

## Supplier EBA and DORA Outsourcing Terms

### 1. Definitions

The following definitions shall apply to this Addendum:

**“Affiliate”** means, with respect to a party, any entity which directly or indirectly, through one or more intermediaries, is controlled by, or is under common control with, such party.

**“Critical ICT Third-Party Service Provider”** or **“CTPP”** means an ICT third-party service provider designated as critical at the European Union level.

**“FIS Client(s)”** means a client or customer of FIS or FIS Affiliates, to which FIS or FIS Affiliates provides software and/or services, in relation to which FIS or FIS Affiliates utilise the Services;

**“Event”** means:

- (a) the application of any resolution power or resolution procedure to FIS by a Regulator in any relevant jurisdiction under applicable legislation in force from time to time in order to safeguard public interests (including without limitation national authority resolution powers under Article 68 and 71 of Directive 2014/59/EU); or
- (b) the execution of any one or more of the options contained in the recovery plan for FIS or the FIS’ Affiliates submitted to FIS’ Regulator in accordance with such Regulator’s rules and guidance;

**“Event Date”** means the date on which an Event occurs;

**“ICT”** means information and communication technology;

**“ICT-related Incident”** means a single event or a series of linked events that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the business of FIS an FIS Affiliate or an FIS Client.

**“Lead Overseer”** means the European Supervisory Authority (“ESA”) designated to oversee a Critical ICT Third-Party Service Provider under applicable law, including its authorised persons;

**“Recipient”** means a person to whom all or part of the business, assets, rights or liabilities of FIS has been transferred;

**“Regulator”** means any resolution authority, regulatory or quasi regulatory authority empowered by law which regulates FIS or FIS Client(s), in connection with the Services, or any replacement or successor body in any relevant jurisdiction from time to time including the Lead Overseer; and

**“Services”** means any services (including, but not limited to, professional services and maintenance) delivered by Supplier under the terms of the Agreement.

### 2. Audit

**2.1 General Duty to Cooperate.** The Supplier undertakes to fully cooperate with FIS and FIS Clients to enable FIS and FIS Clients to and assess the Supplier as its third-party technology / ICT service provider and review on an ongoing basis the Services provided by the Supplier, and effectively supervise the Services and manage the risks associated with the outsourcing / ICT Services provided for in the Agreement and for the purpose of effective oversight by FIS and FIS Clients. This includes cooperating with Regulators, including other persons appointed by them.

**2.2 Supplier Diligence and Audit Materials.** The Supplier shall provide on request by FIS, FIS Clients and FIS Affiliates or the Regulator, accompanied access to (without limitation) the Supplier’s business premises, systems, networks, devices as well copies of other relevant records and information such as audit reports, attestations, and other detailed information regarding the Supplier’s internal systems testing and procedures, and the Supplier’s information security and data privacy controls. Supplier shall complete questionnaires submitted by FIS for this purpose within the reasonable deadline set by FIS. FIS shall be able to make any such records and information available to FIS Affiliates and FIS Clients. These audit materials evidence Supplier’s compliance with industry and regulatory standards and include independent audit reports (such as SSAE 18’s), third-party attestations and certifications (such as ISO certifications, and PCI AOC’s), and detailed information and testing results regarding physical, technical and administrative controls utilized by the Services and the security of FIS’ or FIS Clients’ Confidential Information. Where deemed necessary under applicable laws and regulations by FIS, FIS Clients or a Regulator, FIS and FIS Clients may request a reasonable and legitimate expansion of the scope of these audit reports or certifications.

**2.3 SSAE 18 Audit.** The Supplier shall cause an independent public accounting firm to perform the audits (generally SSAE 18) with respect to the Services being provided under the Agreement. The Supplier shall make available to FIS a copy of the resulting independent audit report(s) relevant to the Agreement and FIS shall be able to make any such report(s) available to FIS Clients, FIS Affiliates and the Regulator. The Supplier shall promptly address and resolve any deficiencies identified in such audit report(s), including any notified to it by FIS.

