mise en œuvre. Les parties conviennent de la portée, des procédures à suivre et de la fréquence de ces inspections et vérifications.

4.5. En ce qui concerne les droits d'accès à l'information, d'inspection, de vérification et de tests des TIC décrits à l'article 4.1 ci-dessus, le client utilisera, dans la mesure du possible, les éléments suivants :

4.5.1. sa propre équipe de vérification interne ou un tiers désigné;

4.5.2. s'il y a lieu, des vérifications regroupées et des tests de TIC regroupés, y compris des tests d'intrusion de menace, organisés conjointement avec d'autres clients ou entreprises qui utilisent des services de TIC du même fournisseur, qui sont exécutés par eux ou par un tiers désigné par eux;

4.5.3. le cas échéant, les certifications de tiers; et

4.5.4. le cas échéant, des rapports de vérification interne ou de tiers mis à la disposition du fournisseur.

4.6. Le client doit utiliser les articles 4.5(c) et (d) ci-dessus au fil du temps seulement si le client :

4.6.1. est satisfait du plan de vérification du fournisseur pour les ententes contractuelles pertinentes;

4.6.2. s'assure que la portée des certifications ou des rapports d'audit couvre les systèmes et les contrôles clés précisés par l'entité financière et la conformité aux exigences réglementaires pertinentes;

4.6.3. évaluer en profondeur le contenu des certifications ou des rapports d'audit sur une base continue et vérifier que les rapports ou les certifications ne sont pas obsolètes;

4.6.4. s'assurer que les systèmes et contrôles clés sont couverts dans les versions futures du rapport de certification ou de vérification;

4.6.5. est satisfait des aptitudes de la partie effectuant la certification ou la vérification; et

4.6.6. est satisfait que les certifications sont émises et que les vérifications sont effectuées selon des normes professionnelles pertinentes largement reconnues et comprennent un test de l'efficacité opérationnelle des contrôles clés en place.

4.7. Le client peut demander l'élargissement de la portée des certifications ou des rapports de vérification à d'autres systèmes et contrôles pertinents; sous réserve du nombre et de la fréquence de la demande, cette demande doit être raisonnable et légitime du point de vue de la gestion des risques.

5. Collaboration avec les autorités compétentes

Si le client est soumis à toute enquête ou intervention par ses autorités compétentes ou des autorités de résolution, le fournisseur s'engage par les présentes à collaborer pleinement avec les autorités compétentes ou les autorités de résolution du client, y compris les personnes désignées par le client.

6. Résiliation

6.1. Nonobstant les dispositions de résiliation contenues dans l'entente, le client peut résilier l'entente pertinente en vigueur immédiatement dans l'une des circonstances suivantes : 6.1.1. en cas de violation importante des lois ou règlements applicables par le fournisseur ou en cas de violation importante des modalités de l'entente;

6.1.2. dans le cas où certaines circonstances ont été repérées par la surveillance du risque de tiers et où ces circonstances sont jugées aptes à modifier l'exécution des fonctions fournies par le fournisseur dans l'entente et le présent supplément, y compris les changements importants qui pourraient avoir une incidence sur l'entente avec le fournisseur ou sur la situation du fournisseur;

6.1.3. les faiblesses démontrées par le fournisseur relativement à sa gestion globale des risques liés aux TIC et, en particulier, à sa façon d'assurer la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, qu'elles soient personnelles ou autrement sensibles ou non personnelles;

6.1.4. lorsque l'autorité compétente ne peut plus superviser le client de manière efficace en raison des conditions ou des circonstances liées à l'entente contractuelle ou à l'entente;

6.1.5. lorsque le fournisseur met en œuvre des changements importants aux ententes de sous-traitance, malgré l'objection du client, ou sans approbation ou réception d'une confirmation d'aucune objection au cours de la période de préavis; ou

6.1.6. lorsque le fournisseur sous-traite un service qui est explicitement interdit d'être sous-traité en vertu de l'entente.

6.2. Lorsque le client est mandaté par une autorité compétente ou une autorité de résolution de résilier une entente, cette entente peut être résiliée par le client sur préavis écrit de 90 jours, à moins qu'une période de préavis plus courte ne s'applique ou soit exigée par une autorité compétente ou une autorité de règlement.

6.3. À la résiliation anticipée, à la demande du client ou de son représentant, le fournisseur :

6.3.1. continuera à fournir les services, en vue de réduire le risque de perturbation pour le client ou d'assurer sa résolution et sa restructuration efficaces; et

6.3.2. continuera à fournir des services pendant une période de transition pour permettre au client de migrer vers un autre fournisseur de services de TIC ou de passer à des solutions internes, conformément à la complexité du service fourni.

7. Divers

7.1. L'entente, ses amendements, ses annexes et le présent supplément constituent l'intégralité de l'entente entre les parties.

7.2. Les lois régissant l'entente régissent également les modalités complétées par le présent supplément et les tribunaux précisés dans l'entente ont également compétence sur les modalités complétées par le présent supplément.

7.3. Chaque partie assume ses propres coûts et responsabilités relativement au présent supplément et à sa mise en œuvre.