DORA ADDENDUM

[V1.0 17th Jan 2025]

THIS DORA ADDENDUM FOR EU FINANCIAL ENTITIES (THE "**DORA ADDENDUM**") CONSTITUTES AN ADDENDUM TO THE **SERVICE ORDER FORM** BETWEEN CHINA TELECOM CONTRACTING ENTITY AND/OR ITS AFFILIATES ("**SUPPLIER**") AND THE CUSTOMER AS DEFINED THEREIN (THE "**CUSTOMER**"). THE SERVICE ORDER FORM TOGETHER WITH OTHER APPLICABLE CONTRACTUAL DOCUMENTATION AS AMENDED BY THIS DORA ADDENDUM CONSTITUTE A LEGAL AND ENFORCEABLE CONTRACT BETWEEN THE CUSTOMER AND THE SUPPLIER ("**AGREEMENT**").

UNLESS THE PARTIES AGREE OTHERWISE IN WRITING, REFERRING TO SPECIFIC PROVISIONS OF THIS DORA ADDENDUM, OR UNLESS THE PROVISIONS OF THE AGREEMENT ARE MORE FAVOURABLE FOR THE CUSTOMER, IN THE EVENT OF A CONFLICT THIS REGULATORY ADDENDUM SHALL PREVAIL OVER ANY OTHER PROVISIONS OF THE AGREEMENT, ITS OTHER ADDENDA AND ORDERS.

TERMS NOT DEFINED IN THIS DORA ADDENDUM SHALL HAVE THE MEANING ASCRIBED TO THEM IN THE AGREEMENT OR ANY AMENDMENT THERETO (AS APPLICABLE). THE SUPPLIER RESERVES THE RIGHT TO UPDATE AND AMEND THIS DORA ADDENDUM FROM TIME TO TIME AS IS NECESSARY AND PERMITTED BY THE GOVERNING LAW OR APPLICABLE LAW OF THE AGREEMENT.

A. GENERAL TERMS APPLICABLE TO ALL EU FINANCIAL ENTITIES

1. DEFINITIONS

1.1 The following capitalised terms used in this DORA Addendum have the meanings set out below:

1.1.1 "**Applicable Laws**" means DORA, EBA Guidelines, EIOPA Guidelines or ESMA Guidelines and other applicable EU financial sector regulations relating to outsourcing, the use of cloud services, and digital operation resilience, as amended from time to time.

1.1.2 "**Auditor**" means the Customer, the Customer's third-party auditor or a Competent Authority, or any person appointed by them in a capacity of an auditor.

1.1.3 "**EBA Guidelines**" means EBA revised Guidelines on outsourcing arrangements of 25 February 2019, with reference EBA/GL/2019/02, available on the European Banking Authority webpage, as the same may change from time to time, and such related national regulations that give effect to the foregoing guidelines in the relevant jurisdiction within the European Economic Area and/or the United Kingdom, as applicable to each Financial Entity falling within the scope of the EBA Guidelines.

1.1.4 "**EIOPA Guidelines**" means (i) the European Insurance and Occupational Pensions Authority Guidelines on information and communication technology security and governance (EIOPA-BoS-20-002), and/or (ii) the European Insurance and Occupational Pensions Authority Guidelines on information and communication technology security and governance (EIOPA-BoS-20/600), all available on the European Insurance and

Occupational Pensions Authority webpage, as the same may change from time to time, and such related national regulations that give effect to the foregoing guidelines in the relevant jurisdiction within the European Economic Area and/or the United Kingdom, as applicable to each Financial Entity falling within the scope of the EIOPA Guidelines.

1.1.5 "**ESMA Guidelines**" means Guidelines on outsourcing to cloud service providers (10/05/2021| ESMA50-164-4285) available on the European Securities and Markets Authority webpage, as the same may change from time to time, and such related national regulations that give effect to the foregoing guidelines in the relevant jurisdiction within the European Economic Area and/or the United Kingdom, as applicable to each Financial Entity falling within the scope of the ESMA Guidelines.

1.1.6 "**Competent Authority**" means any EU or EU Member State official authority, government agency or other government body having regulatory, supervisory or governmental authority over the Customer, including resolution authority if appointed for the Customer.

1.1.7 "**Critical or important function**" means Customer's function or process whose disruption would materially impair the financial performance of the Customer, or the soundness or continuity of its services and activities, or whose discontinued, defective or failed performance would materially impair the continuing compliance of the Customer with the conditions and obligations of its authorisation, or with its other obligations under Applicable Laws.

1.1.8 "**Customer Data**" means: (a) all proprietary and confidential data or other information received from the Customers through the provision of the Supplier's Services, including personal data, (b) any derivatives, improvements or modifications thereof, (c) all materials in any tangible medium of expression that include the information in such materials, that are provided to the Supplier, and (d) any Customer data or information identified as 'Confidential Information' or that could reasonably be assumed to be confidential and proprietary.

