Version 2026-03-12

DORA APPENDIX

1. INTRODUCTION AND DEFINITIONS

1.1 This DORA appendix (this "**Appendix**") supplements the Master Agreement between Outpost24 and the Customer (as updated from time to time) (the "**Agreement**"). This Appendix is an integrated part of the Agreement, for the term of the Agreement provided the Customer, or any duly authorised affiliate of the Customer using the Services, remains subject to the supervision by the Competent Authority (each a "**Regulated Entity**").

1.2 The provisions of this Appendix shall be interpreted and applied consistently with the principle of proportionality underlying DORA, having regard to the nature, scale, complexity and importance of the relevant ICT services, the criticality or importance of the functions they support, and their potential impact on the continuity of the Customer's financial services and activities. The Customer's rights and Outpost24's obligations under this Appendix shall not be construed as exceeding what is required under DORA for the Services at their applicable classification at the relevant time. Outpost24 fulfils its obligations under this Appendix through its Information Security Management System, which is certified in accordance with ISO/IEC 27001 and independently audited, unless otherwise expressly agreed in writing between the Parties.

1.3 Unless otherwise stated, capitalised terms in this Appendix shall have the meaning ascribed to them in Section 2 or, if not defined in this Appendix, in the Agreement. Non-capitalised terms and expressions used in this Appendix that relate to DORA, e.g. 'ICT services', 'ICT-related incidents', 'threat-led penetration tests' etc., shall be construed in accordance with the meaning given to them in DORA.

2. DEFINITIONS

"**Applicable Laws**" means all statutes, laws, regulations and regulatory standards, guidelines, directions, rules, orders, guidance, recommendations, including: (a) Data Protection Law; (b) DORA; (c) laws and regulations relating to bank secrecy, financial secrecy, or equivalent confidentiality obligations applicable to financial institutions; (d) know-your-customer, anti-money laundering and counter-terrorism financing laws and regulations; and (e) any rule, regulation, direction, guidance, recommendation, code of practice or other requirement issued or published from time to time by a Competent Authority, in each case as amended, restated, re-enacted, supplemented or replaced from time to time, which are applicable to a Party to the extent they relate to any aspect of that Party's rights or obligations under the Agreement.

"**Competent Authority**" means any competent national or international government body, regulatory body, or authority, including financial supervisory authority and resolution authority, in the European Economic Area, with binding authority to regulate or supervise the financial services activities of the Regulated Entity and/or Outpost24 from time to time, including the Lead Overseer (as defined in DORA).

"**Customer Data**" means the data that the Customer provides to Outpost24 in connection with the Services or enters into any software made available as part of the Services.

"**Data Protection Law**" means the EU General Data Protection Regulation, European Commission decisions, binding EU and national guidance and all national implementing legislation, including any law amending, supplementing or replacing the aforementioned from time to time.

"**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.

"**Regulated Entity**" means as described in Section 1.1 in this Appendix.

"**Service Levels**" means the qualitative and quantitative service levels and other performance metrics that Outpost24 agrees to meet in the provision of the Services under the Agreement.

"**Transition Period**" means as described in Section 11 of this Appendix.

3. SERVICE LEVELS AND PERFORMANCE MONITORING

3.1 The Service Levels that apply to the provision of the Services are set out in the SLA, which are available at https://outpost24.com/legal/. The obligations further set out in Sections 3.2 and 3.3 below shall only apply where the Services support critical or important functions.

3.2 Outpost24 will, upon Customer's request, make available monitoring tools that enable the Customer to oversee and evaluate the performance of the Services.

3.3 Without prejudice to Section 3.2, Outpost24 shall provide written reports to the Customer in regard to any development that may have a material impact on Outpost24's ability to effectively carry out the Services in line with the agreed Service Levels and in compliance with Applicable Laws.

4. OBLIGATION TO COOPERATE

4.1 Nothing in this Appendix shall be construed as limiting or impeding the Competent Authority's ability to effectively monitor, audit or inspect the Services in accordance with Applicable Law. If the Competent Authority orders any amendment to be made to the Agreement, the Parties shall in good faith negotiate appropriate amendments to address such order, including any financial and other commercial implications.

4.2 Outpost24 shall fully, upon request by the Customer, cooperate with the Competent Authority, including any persons appointed by them.

5. INCIDENT COOPERATION AND SECURITY

5.1 General

Outpost24 implements and maintains appropriate technical and organizational measures to ensure the availability, authenticity, integrity and confidentiality of Customer Data. These measures are implemented through Outpost24's Information Security Management System

(ISMS), which is certified in accordance with ISO/IEC 27001 and independently audited on a regular basis, including through SOC 2 Type II assurance.

5.2 Incident reporting

In the event an ICT-related incident occurs that is related to the Services or Customer Data, Outpost24 shall during the term of the Agreement provide reasonable assistance and support as reasonably requested by the Customer to assess the ICT incident and take appropriate mitigating measures.