**2.4 Dedicated Audit Visit.** FIS shall be entitled to conduct dedicated on-site audit visits of the Supplier and in relation to any such visits:

**2.4.1** FIS may visit the Supplier processing facility, that provides the Services to FIS, twice per calendar year unless the audit visit serves to verify the remediation of a previous adverse audit finding or unless a Regulator or FIS Client requires more

frequent visits; Requests for any on-site audit visit shall be made in writing by FIS at least ten (10) days in advance (unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective or if shorter notice is given by the Regulator or specifically required by the relevant regulatory obligation, in which case FIS will give as much advance notice as is possible in the circumstances and provide the reasoning for the shorter notice);

2.4.2 On-site audit visits shall be conducted during normal business hours for the facility and shall be coordinated with the Supplier so as to cause minimal disruption to the Supplier's business operations;

2.4.3 Any FIS initiated on-site audit visit shall be performed by FIS' employees and/or a reputable third-party auditor, it being understood that FIS (and its representatives) shall at all times be bound by the confidentiality provisions of the Agreement and shall be accompanied by a representative of the Supplier;

2.4.4 When performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated; and

2.4.5 Supplier acknowledges audits may occur on a pooled basis and Supplier shall not unreasonably withhold or delay agreement to pooled audits, or pooled ICT testing, with other clients of Supplier where appropriate.

**2.5 Access in accordance with DORA and EBA Outsourcing guideline.** Where deemed necessary under applicable laws and regulations by FIS, FIS Clients or a Regulator, the Supplier shall grant to FIS, FIS Clients and Regulators, including in relation to oversight activities concerning FIS' status as a Critical ICT Third-Party Service Provider, (a) full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the Critical Services (which access includes making or being provided with copies of relevant information), including related financial information, personnel and the Supplier's and/or its service provider's external auditors reports; and (b) unrestricted rights of inspection and auditing related to the outsourcing arrangement, in each case to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.

**2.6 Annual DORA attestation.** Annually, a senior officer of Supplier (e.g., CISO/CTO) shall attest in writing to FIS that Supplier complies with the obligations in this Addendum relating to the Services, including subcontracting controls and audit readiness.

**2.7 Implementation of oversight recommendations.** Where FIS must adopt measures to implement recommendations or remedial actions addressed by the Lead Overseer and such impact the Services and/or Suppliers obligations under the Agreement including this Addendum, when requested by FIS, Supplier shall implement corresponding changes to the Services, subcontracting, security controls, data locations, testing or services levels as reasonably directed by FIS and mutually agreed by the parties to achieve compliance within the timelines specified by FIS based on the direction of the Lead Overseer.

### 3. Monitoring

3.1 The Supplier acknowledges and accepts that FIS and FIS Clients are under a duty to review and monitor on an ongoing basis the Services and effectively supervise the Services and manage the risks associated with the outsourcing provided for in the Agreement. For the purposes of effective oversight by FIS or a Regulator, FIS and FIS Clients shall have the right to monitor the Supplier's performance of Services (including any sub-contractor) using any methods as FIS or FIS Clients deem appropriate which may include face-to-face, remote monitoring or some other form of contact, in any case on an ongoing basis. Supplier shall reasonably cooperate with FIS and FIS Clients to enable them to perform such monitoring.

### 4. Supplier's obligation to inform and assist

4.1 The Supplier will inform FIS without undue delay (and in any event within 24 hours) after it becomes aware of any ICT-related Incident or of any other development that may have a material impact on the Supplier's ability to effectively provide Services in line with agreed service levels, applicable laws and regulatory requirements. Supplier will provide full assistance to FIS and FIS Clients in case of ICT-related Incidents in connection with the Services. Supplier shall promptly provide FIS with the factual information necessary for FIS or FIS Clients to complete initial, intermediate and final incident reports under applicable law, including, where known: date/time of detection and classification, incident description and type, affected services and systems, threat techniques, geographic spread, impacts on clients/counterparties, activation of business continuity measures, indicators of compromise, and root cause and remediation summary; and indicate whether the incident originates from a third-party and in such case provide the third party's legal name and identification code.