1.1.9 "**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, as amended or replaced from time to time.

1.1.10 "**ICT-related Incident**" or "**ICT Incident**" means a single event or a series of linked events related to the Services or the Supplier, unplanned by the Customer or the Supplier, that compromises the security of the Customer's network and information systems, and has an adverse impact on the availability, authenticity, integrity or confidentiality of Customer Data, or on the services provided by the Customer.

1.1.11 "**Parties**" means the Supplier and the Customer.

1.1.12 "**Services**" used in this Addendum means the ICT services as defined in DORA that are provided by the Supplier pursuant to the Service Order Form. Where a service provided pursuant to the Service Order Form and other applicable contractual documentation does not fall into the scope of ICT

services as defined in DORA, the purchase and provision of such service shall not be subject to this DORA Addendum.

2. SCOPE AND APPLICATION

2.1 This DORA Addendum applies only to Customers who are financial entities as referred to in DORA Article 2 paragraph 2.

2.2 This DORA Addendum is aimed at meeting the regulatory requirements imposed on the Customer under DORA.

2.3 This DORA Addendum supplements the Agreement and is binding on the Parties during the term of the Service Order Form.

2.4 All modifications to this DORA Addendum must be agreed between the Parties and made in the same form as required for a modification of the Agreement.

3. SERVICE LEVEL AND SECURITY

3.1 In providing the Services, the Supplier will comply with the service levels set out in the Service Order Form.

3.2 The Supplier being a public electronic communications network provider and public electronic communications service provider, acting under strict telecommunication regulations, establishes and maintains up-to-date and high-quality information security standards, as well as appropriate physical, technical and organisational measures, tools and policies certified under international recognised standards (including ISO standards), aimed at providing a sufficient level of security of the Services, including of the availability, authenticity, integrity and confidentiality of Customer Data processed by the Supplier in relation to the Services.

3.3 The Supplier will reasonably allow its personnel to participate in the Customer's security awareness programmes and digital operational resilience training as notified with due advance notice to the Supplier, as long as it does not destabilize the safety or continuity of the provision of the Supplier's Services and does not create extensive costs for the Supplier.

3.4 ICT Incident support. Unless other incident reporting procedures are stipulated in the Agreement, the Supplier will, in the event of the occurrence of an ICT Incident that could have a negative impact on the continuity or security of the Services, perform the following without charging any additional fees and without undue delay:

3.4.1 notify the Customer of the ICT Incident;

3.4.2 provide the Customer with such information as can be reasonably requested that the Supplier has on the ICT Incident that the Customer needs to secure the Customer's functions at risk due to the ICT Incident;

3.4.3 provide the Customer with such information as can be reasonably requested on how the Supplier handled the ICT Incident.

3.5 The Parties agree that the information provided by the Supplier to the Customer under this section is confidential. However, the Customer is entitled to disclose such information to competent authorities, if required under Applicable Laws.

4. COOPERATION

4.1 The Supplier will reasonably cooperate with Competent Authorities, including with persons appointed by them, if requested by them and to the full extent required under the Applicable Laws.

4.2 Such requested cooperation cannot lead to or result in a breach of the Supplier's confidentiality obligations towards its other customers or competent authorities nor can it disrupt the Supplier's Services provided to such other customers.

5. CODE OF CONDUCT

5.1 The Supplier will act in an ethical and socially responsible manner, respecting human rights and children's rights, including the prohibition of child labour, will respect the applicable principles on environmental protection, and will ensure appropriate working conditions.

6. DATA LOCATION

6.1 The Supplier will provide the Customer with information on any locations (countries or smaller regions) from which the Supplier or its Subcontractors provide the Services or part of them, and where Customer Data are processed or stored.

6.2 The Supplier and its Subcontractors cannot change the country or region from which the Services are provided or where Customer Data are processed or stored without notifying the Customer at least thirty (30) days in advance.

6.3 If the Customer objects to the abovementioned change for reasonable and justified regulatory reasons, including cybersecurity concerns, and the Supplier or its Subcontractors uphold the proposed change, and no other arrangement is agreed with the Customer within thirty (30) days from the Customer's notification of its objection, the Customer will have the right to terminate its use of the Services affected by the change, effective from the date announced for the implementation by the Supplier of the proposed change. Any minimum notice period which would otherwise apply to such termination will not apply in this case.

