DORA Addendum: Critical ICT Functions

1. Background and purpose

This "**Addendum**" is entered into between Customer and Supplier (as identified below), also collectively referred to as the "**Parties**", and individually as a "**Party**". The Addendum supplements the [agreement and/or order form between the Parties], as updated from time to time (the "**Agreement**"). The Addendum will come into effect from the date Customer effectively becomes subject to DORA.

Customer is in the following assumed to be subject to regulatory requirements under the Applicable Operational Resilience Laws. This Addendum is intended to implement the contractual obligations arising under the Applicable Operational Resilience Laws, with particular emphasis on the requirements set forth in Article 30 of DORA applicable to contracts with ICT third-party service providers. The Parties agree that, within the context of DORA, Supplier provides ICT services supporting critical or important functions to Customer.

2. Structure

This Addendum consists of this cover page and the general terms set out below.

3. Signatures

The Addendum is signed below by duly authorised representatives of both Parties, confirming their acceptance of the terms set forth in the Addendum.

This document can also be signed digitally.

Customer	**Supplier**
[Customer Name]	[Supplier Name]
Signature of the Customer	Signature of the Supplier

General Terms

1. General

1.1. This Addendum constitutes an integral part of the Agreement. Unless otherwise expressly stated in this Addendum, the Agreement remains unchanged. The Parties agree that the Supplier will not be subjected to obligations more burdensome than those reasonably inferred from the Applicable Operational Resilience Laws.

Accordingly, the Addendum is not to be interpreted to impose requirements on the Supplier that deviate from the reasonable interpretation of the Applicable Operational Resilience Laws.

1.2. In case of any inconsistency or conflict between this Addendum and the Agreement, this Addendum prevails, unless expressively stated otherwise.

1.3. Capitalised terms used in this Addendum have the meanings given to them in the definition section below or as otherwise set out in the Addendum.

1.4. If, for any reason, Customer is not or ceases to be subject to DORA, this Addendum will become entirely void from that date. If, for any reason, the Services should not be regarded as ICT services supporting critical or important functions to Customer, the Parties agree that the contractual obligations in this Addendum arising from DORA article 30 nr. 3 do not apply.

2. Service Description

The Parties acknowledge that the Services are described in a clear and complete manner in the Agreement.

3. Subcontracting

3.1. Supplier may subcontract the Services, or parts thereof, if:

(a) Supplier conducts reasonable due diligence and a risk assessment, including evaluating security risks, related to the subcontracted services.

(b) Supplier remains fully accountable for the subcontracted service components.

(c) Supplier oversees the subcontracted services to ensure they comply with Supplier's obligations to the Customer.

(d) Without prejudice to item (b), Supplier makes reasonable efforts to ensure that the subcontracted services meet the agreed service levels.

4. Locations of Services and Customer Data

4.1. The regions and countries from which the Services will be provided and where Customer Data will be processed, including any storage location, are available through the Trust center, as updated from time to time.

www.superoffice.com/trust-center - homepage
https://www.superoffice.com/trust-center/agreements/dpa/ - section 2

4.2. Supplier also may provide the Services and process Customer Data at additional locations necessary for fulfilling the Agreement, which may include locations where Supplier's subcontractors operate data processing operations or as required by law or a binding order from a governmental authority.

4.3. Supplier will provide Customer with advance notice of any proposed changes to the

locations for processing by updating or the list of pre-approved subcontractors.

www.superoffice.com/trust-center - homepage
https://www.superoffice.com/trust-center/agreements/sub-processors/

5. Data Protection

5.1. Supplier undertakes to maintain data management procedures, policies, and measures facilitating the availability, authenticity, integrity, and confidentiality of Customer Data.

5.2. Customer remains responsible for evaluating its own data management needs in line with its policies and risk assessments. Customer is responsible for selecting and implementing any supplementary measures it deems necessary to fulfil its own data management requirements and nsure comprehensive data protection.

6. Confidentiality

6.1. The Supplier commits to maintain the confidentiality of Confidential Information, ensuring it is not disclosed to any third party without Customer’s authorisation.

