DIGITAL AND OPERATIONAL RESILIENCE REGULATION (EU) 2022/2554 ("DORA")
CONTRACTUAL PROVISIONS

SUPPLEMENT 1 - Non-Critical ICT Services

The Digital and Operational Resilience Regulation (EU) 2022/2554 ("**DORA**") is an EU legislation that entered into force on 16 January 2024 and will apply as of 17 January 2025. DORA will affect ICT services which Tower Research Capital B.V. (**TRCE BV**) benefits from. Where you, as a vendor (the "**Vendor**"), provide the group in which TRCE BV sits with "ICT services" (as defined in DORA) that do not support "critical or important functions" (as defined in DORA), unless separately agreed with you in writing, this supplement will apply. This supplement (the "**Supplement**") solely aims to include the DORA mandated contractual terms into the agreement (the "**Agreement**") you have agreed either directly with TRCE BV or you have agreed with an affiliate of TRCE BV (hereinafter referred to as "**Tower**" or your "**Client**") but which benefits TRCE BV. All other contractual provisions in the Agreement will remain unaffected. Where there is any conflict between the terms of the Agreement and the terms of this Supplement, the terms of this Supplement shall take precedent. Unless you notify Tower otherwise in writing, by continuing to provide Tower with the services, you are deemed to accept the terms of this Supplement.

Capitalised terms used but not defined in this Supplement, shall have the meaning given to them in DORA or the Agreement.

NOW THEREFORE the Parties agree to supplement the Agreement with the following provisions to be effective, unless stated otherwise, on 1 January 2025:

1. Service Descriptions and Performance Monitoring

1.1. The Parties agree that:

a) the Agreement sets out the functions, services and service levels (the "**Services**") to be provided by the Vendor to the Client.

b) the Services will be provided globally and the Client's data will be processed globally and stored in various locations including the European Union, United Kingdom and United States of America. The Vendor shall notify the Client in advance if it envisages any location changes for the Services or where the data is processed and/or stored.

1.2. The Vendor agrees to the following requirements:

a) the Vendor shall ensure the protection, availability, authenticity, integrity and confidentiality of the Client's personal and non-personal data, in accordance with all applicable laws and regulations (including data privacy laws and regulations) and the terms of the Agreement.

b) in the event of insolvency, resolution or discontinuation of the business operations of the Vendor, or in the event of the termination of the Agreement, the Vendor will ensure proper access, recovery and return of all Client personal and non-personal data processed by the Vendor, in an easily accessible format;

c) when an ICT-Related Incident occurs, related to the Service provided to the Client, the Vendor undertakes to provide all reasonable assistance to the Client, at no additional cost or at a cost that is determined in advance;
d) in the event that the Client becomes subject to any type of enquiry or intervention by its competent authorities or resolution authorities, the Vendor hereby undertakes to fully cooperate with such competent authorities and/or resolution authorities of the Client, including persons appointed by them; and
e) the Vendor will comply with any reasonable request to participate in the Client's ICT security awareness programs and digital operational resilience training, where appropriate.

2. Termination

2.1. Notwithstanding the termination provisions contained in the Agreement, the Client may terminate the relevant Agreement with immediate effect in any of the following circumstances:

a) in the event that there is a significant breach by the Vendor of any applicable laws and/or regulations or if there is a material breach of the terms of the Agreement;
b) in the event that certain circumstances have been identified, through the monitoring of third-party risk, which circumstances are deemed capable of altering the performance of the functions provided by the Vendor in the Agreements and this Supplement, including material changes that may affect the arrangement with, or the situation of, the Vendor;
c) the Vendor's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality of data, whether personal or otherwise sensitive data, or non-personal data; or
d) where the competent authority can no longer effectively supervise the Client, due to the conditions of, or circumstances related to, the respective contractual arrangement and/or Agreement.

2.2. When the Client is mandated by a competent authority or resolution authority to terminate any Agreement, such Agreement may be terminated by Client upon 90 days' prior written notice unless a shorter notice period applies and/or is required by a competent authority or resolution authority.

3. Miscellaneous

3.1. The Agreement, it's amendments, annexes and this Supplement, constitute the entire agreement between the Parties.
3.2. The laws governing the Agreement also govern the terms supplemented by way of this Supplement and the courts identified in the Agreement also have jurisdiction over the terms supplemented by way of this Supplement.
3.3. Each Party bears its own costs, responsibilities and liabilities in respect of this Supplement and the implementation thereof.