7. ADDITIONAL TERMINATION RIGHTS

7.1 In addition to any termination rights granted to the Customer under the Agreement, the Customer will be entitled to terminate the Agreement in the following circumstances:

7.1.1 if the Supplier significantly breaches Applicable Laws or the provisions of the Agreement, and fails to cure such breach within 30 days of receiving a written notice from the Customer in this respect;

7.1.2 if a final and irrevocable decision is issued under Applicable Laws by a Competent Authority ordering the Customer to terminate the Agreement; in such case, the Supplier will hold discussions with the Customer on how to adapt to the Competent Authority's requirements and, if the Parties fail to reach agreement in this respect, the Customer will be entitled terminate the Agreement by giving sixty (60) days' prior written notice to the Supplier or such other notice as indicated in the decision by the Competent Authority;

7.1.3 if the Supplier makes material changes to the Agreement or to the Services that, as evidenced by the Customer, adversely impact the Customer's ability

to meet its regulatory obligations or to perform its functions with the use of the Services; in such case, the Supplier will hold discussions with the Customer on how to adapt to the Customer's requirements and, if the Parties fail to reach agreement in this respect, the Customer will be entitled terminate the Agreement by giving sixty (60) days' prior written notice to the Supplier;

7.1.4 if the Supplier has evidenced major weaknesses pertaining to its overall ICT risk management, including, in particular, the way the Supplier ensures the availability, authenticity, integrity and confidentiality of data, whether personal data or otherwise sensitive data, or non-personal data, and those weaknesses are not addressed to secure the standards agreed under the Agreement within thirty (30) days of receiving a written notification from the Customer in this respect;

7.1.5 if a Competent Authority states that it can no longer effectively supervise the Customer as a result of the conditions of, or circumstances related to, the Services; in such case, the Supplier will hold discussions with the Customer on how to adapt to the Customer's requirements and, if the Parties fail to reach agreement in this respect, the Customer will be entitled terminate the Agreement by giving sixty (60) days' prior written notice to the Supplier.

B. TERMS APPLICABLE TO THE SUPPLIER'S SERVICES SUPPORTING CUSTOMER'S CRITICAL OR IMPORTANT FUNCTIONS

Notwithstanding Section A of this DORA Addendum, this Section B will apply only if the Supplier is notified by the Customer that the Supplier's Services support the Customer's Critical or important functions, or material parts thereof, and this is confirmed in the Service Order Form between the Parties.

8. TESTING

8.1 The Supplier will annually perform internal independent tests of its Services in accordance with recognised testing standards, including threat-led penetration tests meeting the requirements of Articles 26 and 27 of DORA. the Supplier, on a confidential basis, will make the results of such tests available to the Customer at the Customer's request.

8.2 If the internal tests results mentioned above are insufficient for the Customer due to regulatory requirements identified by it, the Supplier will provide, or will cause that its Subcontractor provide, as the case may be, the cooperation required and reasonable participation in the Customer's testing of the Services, including in pooled ICT testing or threat-led penetration testing, organised by the Customer. The Parties will agree the terms of such participation of the Supplier at least thirty (30) days prior to the date of the tests, unless a shorter term is required by Applicable Laws.

9. BUSINESS CONTINUITY

9.1 During the Term of this Agreement, the Supplier will maintain, update and test its business continuity plans related to the Services, including disaster recovery and crisis management policies, aimed at successfully restoring the Services and key business functions in the event of a disaster. At all times during the Term, the plan will not be materially decreased or diminished by the Supplier and will meet or exceed the criteria

agreed under the Agreement, or in their absence, the criteria provided in Article 11 DORA.

9.2 For the purposes of the security of the Services, the abovementioned business continuity plans are confidential and cannot be revealed to the Customer in their entirety, except for selected materials that the Supplier may be obliged to disclose to the Customer or its competent supervision authority, subject to confidentiality obligations and procedures.

10. AUDIT, MONITORING AND NOTICE PERIODS

10.1 The Supplier will notify the Customer of any development that could have a material impact on the Supplier's ability to effectively provide the Services in accordance with the Agreement or Applicable Laws promptly but no later than within seventy-two (72) hours of obtaining relevant information through the regular incident management processes implemented by the Supplier.

10.2 At the Customer's reasonable request, the Supplier will provide to the Customer, or indicate the source of, the following information:

10.2.1 information that is justifiably necessary to confirm that the Supplier is in compliance with its obligations stipulated in this DORA Addendum;

10.2.2 identification information (i.e. legal names, registered offices, corporate registration numbers, tax identification numbers, etc.) on the Supplier and its Subcontractors;

10.2.3 other information or documentation that proves that the Supplier and its Subcontractors have the business reputation, abilities, expertise and adequate resources (financial, human and technical), as well as information security standards, appropriate organisational structure, risk management and internal controls, authorisations and registrations (if applicable) needed to provide the Services supporting Critical or important functions of the Customer in a reliable and professional manner.

10.3 The Supplier shall provide the Customer with appropriate reports on their activities and services to the financial entity, including periodic reports, incidents reports, service delivery reports, reports on ICT security and reports on business continuity measures and testing if so required by the Customer.