6.2. To the extent necessary to deliver the Services, the Customer hereby grants the Supplier permission to disclose Confidential Information to Supplier’s affiliates, partners, subprocessors, and subcontractors on the condition that these are bound by similar confidentiality obligations as set out in the Addendum.

6.3. Notwithstanding the foregoing, the Supplier may disclose Confidential Information in response to a court order, a request by a competent authority, or as required by law or regulation. This disclosure may also occur to the extent reasonably necessary to defend a claim, enforce rights, or fulfil obligations under or in relation to the Agreement. In such instances, the Supplier commits to: (i) notifying the Customer of the disclosure, provided that such notification is lawful; (ii) disclosing

only the portion of the Confidential Information that is strictly necessary; and (iii) ensuring, to the extent possible, that the Confidential Information remains confidential after disclosure.

6.4. Except as otherwise mutually agreed upon in writing by the Parties, the Supplier's obligation to maintain the confidentiality of the Confidential Information expires three years following termination of the Agreement.

6.5. The confidentiality obligations detailed above do not prejudice or supersede any other confidentiality commitments between the Parties as outlined in the Agreement.

7. Service Discontinuation

In the event of insolvency, resolution, or discontinuation of the business operations of Supplier, Customer may access, recover, and retrieve Customer Data through the Services.

8. Service Level Description and Reporting Obligations

8.1. The agreed service levels are set out in the Agreement.

8.2. Supplier undertakes to notify Customer of any event that might have a material impact on Supplier's ability to effectively provide the Services in accordance with the agreed service levels.

8.3. Supplier must take appropriate corrective actions, without undue delay, when agreed service levels are not met.

9. ICT Incident Assistance

9.1. In case of an ICT-related incident related to the Services, Supplier will provide Customer with reasonable assistance and information, including assistance and information reasonably required to comply with Applicable Operational Resilience Laws.

9.2. Without prejudice to other available remedies for contractual defaults, Supplier is entitled to compensation for such ICT incident assistance on a time and material basis, at the hourly rates set out in the Agreement or as otherwise applicable for the relevant personnel, if Supplier can demonstrate that Customer has caused or contributed to causing the ICT-related incident or the incident is caused by circumstances controlled by, or for which the Customer has the risk and responsibility. Customer may at any time request an overview of the applicable rates.

10. Business Contingency and ICT Security

Supplier undertakes to implement and test business contingency plans and implement ICT security measures, tools and policies that provide an appropriate level of ICT security for the provision of Services to Customer.

11. Cooperation with Authorities

Supplier will fully cooperate with the Supervisory Authority – including any persons appointed by them – in matters related to Applicable Operational Resilience Laws.

12. Termination

12.1. Without prejudice to the termination rights set out in the Agreement, Customer may terminate the Agreement if Customer can demonstrate that:

(a) Supplier has significantly breached applicable laws, regulations, or contractual terms;

(b) Customer has, during its monitoring of ICT third-party risks, uncovered circumstances specifically related to the Supplier that were previously unknown or could not have reasonably been anticipated, and are reasonably and objectively considered likely to materially affect the agreed performance of Services under the Agreement;

(c) there are material, persistent deficiencies in Supplier's overall ICT risk management, as measured against the agreed commitments in the Addendum, including in the way Supplier ensures the availability, authenticity, integrity and confidentiality of Customer Data; or

(d) the Supervisory Authority has determined that it can no longer effectively supervise Customer solely because of circumstances specifically and exclusively related to the Services delivered under the Agreement.

12.2. Before exercising the right to terminate the Agreement under this section, Customer must promptly provide Supplier with written notice of the intent to terminate, specifying the reason for termination. The Parties must, in good faith, endeavour to resolve the grounds for termination, giving each other reasonable time to rectify the grounds for termination, unless prohibited by Applicable Operational Resilience Laws. If Customer does not notify the Supplier within 14 calendar days after becoming, or reasonably should have become, aware of the grounds for termination, the termination rights under this provision are forfeited.

12.3. Except as expressly required by law, neither Party will be liable to the other for compensation, reimbursements, or damages caused by the termination pursuant to this section. The termination will not relieve either Party of obligations incurred prior to the effective date of the termination.