DIGITAL AND OPERATIONAL RESILIENCE REGULATION (EU) 2022/2554 ("DORA")
CONTRACTUAL PROVISIONS

SUPPLEMENT 2 - Critical ICT Services

The Digital and Operational Resilience Regulation (EU) 2022/2554 ("**DORA**") is an EU legislation that entered into force on 16 January 2024 and will apply as of 17 January 2025. DORA will affect ICT services which Tower Research Capital B.V. (**TRCE BV**) benefits from. Where you, as a vendor (the "**Vendor**"), provide the group in which TRCE BV sits with "ICT services" (as defined in DORA) that support "critical or important functions" (as defined in DORA), unless separately agreed with you in writing, this supplement will apply. This supplement (the "**Supplement**") solely aims to include the DORA mandated contractual terms into the agreement (the "**Agreement**") you have agreed either directly with TRCE BV or you have agreed with an affiliate of TRCE BV (hereinafter referred to as "**Tower**" or your "**Client**") but which benefits TRCE BV. All other contractual provisions in the Agreement will remain unaffected. Where there is any conflict between the terms of the Agreement and the terms of this Supplement, the terms of this Supplement shall take precedent. Unless you notify Tower otherwise in writing, by continuing to provide Tower with the services, you are deemed to accept the terms of this Supplement.

Capitalised terms used but not defined in this Supplement, shall have the meaning given to them in DORA or the Agreement.

NOW THEREFORE the Parties agree to supplement the Agreement with the following provisions to be effective, unless stated otherwise, on 1 January 2025:

1. Service Descriptions and Performance Monitoring

1.1. The Parties agree that:

1.1.1. the Agreement sets out the functions, services and service levels (the "**Services**") to be provided by the Vendor to the Client.
1.1.2. subcontracting is permitted. The conditions for such subcontracting are set out below;
1.1.3. the Services will be provided globally and the Client's data will be processed globally and stored in various locations including the European Union, United Kingdom and United States of America; and
1.1.4. the current service levels and performance targets are reflected in the Agreement.

1.2. The Vendor hereby undertakes to:

1.2.1. notify the Client in advance if it envisages any location changes for the Services and/or location changes where the data is processed and/or stored;

1.2.2. notify the Client of any development that might have a material impact on the Vendor's ability to effectively provide the Services in line with agreed service levels; and

1.2.3. in the event that the agreed service levels are not met, take appropriate corrective actions upon the instruction from the Client, without undue delay.

2. Sub-contracting

2.1. For each eligible subcontracted Service, the Vendor agreed and undertakes to:

2.1.1. be responsible for the provision of the services provided by the subcontractors;

2.1.2. monitor all subcontracted Services to ensure that its contractual obligations are continuously met;

2.1.3. monitor the performance of all subcontractors and periodically report the outcomes of such monitoring to the Client;

2.1.4. assess all risks associated with the location of the current or potential subcontractors and its parent company and the location where the Service is provided from and the location of data processed or stored by the subcontractor, where relevant;

2.1.5. specify in its written contractual agreement with the subcontractor the monitoring and reporting obligations of the subcontractor towards the Vendor, and where agreed, towards the Client;

2.1.6. ensure the continuity of the subcontracted Services throughout the chain of subcontractors in case of failure by a subcontractor to meet its contractual obligations, and it shall have a contractual agreement with the subcontractor that the subcontractor implements business contingency plans to at least the standard defined by European regulation and such agreement shall define the service levels to be met by the subcontractor in relation to these plans;

2.1.7. in its written contractual agreement with the subcontractor it states the ICT security standards and any additional security requirements, where relevant, that shall be met by the subcontractors in line with relevant European regulation;

2.1.8. ensure that the subcontractor is required to grant to the Client and relevant competent and resolution authorities the same rights of access, inspection and audit granted to the Client and relevant competent and resolution authorities by the Vendor; and

2.1.9. notify the Client of material changes to subcontracting arrangements.

2.2. Where the Vendor is permitted to subcontract, it will inform the Client, as soon as reasonably practicable of the ICT subcontracting chain and ensure that it remains up to date over time.

2.3. The Vendor shall monitor the performance and ICT risks presented by any subcontractor and report periodically to the Client on those risks, such reporting shall involve sharing Key Performance Indicator information, where relevant, with the Client.

2.4. The Vendor will inform the Client, by means of written notice, of any material changes to its subcontracting arrangements within 60 day of becoming aware of these changes. The Vendor

agrees that the material changes to subcontracting may only be implemented following receipt of consent or no objection to those changes from the Client.

2.5. If the Client, following its internal risk assessment of the proposed material changes to subcontracting notified to it in accordance with Clause 2.4 above, determines that the proposed changes are not acceptable, the Client may object to the changes and request modifications to the proposed changes and the Vendor agrees to take reasonable endeavours to implement those changes with the subcontractor and, where it cannot, the Vendor shall terminate the subcontracting arrangement.

3. Protection and Resilience

3.1. The Vendor will ensure the protection, availability, authenticity, integrity and confidentiality of the Client's personal and non-personal data, in accordance with all applicable data privacy laws and regulations.

3.2. The Vendor represents and warrants that it has, or undertakes to, implement and test business contingency plans and to have in place ICT security measures, tools and policies at an appropriate level to allow the Client to operate within its regulatory framework.

3.3. In the event of insolvency, resolution or discontinuation of the business operations of the Vendor, or in the event of the termination of the Agreement, the Vendor will ensure proper access, recovery and return of all Client personal and non-personal data processed by the Vendor, in an easily accessible format.

3.4. When an ICT-Related Incident occurs, related to the Service provided to the Client, the Vendor undertakes to provide assistance to the Client, at no additional cost or at a cost that is determined in advance.