### 5. Security awareness and digital operational resilience training

5.1 For Supplier personnel whose roles require log-on credentials to FIS or FIS Client's systems and/or access to FIS or FIS Client's premises, FIS or FIS Clients may offer ICT security awareness and digital operational resilience training to Supplier and Supplier personnel shall participate in such training upon request.

### 6. Penetration testing

6.1 Upon FIS' or FIS Client's request, the Supplier will allow for, participate and fully cooperate in any penetration and vulnerability testing of the Supplier's systems, devices (whether internal or external) and any other relevant infrastructure utilized in the provision of the Services ("**Suppliers Systems**") in accordance with standard industry practice ("**Penetration Testing**") to be conducted by or on behalf of FIS or any FIS Client either by themselves or by using a reputable third party selected by FIS or FIS Clients. If the results identify any material (in particular "high" or "critical" level) risks, the Supplier shall

promptly use all reasonable endeavours to remediate such risks as soon as reasonably possible and inform FIS as soon as any such remedial work is completed and provide evidence of closure.

## 7. Location information

7.1 The Services will be provided, and FIS' and FIS Client's data will be kept and processed, from the country(ies) individually listed in Appendix E of the Main Vendor Agreement and/or the Engagement Document:

7.2 Upon FIS' request, Supplier shall provide the physical address of each service and data processing location relevant to the Services.

7.3 The Supplier shall not change the locations stipulated above or sub-contract data without FIS' prior written consent.

## 8. Personal Data

The Supplier will ensure the accessibility, availability, integrity, security and protection of any personal data held by it in connection with the Services in accordance with the terms of the Agreement.

## 9. Sub-contracting Services

9.1 The Supplier will not sub-contract any of its obligations in relation to the Services, or make any material changes to the sub-contracting arrangements, without FIS' prior written consent, which FIS will not unreasonably withhold. The Supplier shall announce any planned sub-contracting or any planned material changes to the sub-contracting arrangements at least 90 calendar days before planned implementation to be able to obtain timely consent. If the Supplier subcontracts or makes any material changes to sub-contracting arrangements without FIS' prior consent, without any limitation to any other remedies, FIS has the right to terminate the Agreement, or terminate any part of the Services affected by the change or limit the scope of the Services by providing at least 10 calendar days prior written notice to the Supplier.

9.2 Before using or proposing to use any subcontractor, the Supplier will assess at least the following: (i) business reputation, (ii) resources including expertise and adequate financial, human and technical resources, (iii) information security, (iv) organizational structure, (v) risk management and internal controls in place; and the Supplier will provide appropriate information to FIS and FIS Clients about these aspects upon request. These assessments are intended to address all risks, including ICT risks, associated with the location of the potential subcontractor and its parent company and the location where the subcontracted Services are provided from.

9.3 Supplier shall and shall ensure that all subcontractors which are legal persons, obtain and maintain a valid and active legal entity identifier (LEI) or otherwise accepted identifier.

9.4 FIS hereby authorises the Supplier to use the sub-contractors set out individually in Appendix E of the Main Vendor Agreement and/or the Engagement Document below in the provision of the Services (each being an **"Authorised Sub-Contractor"**):

9.5 Supplier shall provide and maintain accurate information needed by FIS and FIS Clients to populate and update the DORA register of information (**"RoI"**), including: contract references; service descriptions; function mapping and classification; locations (regions/countries) of provision and data processing; chain of subcontractors and rank; and valid and active LEI for Supplier and, for Critical Services, for subcontractors providing such services or part thereof. Supplier shall notify FIS of updates promptly to enable timely RoI updates.

