Addendum DORA

1 Scope of application

This Addendum applies only if the Customer is subject to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (the “Regulation” or the “Regulation 2022/2554”) and qualifies as a “financial entity” under Article 2 of the Regulation. It forms an integral and substantive part of the General Terms and Conditions of Sale published in the Legal & Compliance section of the VEM’s website **https://vem.com/**.

This Addendum applies where VEM delivers services supporting essential or important functions of the Customer pursuant to the Regulation (“Critical ICT Services”) and, except for Articles 3.2, 4.4, 5.1 paragraph 2, 5.2, 5.3, 7.1 paragraph 2, 7.2 and 11 below, also in the case of non-critical ICT services.

The Customer shall assess which essential or important functions may be affected by the services supplied by VEM and notify VEM thereof at the time the agreement is entered into.

Subject to mandatory regulatory requirements, the rights granted to the Customer under this Addendum may not be exercised in a manner that would compromise the protection of personal data or the security of data belonging to any other Customer. Where the Customer’s data include personal data and VEM acts as data processor on behalf of the Customer, such processing is governed by a data processing agreement pursuant to Article 28 of Regulation (EU) 2016/679.

2 Priority of documents

If any provision of the agreement conflicts with this Addendum, this Addendum shall prevail.

Except as amended by this Addendum, the agreement remains unchanged and in full force and effect.

3 VEM’s obligations

3.1 Support and assistance

In accordance with Article 30(3)(b) of the Regulation, VEM shall promptly inform the Customer, without undue delay, as soon as it becomes aware of any development that may materially affect its ability to deliver the services.

In accordance with Article 30(2)(f) of the Regulation and to the extent required by applicable law, VEM shall assist the Customer in relation to any incidents in connection with the services that materially affect the confidentiality, integrity or availability of the Customer’s information.

In particular, VEM shall notify the Customer without undue delay of any incidents arising in connection with the services and shall provide any information in its possession that the Customer reasonably requires to mitigate the associated risks, together with information regarding how such incidents are being managed.

Where VEM incurs costs in providing support in relation to incidents that are not proven to originate from services supplied by VEM, such costs shall be charged to the Customer, as defined in the economic offer.

3.2 Sub-contracting of Critical ICT Services

If VEM subcontracts any part of the Critical ICT Services, VEM confirms that such services will be performed in accordance with this Addendum.

At the Customer's request, VEM shall disclose the location where the subcontracted Critical ICT Services are performed and where the associated data are processed and stored and shall give prior notice of any intended change to such location.

4 Security

4.1 Security policies and standards

Provisions relating to availability, authenticity, integrity and confidentiality for data protection purposes, including in respect of personal data, are available at the following link **https://vem.com/wp-content/uploads/2025/11/Security-Measures-VEM-PROT.00_NOV.25.pdf** , and form an integral part of the agreement and this Addendum.

4.2 Location of service delivery and data storage

The Parties acknowledge that data will be stored by VEM within the European Union in duly certified facilities. VEM shall promptly notify the Customer of any change to the location of service delivery or data storage. The Customer may object within 10 business days of receipt of such notice, with duly reasoned grounds, if the transfer concerns a third country that does not ensure compliance with the obligations under the agreement and this Addendum or does not guarantee an adequate level of data security and protection, without prejudice to the Customer's right to exercise its termination rights under the agreement.

4.3 Security training

At the Customer's request, VEM shall use reasonable efforts to attend, at the Customer's expense and not more than once per year, the Customer's ICT security awareness and digital operational resilience training programmes.

4.4 Threat-Led Penetration Testing (TLPT)

For Critical ICT Services only, the Customer may request VEM to participate in TLPT once every three years, unless a different interval is mandated by a competent authority. If such participation is requested, VEM shall make available any third-party certifications and TLPT reports (including those issued by any competent authority) from the three years prior to the request, and the Customer shall rely on such certifications and reports.

If the Customer, acting in good faith, demonstrates that such certifications are insufficient to meet the requirements of the Regulation, the Customer may require VEM to participate in TLPT by giving

at least 30 days' notice (unless a different notice period is mandated by a competent authority). The Customer shall ensure that any TLPT it conducts or commissions includes effective risk-management controls to avoid any harm to VEM and/or any third party.