5.3 Security training and penetration tests

5.3.1 Outpost24's security awareness training program forms part of its ISO/IEC 27001-certified ISMS and is designed to ensure that personnel involved in the provision, support, security, or incident management of the Services are aware of their information security responsibilities and applicable security requirements. Outpost24 conducts regular security testing and assurance activities as part of its ISO/IEC 27001-certified ISMS and SOC 2 Type II audited control environment. Such testing is designed to assess the effectiveness of implemented security measures and processes in a risk-based and proportionate manner. The obligations further set out in Sections 5.3.2-5.3.4 below shall only apply where the Services support critical or important functions.

5.3.2 During the term of the Agreement, Outpost24 agrees to provide the Customer information on test results from relevant penetration tests carried out by or on behalf of Outpost24, including internal tests conducted on a quarterly basis and external tests conducted on an annual basis. Such test results shall be made available to the Customer via Outpost24's compliance platform. If the Customer reasonably determines that such test results are not sufficient for it to assess the effectiveness of the implemented security measures and processes or to comply with its obligations under Applicable Law, the Customer may, subject to reasonable prior notice, planning and coordination with Outpost24 and compliance with Outpost24's security policies, carry out threat-led penetration tests made in accordance with the requirements set out in DORA to test and assess implemented security measures and processes. Outpost24 agrees to participate in and fully cooperate with the Customer in relation to such threat-led penetration test.

5.3.3 If the Customer's penetration test compromises or impacts the security, privacy or integrity of any data that is not Customer Data or threatens to do so, the Customer shall immediately cease conducting the penetration test. The Customer shall promptly report any discovered vulnerabilities to Outpost24 in detail.

5.3.4 All testing results and any potential vulnerabilities shared by Outpost24 or identified by the Customer, and any other reporting or information sharing regarding Outpost24's security or resilience pertaining to penetration tests hereunder, are Outpost24's Confidential Information.

5.4 Cost allocation

The Customer shall bear its own costs and expenses related to the activities performed under Sections 5.2 and 5.3. In addition, the Customer shall compensate Outpost24 for any reasonable and verified costs incurred by Outpost24 in providing cooperation and assistance under said Sections.

6. LOCALISATION AND DATA ACCESS

6.1 The Services will be provided and Customer Data will be stored in the location(s) as set forth in the DPA. Outpost24 will give the Customer prior written notice before changing any such location(s), unless it is necessary to change such location before giving the notice due to an emergency situation in which case the notice will be given promptly after the change.

6.2 During the term of the Agreement, the Customer will have access to the Customer Data in a manner consistent with the functionality of the Services. If Outpost24: (a) becomes insolvent, is declared bankrupt or enters in liquidation or resolution (or equivalent); (b) is dissolved or wound up; (c) discontinues its entire business operations; or (d) upon termination of the Agreement, the Customer shall have the right to retrieve all Customer Data. Customer Data is accessible by the Customer in source format, which the Customer has verified to be easily accessible.

7. SUBCONTRACTING

7.1 If a subcontractor of Outpost24 is used for a critical or important function, the terms of this Section 7 shall apply.

7.2 Outpost24 has the Customer's general authorisation for the engagement of subcontractors, subject to the terms set out in the Agreement and this Section 7. Outpost24 shall inform the Customer of any intended changes concerning the addition or replacement of subcontractors within reasonable time in advance, thereby giving the Customer the opportunity to object to such changes prior to the engagement of the concerned subcontractors. Outpost24 will only use subcontractors that are suitable and have the required qualification and competence to perform their tasks in such way that the Services are provided in accordance with Applicable Laws and the Agreement. When assessing whether a subcontractor is suitable, Outpost24 shall consider all risks associated with the location of the subcontractor (including its parent company), the location(s) where the subcontracted ICT services are performed and, where relevant, the location of the data processed or stored by the subcontractor.

7.3 Customer may object in writing to Outpost24 regarding the appointment of any new subcontractor within thirty (30) days of receiving notice in accordance with Section 7.2 if the appointment materially increases Customer's risk associated with the Services. In the event of such reasonable objection the Parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Outpost24 may, at its sole discretion, either not appoint such subcontractor, or permit Customer to terminate the Services affected by the appointment, without liability to either Party.

7.4 Outpost24 shall oversee and be responsible for the performance of subcontracted Services to ensure that they are continuously provided in accordance with the Agreement. Additionally, Outpost24 shall ensure that its contractual relationships with the engaged subcontractors include appropriate terms regarding:

(a) monitoring and reporting obligations of the subcontractor;

(b) business contingency plans and ICT security standards;

(c) service levels; and

(d) access, audit and inspection rights.

8. SECURITY AND BUSINESS CONTINUITY REQUIREMENTS

8.1 The obligations set out in this Section 8 shall only apply where the Services support critical or important functions.

8.2 Outpost24 has implemented and shall maintain and tested business continuity and disaster recovery measures, as well as ICT security controls, through its ISO/IEC 27001-certified Information Security Management System. These measures are designed to provide an appropriate level of security and operational resilience for the provision of the Services, taking into account their nature, scale, complexity, and criticality.

9. RIGHT OF ACCESS, AUDIT AND INSPECTION

9.1 The obligations set out in this Section 9 shall only apply where the Services support critical or important functions.