9.6 At all times:

9.6.1 the Supplier shall impose upon any subcontractors obligations that are equivalent to those set out in the Agreement;

9.6.2 any obligation on the Supplier to do, or to refrain from doing, any act or thing under this Addendum or otherwise shall include an obligation upon the Supplier to procure that all sub-contractors it utilizes in relation to the Services also do, or refrain from doing, such act or thing. The Supplier shall ensure that all sub-contractors it utilizes in relation to the Services comply with all applicable laws and regulatory requirements. The Supplier shall be responsible for overseeing all such sub-contractors to ensure that all contractual obligations between the Supplier and FIS are continuously met;

9.6.3 the Supplier undertakes to ensure that FIS and any Regulator has the same contractual rights of access and audit in respect of all sub-contractors that the Supplier utilizes in relation to the Services as those granted by the Supplier;

9.6.4 the Supplier will ensure the continuous provision of Services in accordance with its contractual obligations under the Agreement, even in case of failure by a subcontractor to meet its service levels or any other contractual obligations;

9.6.5 the Supplier shall be liable for the acts and omissions of each sub-contractor it utilizes in relation to the Services as if each sub-contractor's acts or omissions were the acts or omissions of the Supplier; and

9.6.6 the appointment of any sub-contractor that the Supplier utilizes in relation to the Services shall not relieve the Supplier of its obligations under this Addendum.

## 10. Business Continuity and Disaster Recovery

10.1 The Supplier will establish and maintain disaster recovery and business continuity plans designed to minimise the risks associated with a disaster affecting the Supplier's ability to provide the Services, which includes off-site data storage and



recovery infrastructure, recovery time objective (“**RTO**”) and recovery point objective (“**RPO**”), in each case the RTO and RPO shall be at least of a leading industry standard.

10.2 The Supplier will:

10.2.1 maintain adequate backup procedures in order to recover FIS’ (or if applicable, any FIS Client’s) data to the point of the last available good backup; and

10.2.2 test its disaster recovery and business continuity plans, including call trees, not less frequently than annually.

10.3 If the Supplier:

10.3.1 fails to meet the RTO and RPO in any annual test, the Supplier shall perform a root cause analysis of the cause of the failure to meet the RTO or RPO and will promptly remediate the cause of such failure and retest, in any event within six (6) months of the first failed test; or

10.3.2 fails to meet the RTO or RPO in the retest, the Supplier will have a second six (6) month period to remediate and retest but shall endeavor to remediate as soon as reasonably practicable. If the Supplier fails a second time, FIS may request that the parties attempt to reach a mutually agreeable resolution, and if the parties are unable to agree upon a resolution within thirty (30) days of FIS’ request, FIS may terminate the Agreement by written notice with no further financial obligation to the Supplier.

10.4 The Supplier will provide its disaster recovery plan and test results to FIS and FIS may share such disaster recovery plan and test results with FIS Clients who have contracted for the Services, FIS’ auditors, and FIS’ Regulators or other professional advisors.

10.5 The Supplier will implement the applicable disaster recovery or business continuity plan upon the occurrence of a disaster and shall notify FIS promptly following such event. In the event of a disaster (as defined in the plan), the Supplier will not charge fees higher than or in addition to the agreed fees under the Agreement. The Supplier will notify FIS of, and invite FIS to participate in (at no additional charge to FIS), the Supplier’s disaster recovery and business continuity plan test.

## **11. Return of data**

11.1 The Supplier will ensure in a demonstrable manner that FIS and each FIS Client can access, recover and receive all their data in Supplier’s possession in the case of insolvency, resolution or discontinuation of the business operations of the Supplier. Where appropriate in relation to the Service provided, Supplier shall offer functionalities and/or provide services to easily store create any required backups and data exports of such data.

11.2 In the event that the Supplier:

11.2.1 ceases to do business;

11.2.2 no longer offers support or provides the Services under the Agreement;

11.2.3 is subject to any resolution proceedings;

11.2.4 is subject to any of the following:

(a) bankruptcy;

(b) receivership;

(c) insolvency;

(d) dissolution; or

(e) any other similar proceedings are instituted by or against the Supplier,

the Supplier agrees, at its own expense, to provide to FIS, as soon as reasonably possible (no later than within 30 days), all then-current data or information relating to the Services in a durable medium and format as requested by FIS. This may include (without limitation) data to be returned in a secure manner and particular level of encryption commensurate with the sensitivity of the data or information.