The TLPT scope shall be limited to live production systems supporting essential or important functions of the financial entity.

If it is anticipated that VEM's participation in TLPT would have an adverse effect on the quality or security of any services delivered to Customers outside the scope of Regulation 2022/2554, or on the confidentiality of data relating to such services, the Parties shall use reasonable efforts to enter into an agreement with an external auditor so that joint TLPT ("Aggregated Tests") may be carried out, under the direction of a designated financial entity, together with other financial entities to which VEM delivers Critical ICT Services.

The Customer shall ensure that TLPT does not disrupt VEM's operations or delay service delivery or prevent VEM from complying with its contractual or regulatory obligations.

5 Monitoring and Audit

5.1 Monitoring of VEM

The Customer is entitled to monitor the services delivered by VEM on an ongoing basis and to request alternative assurance where the rights of other Customers may be affected.

Except in the case of force majeure, VEM shall inform the Customer within thirty (30) days of any development that may materially affect its ability to effectively deliver the Critical ICT Services in accordance with the agreed service levels.

VEM shall cooperate, as required under the Regulation, with onsite inspections and audits carried out by competent authorities, the Customer, or any third party appointed pursuant to the Regulation.

5.2 Monitoring of the sub-contracting chain

If Critical ICT Services are subcontracted, VEM shall use reasonable efforts to monitor the subcontracted services in order to ensure continued compliance with VEM's obligations to the Customer.

VEM shall use reasonable efforts to assess any risks associated with the location of existing or prospective subcontractors providing Critical ICT Services and their parent companies, and the location from which such services are delivered.

5.3 Audits

Subject to contractual confidentiality obligations, VEM shall use reasonable efforts to make available to the Customer any (i) third-party certifications and/or (ii) internal or third-party audit reports and/or (iii) service delivery status reports, if requested by the Customer and limited to Critical ICT Services.

If such certifications and reports relate to (i) tools, systems and controls for Critical ICT Services and (ii) regulatory requirements, the Customer shall rely on them.

The Customer may request, at a reasonable frequency and where justified from a risk-management perspective, that the scope of certifications or audit reports be expanded to include other relevant systems and controls.

If the information and documentation provided are insufficient to demonstrate VEM's compliance with its contractual obligations, the Customer may request an onsite inspection or audit, where

reasonable and appropriate from a risk-management standpoint. Where relevant, such inspections or audits may be organised jointly with other financial entities or contracting parties that use Critical ICT Services and may be carried out by those entities or contracting parties or by a third party appointed by them.

VEM shall support the Customer's inspections and audits subject to the following conditions:

- The Customer shall provide details of the scope and purpose of the inspection or audit, and any other relevant information, giving not less than fifteen (15) calendar days' notice.
- The inspection or audit may relate only to the tools and systems used by VEM to deliver the Critical ICT Services.
- Individuals conducting the audit shall comply with VEM's policies, procedures and security measures in force at the relevant premises at the time of the inspection or audit (including, without limitation, health and safety requirements, access and facilities-use rules, and confidentiality obligations).
- The inspection or audit shall be carried out in the presence of VEM personnel, consultants or contractors designated for that purpose.
- The inspection or audit shall take place during business hours and be completed as promptly as reasonably practicable, as agreed between the Parties.
- If, during the inspection or audit, there is a risk that the rights of other Customers may be affected, the Parties shall agree alternative assurance measures.

The Customer shall conduct any inspection or audit so as not to interfere with VEM's normal business operations.

Any inspection or audit may be carried out by: (i) the Customer's internal auditor; (ii) an external auditor, provided that such auditor is not a competitor of VEM; or (iii) a team comprising the Customer's internal auditor and an external auditor, provided that the external auditor is not a competitor of VEM.

The Customer shall ensure that all auditors have the necessary expertise and experience to carry out the relevant audits and assessments effectively.

Unless otherwise provided in the agreement, if any monitoring, audit or inspection by the Customer requires VEM and/or its authorised subcontractors to perform activities outside the scope of the agreement, the associated time and costs shall be charged to the Customer.

The Customer may allow one of its own customers to participate in the audit or inspection, provided that such customer complies with this Addendum.