13. Exit Plan

13.1. Without affecting the termination rights set out in the Agreement, Customer may, upon termination, request that Supplier continue to provide the Services in accordance with the Agreement for up to [12 months], at the then-applicable rates. Additionally, Customer may access and download Customer Data for transfer of the Services to another supplier or back to Customer before termination.

13.2. To exercise the exit rights above, Customer must provide written notice to Supplier at least 30 days before the intended termination date, clearly specifying the exact exit rights Customer wishes to use. However, if giving 30 days' notice isn't possible due to immediate termination, Customer may exercise the exit rights by notifying Supplier promptly.

13.3. Notwithstanding the above, Supplier can suspend the continuation of the Services if

Customer:

(a) is involved in illegal activities, including, but not limited to, corruption, fraud, or any other activity that could reasonably harm Supplier's reputation or violate the law; or

(b) materially defaults on payment obligations under the Agreement.

13.4. Upon termination, Supplier must delete Customer Data from its systems within reasonable time, unless laws or court orders require otherwise. If Supplier is legally required not to delete Customer Data, Supplier must continue securing the data as outlined in the Agreement. Once deleted, Supplier has no further obligations regarding Customer Data.

14. Participating in Training

14.1. Where required under Article 13 (6) of DORA, Supplier will provide reasonable participation in Customer's ICT security awareness programs and digital operational resilience training. Upon request, Supplier will assist Customer with identifying the appropriate participants from its personnel who should attend the program or training based on their authority and capability to access and process Customer Data.

14.2. Customer must submit a written request for Supplier's participation in any programs or training at least one month in advance of the scheduled date. The request must include detailed information about the training, as well as specify the personnel or categories of personnel required to participate. Customer will endeavour to limit Supplier's involvement to what is strictly necessary.

14.3. Customer agrees that any of Supplier's personnel who have participated in similar ICT security programs or digital operational resilience training will be exempt from Customer's programs and training sessions, unless their participation is strictly necessary for compliance with Applicable Operational Resilience Laws, and validated by formal documentation from Customer detailing this requirement.

15. Threat-led Penetration Testing

15.1. If and to the extent that the Supplier is within the scope of Customer's obligation to perform threat-led penetration testing in accordance with Articles 26 and 27 of DORA, Supplier shall cooperate to facilitate such testing.

15.2. Customer must submit a written request for Supplier's participation in any threat-led penetration testing no less than one month before the testing commences. The request must include detailed information about the scope and purpose of the testing, in addition to a detailed overview of Supplier's contribution. Customer agrees to limit Supplier's involvement to what is strictly necessary and whenever possible seek to meet its requirements through other means.

16. Audits

16.1. The Supervisory Authority and Customer have the right to inspect and audit Supplier. Such audits may include reasonable on-site examinations and access to relevant information, records, and documents. Customer has the right to take copies of relevant documentation on-site if the documents are critical to the operations of the Services and such copies are strictly required for compliance with Applicable Operational Resilience Laws, validated by formal documentation from Customer detailing this requirement. Data or information related to other customers of the Supplier are excluded from such audits or inspections.

16.2. Supplier will cooperate fully during agreed onsite inspections and audits.

16.3. Instead of conducting a full inspection or audit, the Customer will, whenever possible, aim to meet its requirements through alternative methods. These may include utilising standard features of the Services, leveraging previously provided information, or relying on existing third-party certifications and external or internal audit reports. When an inspection or audit is indispensable, Customer will endeavour to conduct joint audits with other financial entities that are also customers of Supplier.

16.4. Unless otherwise required by Applicable Operational Resilience Laws, all audits or inspections by Customer must be carried out by a reputable third-party auditor – as agreed between the Parties.

16.5. Customer is responsible for ensuring that any individual or entity, other than the Supervisory Authority, who audits or gains access to any information regarding the Supplier or the Services during or after an inspection or audit adheres to the following confidentiality obligations: (i) Not disclosing the information to any third party without the Supplier's prior written consent; (ii) Using the information solely for the purposes of the audit or as otherwise authorised in writing by the Supplier; (iii) Implementing appropriate safeguards to protect the confidentiality of the information, consistent with industry standards; (iv) Immediately notifying the Supplier of any unauthorised access, use, or disclosure of the information; and (v) Deleting all confidential information upon completion of the audit or upon the Supplier’s request, ensuring no copies remain unless required by applicable law.