## **12. Termination**

12.1 In addition to the termination rights specified in the Agreement (in particular for cause, including for material breach of contract by FIS), FIS may terminate the Agreement (or any part of it) without liability (other than its obligation to pay any accrued fees up to the date of termination) if:

12.1.1 the Supplier is in breach of applicable law, regulations or any contractual provisions under the Agreement or this Addendum;

12.1.2 FIS or any FIS Client is ordered to do so by any Regulator or a valid order of a Court having jurisdiction over FIS;

12.1.3 a Regulator with jurisdiction over FIS issues a formal notice prohibiting FIS from performing under the Agreement;

12.1.4 a Regulator informs FIS or an FIS Client that it is unable to effectively supervise FIS or such FIS Client as a result of the conditions of, or circumstances related to, the Services;

12.1.5 FIS, in its reasonable opinion, determines Supplier is hindering FIS in meeting its requirements as a Critical ICT Third-Party Service Provider and/or the requirements of its Lead Overseer;

12.1.6 in the reasonable opinion of FIS, there are impediments which are capable of altering the performance of the Services;

12.1.7 in the reasonable opinion of FIS, there are material changes to the Services such that they affect the outsourcing arrangement or the Supplier's ability to provide the Services;

12.1.8 the Supplier sub-contracts any of its obligations in relation to the Services without obtaining FIS' prior consent; or

12.1.9 where in the reasonable opinion of FIS, there are weaknesses regarding the Supplier's management and security of Confidential Information or Personal Data, or a breach of security of Confidential Information or Personal Data or any other sensitive data in relation to the Services provided by the Supplier.

12.2 If requested by FIS, the Supplier shall provide the services and assistance required to facilitate the complete transition of the Services from the Supplier to any incoming supplier or successor of the Services. The Supplier's services and assistance, under this provision, will include, as a minimum, uninterrupted continuation of services to FIS for a period of 6 months. The Supplier will support FIS with the orderly transfer of all information or data held by the Supplier or its sub-contractors in relation to the Services. The Supplier will upon request assist FIS or FIS Client in designing an exit management plan with the aim of ensuring there is an orderly and smooth transition off the Services (and each element thereof) to FIS or the FIS Client and/or the successor supplier without any material disruption in the supply of Services or material deterioration in the quality of delivery of the Services.

### 13. Additional Provisions

Where FIS is a regulated entity, the following additional provisions apply:

#### 13.1 Recovery and Events

13.1.1 If FIS was, immediately prior to the Event Date, entitled to receive Services pursuant to the Agreement and/or receive any other benefit of the Agreement (as applicable) (the "Supply") and is subject to an Event, then the Supplier shall:

(a) provide all assistance and services required by FIS (or the Regulator) to give effect to and assist in the continuation of the Supply which FIS was receiving prior to the Event on the same terms as applicable immediately prior to the Event Date; and

(b) for a maximum period of 24 months from the Event Date (or such longer period specified by a Regulator), not terminate, suspend, withhold or materially alter any Supply provided pursuant to the Agreement (regardless of whether such right to terminate, suspend, withhold or materially alter has arisen but has not been exercised prior to the Event Date) unless:

(i) the Regulator consents to the termination, suspension, withholding or alteration;

(ii) Supplier is compelled by the order of a Court in a competent jurisdiction; or

(iii) FIS fails to fulfil its payment obligations under and in accordance with the terms of the Agreement.

13.1.2 The Regulator shall be entitled to enforce the Agreement or part of it (as applicable) on behalf of FIS or any FIS Affiliate, and Supplier and each Supplier Affiliate (if relevant) shall act upon directions and instructions given by the Regulator, as if the Regulator were FIS and those directions or instructions were given to the Supplier or the relevant Supplier Affiliate by FIS.

13.1.3 If managing an Event involves a transfer of any part of the business of FIS to a Recipient, the terms of Section 13.2 (Divestment) shall apply.

