Maestro DORA and UK outsourcing addendum

DORA and UK outsourcing addendum · Draft · 27 November 2026

Template for legal review. This addendum supplements the Maestro Terms of Service v1.1 and the order form (together called the MSA here) where the Customer is a financial entity under Regulation (EU) 2022/2554 (DORA) or uses Maestro in an outsourcing or third-party arrangement within PRA SS2/21 or FCA SYSC 8. It prevails over the MSA, the DPA (Schedule 4 or the enterprise DPA) and the service levels (Schedule 3 or the enterprise SLA) where they conflict. The order form states whether Maestro supports a **critical or important function** of the Customer; the Customer decides this.

Part A: Terms for all regulated customers

A1 Description of services. The services, functions and deployment option are described in the order form and the documentation. Promethean will tell the Customer in advance of any change that materially affects them.

A2 Locations. The countries and regions where the services are provided and where Customer Data is stored and processed are listed in the order form and the DPA (Annex 3). Promethean will give at least [60] days' notice before changing any of them, and will not change them for a critical or important function without the Customer's consent.

A3 Data protection and security. Promethean protects the availability, authenticity, integrity and confidentiality of Customer Data, including personal data, under the DPA and its technical and organisational measures, and keeps those measures in line with good industry practice.

A4 Access, recovery and return of data. If Promethean becomes insolvent, stops trading or the agreement ends for any reason, the Customer can retrieve all Customer Data in a common machine-readable format, as set out in the exit terms.

A5 Service levels. The SLA applies, with any updates agreed in writing.

A6 ICT incidents. Promethean will help the Customer with any ICT-related incident affecting the services, at no extra cost [or at the rates agreed in the order form]. It will notify the Customer of any major incident affecting the services without undue delay and within [4] hours of classifying it, and give the information the Customer needs for its own regulatory incident reporting.

A7 Cooperation with authorities. Promethean will cooperate fully with the Customer's competent authorities and resolution authorities, including people they appoint.

A8 Subcontracting. Promethean will not subcontract any part of the services that supports a critical or important function without the Customer's prior consent. For any subcontracting, Promethean remains responsible, flows down equivalent obligations (including audit and access rights) and tells the Customer of material changes at least [60] days in advance, giving the Customer the right to object and, if the change goes ahead, to terminate.

A9 Security awareness. Promethean will take part in the Customer's ICT security awareness programmes and digital operational resilience training where the Customer reasonably requests.

A10 Termination rights. In addition to the MSA, the Customer may terminate on notice where: Promethean significantly breaches applicable law, regulation or contract terms; circumstances identified through monitoring could change the performance of the services; there are evidenced weaknesses in Promethean's ICT risk management, including in the security of data; or a competent authority can no longer effectively supervise the Customer because of the arrangement. Termination under this clause is without penalty, with a refund of prepaid fees for the remaining term.

Part B: Extra terms for critical or important functions

B1 Precise service levels. The SLA's targets apply as binding quantitative service levels. Where the Customer needs different targets, they are set in the order form. Promethean reports performance monthly, and both parties agree corrective actions when targets are missed.

B2 Notice and reporting. Promethean will report to the Customer, in writing and without undue delay, any development that could materially affect its ability to provide the services effectively and in line with this agreement and the law, including changes of control, material subcontracting changes and material incidents.

B3 Business continuity. Promethean will keep and test a business continuity and ICT disaster recovery plan for the services, at least [once a year], and share a summary of the results. The plan sets recovery time and recovery point objectives agreed in the order form [target RTO ● hours, RPO ● hours].

B4 Security measures and testing. Promethean will keep ICT security measures appropriate to the Customer's regulatory obligations, commission an independent penetration test at least [yearly] and after material changes, and share the summary findings and remediation status.

B5 Threat-led penetration testing. Where the Customer is required to carry out threat-led penetration testing (TLPT) that covers the services, Promethean will take part and cooperate under agreed rules of engagement.

B6 Audit, access and inspection. The Customer, its auditors and its competent authorities have unrestricted rights of access, inspection and audit, including to Promethean's premises, relevant systems, data and records, and may take copies of relevant documents. The parties will agree reasonable arrangements so that audits do not compromise other customers' data or security. Pooled audits with other customers and third-party certifications may be used where the Customer agrees, without limiting its rights.

B7 Exit strategy. Promethean will keep an exit plan for the services. On termination, it will continue to provide the services and reasonable transition help for a transition period of up to [6] months, at the prices in the order form, so that the Customer can move to another provider or bring the service in-house without disruption and while staying compliant. Promethean will return all Customer Data in a common format and delete it as the DPA requires.

B8 Register information. Promethean will provide, and keep up to date, the information the Customer needs for its register of information on ICT third-party arrangements and for its supplier reporting to the PRA and FCA.

Requirement map

For the Customer's third-party risk file: where each requirement is met. Article references are to DORA Article 30; check against the final text and the Customer's own policy.

Requirement	DORA Art. 30	PRA SS2/21 theme	Where met
Clear description of services	2(a)	Written agreement	A1, order form
Locations of services and data	2(b)	Data and location	A2, DPA Annex 3
Data protection and security	2(c)	Data security	A3, DPA Annex 2
Access and return of data on exit or insolvency	2(d)	Access, exit	A4, B7, MSA 14
Service level descriptions	2(e)	Service levels	A5, SLA
Incident assistance	2(f)	Incident reporting	A6, DPA 8
Cooperation with authorities	2(g)	Access for regulators	A7
Termination rights	2(h)	Termination	A10, MSA 13

Requirement	DORA Art. 30	PRA SS2/21 theme	Where met
Security awareness training	2(i)	Operational resilience	A9
Quantitative service levels	3(a)	Service levels	B1
Notice and reporting duties	3(b)	Ongoing oversight	B2
Business continuity, tested	3(c)	Business continuity	B3
ICT security measures	3(c)	Data security	B4
Participation in TLPT	3(d)	Testing	B5
Audit, access and inspection	3(e)	Access, audit, information	B6
Exit strategy and transition period	3(f)	Exit planning	B7
Sub-outsourcing control	Art. 30 and related standards	Sub-outsourcing	A8
Register of information	Art. 28(3)	Supplier reporting	B8

Signed for the Customer: _____ Name, title, date

Signed for Promethean Systems Ltd: _____ Federico Nordenstahl, Director, date