3.5. When the Client is required to perform a Threat-Led Penetration Test, the Vendor will participate and fully cooperate in such testing upon reasonable notice to the Vendor.

3.6. The Vendor shall comply with any reasonable request to participate in the Client's ICT security awareness programs and digital operational resilience training, where appropriate.

4. Monitoring and Audit Rights

4.1. The Vendor authorizes the Client to monitor the Vendor's performance on an ongoing basis and agrees and undertakes to:

4.1.1. grant unrestricted rights of access, inspection and audit to the Client, and/or a competent authority (including a Lead Overseer) and/or a third party reasonably appointed by the Client, a competent authority or Lead Overseer;

4.1.2. provide any of the persons mentioned above, the right to make copies of relevant documentation on its premises, if they are critical to the operations of the Vendor;

4.1.3. agree with the Client on alternative assurance levels if other clients of the Vendor's rights are affected; and

4.1.4. fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, Client or an appointed third party.

4.2. The Parties undertake to act in good faith in granting and exercising the rights set out in clause 5.1 above.

4.3. The Client will provide reasonable notice before performing an audit or inspection and shall conduct its audit within normal business hours.

4.4. The effective exercise of these rights may not be impeded or limited by other contractual arrangements or implementation policies. The Parties shall agree details as to the scope, procedures to be followed and frequency of such inspections and audits.

4.5. With respect to the information access, inspection, audit and ICT testing rights outlined in clause 4.1 above, the Client will, to the extent possible, use:

4.5.1. its own internal audit team or an appointed third party;

4.5.2. where appropriate, pooled audits and pooled ICT testing, including Threat Led Penetration Testing, organized jointly with other Clients or firms that use ICT services of the same Vendor, that are performed by them or by a third party appointed by them;

4.5.3. where appropriate, third-party certifications; and

4.5.4. where appropriate, third-party or internal audit reports made available by the Vendor.

4.6. The Client shall make use of Clauses 4.5(c) and (d) above, over time, only if the Client:

4.6.1. is satisfied with the audit plan of the Vendor for the relevant contractual arrangements;

4.6.2. ensures that the scope of the certifications or audit reports cover the systems and key controls identified by the financial entity and the compliance with relevant regulatory requirements;

4.6.3. thoroughly assesses the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;

4.6.4. ensures that key systems and controls are covered in future versions of the certification or audit report;

4.6.5. is satisfied with the aptitude of the certifying or auditing party; and

4.6.6. is satisfied that the certifications are issued, and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place.

4.7. The Client may request the expansion of the scope of the certifications or audit reports, to other relevant systems and controls; subject to the number and frequency of the request, shall be reasonable and legitimate from a risk management perspective.

5. Cooperation with Competent Authorities

In the event that the Client becomes subject to any type of enquiry or intervention by its competent authorities or resolution authorities, the Vendor hereby undertakes to fully cooperate with such competent authorities and/or resolution authorities of the Client, including persons appointed by them.

6. Termination

6.1. Notwithstanding the termination provisions contained in the Agreement, the Client may terminate the relevant Agreement with immediate effect in any of the following circumstances:

6.1.1. in the event that there is a significant breach by the Vendor of any applicable laws and/or regulations or if there is a material breach of the terms of the Agreement;

6.1.2. in the event that certain circumstances have been identified, through the monitoring of third-party risk, which circumstances are deemed capable of altering the performance of the functions provided by the Vendor in the Agreement and this Supplement, including material changes that may affect the arrangement with, or the situation of, the Vendor;

6.1.3. the Vendor's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality of data, whether personal or otherwise sensitive data, or non-personal data;

6.1.4. where the competent authority can no longer effectively supervise the Client, due to the conditions of, or circumstances related to, the respective contractual arrangement and/or Agreement;

6.1.5. when the Vendor implements material changes to subcontracting arrangements, despite the objection of the Client, or without approval or receipt of a no-objection confirmation within the notice period; or

6.1.6. when the Vendor subcontracts a Service, which is explicitly not permitted to be subcontracted in terms of the Agreement.

6.2. When the Client is mandated by a competent authority or resolution authority to terminate any Agreement, such Agreement may be terminated by Client upon 90 days' prior written notice unless a shorter notice period applies and/or is required by a competent authority or resolution authority.

6.3. Upon early termination, where requested by the Client or its representative, the Vendor will:

6.3.1. continue providing the services, with a view to reducing the risk of disruption for the Client or to ensure its effective resolution and restructuring; and

6.3.2. continue to provide services during a transition period to allow the Client to migrate to another ICT third-party service provider or change to in-house solutions, consistent with the complexity of the service provided.

7. Miscellaneous

7.1. The Agreement, it's amendments, annexes and this Supplement, constitute the entire agreement between the Parties.

7.2. The laws governing the Agreement also govern the terms supplemented by way of this Supplement and the courts identified in the Agreement also have jurisdiction over the terms supplemented by way of this Supplement.

7.3. Each Party bears its own costs, responsibilities and liabilities in respect of this Supplement and the implementation thereof.