13.1.4 FIS shall be entitled to, in accordance with the terms of Section 13.2 (Divestment), novate or transfer its rights and obligations under the Agreement to a Recipient (including a "bridge bank" or other corporate entity to which the Regulator has directed the Agreement be novated or transferred). The effect of such transfer shall be that the Agreement shall be treated as having been originally entered into between the Supplier and the Recipient. The Supplier shall enter into and execute any documentation required by FIS or any Regulator and any such Recipient for the purpose of novating or transferring the Agreement and otherwise for giving effect to such novation or transfer provided, however, that the Supplier will continue to provide such Services to the Divested Business in accordance with Section 13.2.1 until such time as the new agreement has been signed. The Supplier acknowledges that following the completion of such novation or transfer the Recipient or FIS shall be entitled to exercise any of its rights set out in this Section 13.1 (Recovery and Events) and Section 13.2 (Divestment).

13.1.5 The Supplier acknowledges that Regulators may have certain powers in respect of FIS and its affiliates, including: (i) the power of resolution authorities to require any person to provide any information required for the relevant Regulator to decide upon and prepare a resolution action plan including updates and supplements of information provided in the resolution plans and including requiring information to be provided through on-site inspections; and (ii) all information gathering and investigatory powers that are necessary for the Regulators to exercise their functions.

#### 13.2 Divestment

13.2.1 If FIS sells, transfers or otherwise disposes off, as a result of an Event, any Affiliate of FIS or any part of the business of any Affiliate of FIS that is directly receiving the benefit of the Services (the "**Divested Business**") at the date of the sale or disposal ("**Disposal Date**") to a Recipient which is not and is not intended to become an Affiliate of FIS, then the Supplier shall at the request and choice of FIS or the Regulator (if applicable) either:-



(a) provide all assistance and services (including signing all documents) required by FIS (or the Regulator) to give effect to and assist in the continuation of the Supply which the Divested Business was receiving prior to the Disposal Date for a period reasonably requested by FIS and/ or as otherwise required by the Regulator. During the aforementioned period, and subject to the payment by FIS to Supplier of Supplier's reasonable costs in providing such assistance and services to the Divested Business (to the extent that the services and assistance are outside of the scope of the Services), the Divested Business will be entitled to receive the Services on the same terms as applicable immediately prior to the Disposal Date; or

(b) promptly enter into a direct agreement with the Divested Business, subject to agreement of commercial terms, for a separate supply of Services on operational terms that are the same as (or better than) the Agreement [that shall in no way enlarge or reduce the obligations on the Supplier's part] provided, however, that the Supplier will continue to provide such Services to the Divested Business in accordance with sub-Section 13.2.1(a) above.

13.2.2 Under Section 13.2.1(a), the Divested Business shall continue to enjoy the rights and benefits it is entitled to under the Agreement as if it were still a part of FIS' business or an Affiliate of FIS, provided that whilst the Divested Business is deemed to remain an Affiliate of FIS, FIS shall remain fully liable for the acts and omissions of the Divested Business and shall be responsible for the compliance of such Divested Business with the terms and conditions of the Agreement, as if such Divested Business were a party hereunder.

13.2.3 In order to achieve the efficient and effective transition of the Divested Business to a Recipient, the Supplier shall provide all assistance and services reasonably requested by FIS with respect to such transition, which shall include such assistance as FIS (or the Regulator) may consider to be appropriate in the circumstances.

13.2.4 The Agreement shall remain in full force and effect in respect of any part of the business of any Affiliate of FIS which is not divested pursuant to this Section 13.2 (Divestment).

13.2.5 The parties may disclose to any Recipient any Confidential Information which relates to the performance of the Services to the extent necessary for the Recipient to use or receive the Services pursuant to this Section 13.2 (Divestment).

**13.2.6 Structural changes and novation to EU entities.**

Supplier acknowledges that FIS may novate or assign the Agreement, this Addendum or relevant parts to any European Union subsidiary or entity in order to comply with oversight requirements for it as a Critical ICT Third-Party Service Provider. Supplier shall execute all documentation reasonably required to affect such novation or assignment without charge.