9.2 Outpost24 shall fully cooperate with the Regulated Entity or any Competent Authority, including any persons appointed by them, in respect of any activity conducted under this Section 9.

9.3 To facilitate the Regulated Entity's ability to perform audit in respect of the Services in accordance with its regulatory obligations under Applicable Laws, Outpost24 shall, upon the Regulated Entity's request, provide the Regulated Entity with Outpost24's certificates and reports produced by external auditors/auditing firms or certification bodies as a result of any internal audits. The Regulated Entity may use such documents, and other information regarding the Services made available by Outpost24, to respond to a request from a Competent Authority regarding the Services. In addition, if requested by the Regulated Entity, Outpost24 will provide the Regulated Entity and/or the Competent Authority the opportunity to discuss such documents with Outpost24's personnel (e.g. a security or service expert). Such documentation may include, where applicable, Outpost24's ISO/IEC 27001 certification, SOC 2 Type II reports, and other independent audit or assurance reports relevant to the Services. The Regulated Entity may rely on such documentation for the purpose of fulfilling its regulatory obligations under Applicable Laws.

9.4 If the Regulated Entity or the Competent Authority determines that the activities under Section 9.3 are insufficient for the purposes of an audit or inspection under Applicable Laws (taking into account the principles in Section 1.2), the Regulated Entity and any Competent Authority, including any persons appointed by them, shall have an unrestricted right to:

(a) audit and inspect the Services used by the Regulated Entity to assess and verify compliance with Applicable Laws and the requirements under the Agreement;

(b) access Outpost24's business premises relevant for the provision of the Services used by the Regulated Entity, including the full range of relevant devices, systems, networks, information and data used for providing the Services, including related financial information, personnel and Outpost24's external auditors; and

(c) take copies of relevant documentation at the business premises if they are considered critical to the business operations of Outpost24.

9.5 Any exercise of the rights under Section 9.4 shall be made with reasonable prior notice and during regular business hours, unless it is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.

9.6 The scope, frequency, and duration of the rights under Section 9.4 shall be reasonably determined on a risk-based approach, considering, *inter alia*, the nature, scale and complexity of the Services and the related risk they pose to the Customer's business.

9.7 When such access and rights as set out in Section 9.4 are being exercised by the Regulated Entity and such other parties mentioned therein, appropriate caution shall be taken to ensure that the risk for Outpost24's services to other customers (including their environment) being affected are avoided or mitigated. If it is determined, in Outpost24's sole discretion, that an audit or inspection will affect the rights of other clients to Outpost24, the Parties shall agree on alternative assurance levels to mitigate such effects.

9.8 Outpost24 shall, for its assistance under this Section 9, be entitled to compensation for its verifiable costs, unless the audit reveals instances of Outpost24 materially breaching its undertakings under the Agreement.

9.9 The Regulated Entity shall not appoint a competitor of Outpost24 or a competitor of any of Outpost24's subcontractors as an auditor under Section 9.4 and any such third-party must possess the expertise and experience necessary to effectively perform the audit and/or inspection.

9.10 All information and documentation access or made available by Outpost24 in connection with any activity under this Section 9 are Outpost24's Confidential Information.

10. SPECIFIC TERMINATION GROUNDS

The Customer may terminate the Agreement, by giving written notice of at least thirty (30) days and not more than ninety (90) days, if:

(a) Outpost24 violates Applicable Laws and such violation has a material impact on the Services or the risk they pose to the Regulated Entity's business;

(b) impediments occur which are capable of altering the performance of the Services in a manner which materially increases the risk they pose to the Regulated Entity's business or adversely affects the Regulated Entity's ability to comply with its regulatory obligations under Applicable Laws, provided such impediments are not remedied or appropriately mitigated within reasonable time;

(c) there are evidenced material weaknesses regarding Outpost24's overall ICT risk management, particularly in regard to ensuring availability, authenticity, integrity and confidentiality, of Customer Data and security of Customer Data, which demonstrate that Outpost24 cannot fulfil its obligations in relation to ICT risk management under the Agreement;

(d) such instructions are given by the Customer's Competent Authority; and

(e) a subcontractor change under Section 7 (if applicable) is made in breach of this Appendix.

11. EXIT ASSISTANCE

11.1 The obligations set out in this Section 11 shall only apply where the Services support critical or important functions.

11.2 Upon termination or expiration of the Agreement or a relevant Quotation, Outpost24 will, with the aim of enabling transition of the Services to the Regulated Entity or to any vendor, service provider or other successor appointed by the Customer and reducing the risk of disruption to the Regulated Entity or ensuring its effective resolution and restructuring: (a) continue to provide the Services in accordance with the terms of the Agreement for a maximum of one (1) month (the "Transition Period"); and (b) enable the Customer to retrieve its Customer Data in source format and in a manner consistent with the functionality of the Services during the Transition Period, provided that the Customer complies with the Agreement and requests a Transition Period in writing before the relevant termination or expiration date. The Customer is only entitled to one (1) Transition Period. During the Transition Period, the Services shall be subject to the same terms as immediately prior to the termination or expiration date, save for any fee adjustments made in accordance with the Agreement.