10.4 Audit and Access Right. the Supplier will make available to the Customer a copy of audit reports related to the Services prepared by a qualified third-party auditor. Such reports are the Supplier's Confidential Information under the Agreement.

10.5 If, in order to comply with the Customer's regulatory obligations, the Customer, its Auditor or a Competent Authority requires additional information not included in the reports, the Customer will inform the Supplier of this to enable the Supplier to provide such additional information. If a further audit is required, the Customer and its Competent Authority, and any other auditor appointed by the Customer or Competent Authority, will be granted:

10.5.1 full access to the Supplier's relevant operational business premises, including to data and similar operation centres, and to relevant devices, systems, networks, information and data other than Customer Data used for providing

the Supplier's Services, including related financial information, personnel, operational reporting and operational testing relevant for the Services; and

10.5.2 unrestricted rights of inspection and auditing related to the applicable Service pursuant to the Agreement and this DORA Addendum, to enable them to audit the provision of the Services pursuant to the Agreement and to ensure compliance with all Applicable Laws.

10.6 The Customer, the appointed Auditor or Competent Authority will execute a written confidentiality agreement acceptable to the Supplier or will otherwise be bound by a statutory or legal confidentiality obligation before executing their Audit and Access Rights. Notwithstanding the above, any information provided by the Supplier or otherwise accessed by the Auditor during the audit procedures, shall be deemed to be the Supplier's Confidential Information.

10.7 Nothing in this DORA Addendum shall entitle any Competent Authority, Auditor or the Customer to have access to information about any other customer of the Supplier or to any parts of the Supplier's business that are not engaged in the provision of the Services to the Customer.

10.8 Unless required by Applicable Laws, the Supplier shall not be obliged to disclose information in relation to any audit where to do so would place the Supplier in breach of any confidentiality obligations owed to third parties or would infringe a third party's intellectual property rights or otherwise be unlawful.

10.9 Lack of Compliance. If an audit reveals that the Supplier or its Subcontractor are not in compliance with the Applicable Laws or the Agreement, including this DORA Addendum, the Supplier shall take, or will cause its Subcontractor to take, such action as is needed to correct any non-compliance identified at its own expense.

10.10 For the avoidance of doubt, the meaning and scope of the Audit and Access Right described above shall be interpreted in accordance with the provisions of DORA, the Regulatory Technical Standards issued under DORA, and any applicable regulatory guidelines, as amended or replaced from time to time.

11. SUBCONTRACTORS

11.1 The Supplier is authorised to engage Subcontractors in the performance of its obligations under the Agreement, provided that the Supplier remains primarily liable for the proper performance of such obligations towards the Customer.

11.2 A list of Subcontractors can be provided to the Customer if required.

11.3 The Supplier will:

11.3.1 flow down the obligations provided in this DORA Addendum, Section B, to its Subcontractors;

11.3.2 oblige its Subcontractors to flow these terms down to their Subcontractors further down the subcontracting chain.

11.4 Neither the Supplier nor its Subcontractors may change their Subcontractors or material arrangements with them without notifying the Customer at least thirty (30) days in advance. If the Customer objects to any such proposed change of the Subcontractor or material arrangements with them due to regulatory, including cybersecurity, concerns, and the Supplier or its Subcontractors, nonetheless, choose to

implement such proposed change, and no other arrangement is agreed with the Customer within 30 days from the Customer's notification of their objection:

11.4.1 the Customer shall be entitled to terminate its use of the Service affected by the change with effect from the announced date of implementation of the proposed change; and

11.4.2 any minimum notice period which would otherwise apply to such termination will not apply.

12. EXIT ASSISTANCE

12.1 If the Agreement is terminated for any reason, including in the case of the resolution or restructuring of the Customer, the Supplier will reasonably co-operate with the Customer to allow it to terminate the Services or to migrate them in-house or to another service provider.

12.2 The abovementioned cooperation will be provided by the Supplier at the request of the Customer and at the then-current rates for such services at the Supplier.

12.3 At a minimum, the Customer will have the right to choose to extend the Services for a reasonable period of up to six (6) months from the date of termination of the Agreement, by providing a written request to the Supplier at least sixty (60) days before the Agreement is terminated. During such extension period, (i) the Supplier will continue to provide the Services and the Customer will continue to pay for them, pursuant to the terms and conditions of the Agreement, and (ii) the Customer will be able to request the retrieval of the Customer Data held by the Supplier by means of the standard processes and tools then offered by the Supplier.

12.4 For three (3) months after the Customer’s access to the Services ends, including due to termination of the Agreement or the insolvency, resolution or discontinuation of the Customer’s business operations, the Supplier will, to the extent permitted by Applicable Laws, return to the Customer, in an easily accessible format, the Customer Data possessed by the Supplier in relation to the Services (or will ensure access or recovery, if the Customer prefers this to return).