6 Co-operation with competent authorities

VEM shall provide the Customer's competent or resolution authorities, or any third party appointed by them, with such cooperation and assistance as is necessary to verify that the services comply with the Regulation.

The Customer shall use reasonable efforts to ensure that any inspection or audit by such authorities shall not interfere with VEM's normal business operations.

7 Subcontracting

7.1 General provisions

The Customer may request, at any time, the full list of authorised subcontractors involved in the delivery of the services, together with the locations where the relevant data are processed or stored.

With respect to Critical ICT Services, VEM shall use reasonable efforts to replicate the relevant obligations set out in this Addendum in its subcontracting agreements with authorised subcontractors.

7.2 Material changes to subcontracting agreements

In the event of any material change to a subcontracting agreement relating to the delivery of Critical ICT Services, VEM shall notify the Customer at least fifteen (15) days in advance, so that the Customer may assess whether such change may have a significant impact on the services and/or affect VEM's ability to comply with its contractual obligations. This notice requirement shall not apply in cases of force majeure or where the change is necessary to ensure service continuity or the availability, authenticity, integrity or confidentiality of the Customer's data.

By the end of the notice period, the Customer shall inform VEM of the outcome of its risk assessment and whether it approves or rejects the proposed changes.

If the Customer, acting in good faith and on reasonable and legitimate grounds, rejects the material changes to the subcontracting arrangements, it may terminate the agreement in accordance with Article 8 of this Addendum.

Failure to respond within the notice period and/or continued use of the Critical ICT Services shall be deemed acceptance of the material changes to the subcontracting arrangements.

8 Additional termination events

In addition to any termination rights under the agreement, the Customer may terminate the agreement by certified email, giving at least thirty (30) days' notice, in any of the following circumstances:

i. an unexpected interruption of the services, lasting more than fifteen (15) days, exclusively attributable to VEM;
ii. failure to deliver the services in full due to reasons exclusively attributable to VEM;
iii. a serious breach by VEM of any applicable laws or regulations and/or of the agreement;
iv. if any circumstances identified through third-party ICT risk monitoring are not promptly remedied and are such as to materially affect the delivery of the services, including any material changes impacting the agreement;
v. if any weaknesses attributable to VEM arise in its overall risk-management framework, and are not promptly remedied, particularly in relation to how it ensures the availability, authenticity, integrity and confidentiality of the Customer's data; in such case, the Customer shall provide documentary evidence of its internal risk assessment;
vi. if a competent authority is unable to effectively supervise the Customer due to any conditions or circumstances arising from the agreement; in such case, the Customer shall provide formal evidence that it has been notified by the competent authority that effective supervision of the Customer is not possible;
vii. if VEM makes any material changes to subcontracting agreements for the delivery of Critical ICT Services without the Customer's approval within the fifteen (15)-day notice period; in

such case, the Customer shall provide written reasons explaining the scope of the changes, why they are considered material, and the grounds for its objection;

viii. unauthorised subcontracting of Critical ICT Services.

9 Effects of termination

This Article applies only where Customer data are processed or stored by VEM.

Upon termination of the agreement, VEM shall provide access to, restore and return all Customer data processed by VEM in an easily accessible format.

VEM may retain data and information as required to comply with applicable record-keeping obligations, and any automatic backup copies generated by filing systems that cannot be immediately retrieved using ordinary procedures.

10 Exit plan

If performance of the agreement is permanently or temporarily suspended for any reason (including, without limitation, insolvency, termination or service interruption), VEM shall, upon written request by the Customer submitted within seven (7) days of termination, cooperate in preparing an exit plan.

VEM shall use reasonable efforts to ensure that termination of the agreement occurs without disruption to the Customer’s operations.

The Parties shall agree a transition period, to be set out as part of the exit plan, not exceeding four (4) months. During this transition period, VEM shall continue to deliver the services to minimise disruption and enable migration to another provider or an internal solution consistent with the complexity of the services.

11 Emergency plan

VEM shall use reasonable efforts to implement and test business emergency plans to ensure adequate security in delivering Critical ICT Services.

VEM shall use reasonable efforts to ensure continued delivery of Critical ICT Services including where a subcontractor fails to meet its service levels or contractual obligations.

12 Amendments to the Addendum

Any amendments to this Addendum shall be agreed in writing by the Parties.