16.6. Customer must give Supplier written notice of any audits or inspections at least one month before the audit or inspection is intended to take place.

17. Miscellaneous

17.1. **Disclosure**

Insofar as it is necessary to fulfil the obligations outlined in this Addendum, comply with the Applicable Operational Resilience Laws, or respond to requests from the Customer or Supervisory Authorities, Customer hereby authorises the Supplier to disclose Customer Data, including Confidential Information, to the pertinent Supervisory Authority or any third party designated by the Customer or Supervisory Authority to perform tasks in relation to the Agreement.

17.2. **Cost Allocation**

Customer must pay its own costs for activities related to this Addendum or to comply with Applicable Operational Resilience Laws, including, but not limited to, costs for audits and hiring third parties. Supplier is entitled to compensation for its direct, reasonable, and documented costs from: (i) participating in Customer's ICT-security awareness programme and digital operational resilience training; (ii) cooperating in Customer's threat-led penetration tests; (iii) audits and inspections; (iv) assisting the Customer according to the exit plan; and (v) addressing incidents directly or indirectly, fully or partially, caused by Customer. Any supplementary measures or services implemented or provided by the Supplier will be conducted against payment. Supplier will endeavour to provide Customer with cost estimates or the methodology for calculating the applicable costs, such as relevant hourly rates for required personnel, before any such costs are incurred.

17.3. **Severability**

If any term or provision of the Addendum is held by a competent court or authority to be void, illegal, or unenforceable, the validity or enforceability of the remainder of the Addendum will not be affected unless such enforcement would be clearly unreasonable. The Parties commit to negotiate in good faith with the aim of replacing any terms deemed void, illegal, or unenforceable with a legal, valid, and enforceable provision that, seen in the context of this Addendum as a whole, achieves as closely as possible the intention of the Parties under this Addendum.

17.4. **Amendments**

17.4.1. Supplier reserves the right to amend this Addendum, in accordance with Applicable Operational Resilience Laws, to reflect changes in regulatory guidance and interpretations. Supplier will provide the Customer with notice of any such amendments. Amendments are considered accepted unless Customer objects in writing within 30 days of Supplier's notification.

17.4.2. Supplier may terminate the Agreement with immediate effect in case the Supervisory Authority requests amendments to the Agreement or the Addendum which are reasonably not acceptable to Supplier.

17.4.3. At the interval for renewal of the Agreement, Supplier reserves the right to consider adopting the standard contractual clauses developed by public authorities subject to DORA article 30 nr. 4, and to amend the Addendum in accordance with regulatory standards adopted by the EU Commission pursuant to DORA article 30 nr. 5.

18. Definitions

18.1. Capitalised terms used in this Addendum have the meanings given to them below or as otherwise set out in the Addendum: **"Applicable Operational Resilience Laws"** means applicable national laws and regulations implementing the DORA Regulation.

"**End User**" means any individual or entity that directly or indirectly through another user accesses or uses Customer Data or otherwise accesses or uses the Services under Customer's account.

"**Customer Data**" means all files, personal data, and other information and data that Customer or any End User transfers to Supplier for processing, storage, or hosting by the Services in connection with Customer's account.

“**Confidential Information**” means Customer Data of a secret, confidential, or commercially sensitive nature. Confidential Information does not encompass information that: (i) has entered or enters the public domain other than as result of Supplier's default of the confidentiality undertaking; or (ii) was independently developed by Supplier without reference to or reliance upon Confidential Information.

“**DORA**” means Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

“**Services**” means the services provided by the Supplier under the Agreement.

“**Supervisory Authority**” means any national or EU authority designated under Applicable Operational Resilience Laws to supervise Customer’s or Customer’s ICT third-party service providers' compliance with the operational resilience requirements established therein, including resolution authorities if applicable. 18.2. Terms defined in DORA have the same meaning when used in this Addendum.