FSI ADDENDUM (DORA)

This FSI Addendum (DORA) supplements the General Terms, Sales Order, or other written or electronic terms agreement between Adobe and Customer under which Adobe supplies Customer with Cloud Services, whether directly or indirectly and including all annexes and appendices ("Agreement").

1 Application of this Addendum

This Addendum is aimed at helping Customer, as a Regulated Entity, to meet its regulatory requirements imposed under Applicable Law. It applies where Customer is a Regulated Entity and is subject to oversight by the Regulator in relation to any Cloud Services procured under the Agreement. The respective rights and obligations of the Parties are described in writing in the applicable terms of the Agreement. This Addendum shall take effect the later of (i) January 17, 2025, or (ii) when executed by all parties.

2 Definitions

2.1 **"Adobe"** means Adobe Inc., Adobe Systems Software Ireland Limited, and any other Adobe entity which is party to the Agreement.

2.2 **"Applicable Law**" means the applicable laws and regulations administered by the Regulator in connection with the Regulated Entity's use of the Cloud Services.

2.3 **"Cloud Services"** means all the On-demand and Managed Services made available by Adobe or its Affiliates under the Agreement. References to Cloud Services in this Addendum refers to Cloud Services that constitute ICT services under DORA (referred to interchangeably in this Addendum as "Cloud Services" or "ICT services").

2.4 **"Customer Data"** has the same meaning as defined in the Adobe General Terms and shall include Customer Content if separately defined in the Adobe General Terms. Customer Data includes both personal and non-personal data.

2.5 **"DPA"** means the data processing agreement or data processing addendum, as applicable, between Customer and Adobe governing the processing of personal data by Adobe on behalf of Customer.

2.6 **"DORA Regulation" or "DORA"** means The Digital Operational Resilience Act published by the Official Journal of the European Union as Regulation 2022/2554 or any successor or update thereto (subject to such successor or update being in force).

2.7 **"ICT-related incident"** means a single event or a series of linked events unplanned by the Customer that compromises the security of the network and information systems, and have an adverse impact on (i) the availability, authenticity, integrity or confidentiality of data of the Regulated Entity, or (ii) on the services provided by the Customer.

2.8 **"ICT services"** has the meaning as defined under DORA Regulation.

2.9 **"Regulated Entity"** means the Customer or the Customer's End User if and so long as such entity is regulated by or subject to oversight within the meaning of Article 2 of the DORA Regulation.

2.10 **"Regulator"** means a government or regulator body in the European Union, with binding authority to regulate, supervise or govern Regulated Entity's financial or insurance services activities under DORA, including the resolution authorities of Regulated Entity.

2.11 If a term is not defined, it shall have the meaning as defined in DORA or the underlying Agreement.

3 Key Contractual Provisions for ICT services

3.1 **Description of functions and ICT services.** The description of the functions and ICT services is described in the Agreement governing the Customer's use of Cloud Services provided by Adobe.

3.2 **Locations for the provision of ICT services.** For all Cloud Services, Adobe offers data storage and processing locations in the European Union or United Kingdom. Customer Data storage and processing locations are specified at https://www.adobe.com/privacy/sub-processors.html. The data storage processing locations might be added or changed in connection with the ICT Services in case Adobe engages a new subcontractor and Customer will be informed in line with the process agreed under the Data Processing Addendum in such case.

3.3 **Availability, authenticity, integrity and confidentiality in relation to the protection of data.** Adobe's obligation with regards to the availability, authenticity, integrity and confidentiality are set forth in the DPA and Agreement. Notwithstanding the above, at its own discretion, Adobe has implemented, maintains and regularly tests the security of its Cloud Services and will continue to do so during the term of this Addendum. A list of certifications and attestations for the Cloud Services are available at https://www.adobe.com/trust/compliance/compliance-list.html; detailed information including access to the certifications and attestations can be found in Adobe's Trust Center available at: https://www.adobe.com/trust.html.

3.4 **Access, recovery and return of Customer Data.** In the events defined in Art. 30 par. 2 (d) DORA, Customer Data stored within the Cloud Services will be available to Customer for 30 days in the same format then available within the reporting interface(s), unless specified otherwise in the respective PSLT.

3.5 **Service level descriptions, including updates and revisions thereof** are defined in the applicable Agreement including the applicable Adobe service level agreement(s) as agreed by the Customer and Adobe or, if not specifically agreed, available at: https://www.adobe.com/uk/legal/service-commitments.html.

3.6 **Provision of assistance when an ICT incident occurs.** Adobe shall provide necessary assistance to Customer when an ICT-related incident that is related to the Cloud Service provided to Customer occurs. Unless other incident support or reporting procedures are agreed between Adobe and Customer, in the event of the occurrence of an ICT-related incident that could have a negative impact on the continuity or security of the Cloud Services, Adobe will, without undue delay:

- 3.6.1 notify Customer of the ICT incident;
- 3.6.2 provide Customer with reasonably requested information Adobe has on the ICT incident that Customer needs to secure Customer's functions at risk due to the ICT incident; and
- 3.6.3 provide Customer with reasonably requested information on how Adobe handled the ICT incident.

3.7 **Cooperation with competent authorities and resolution authorities of Customer.** To the extent required under Applicable Law, Adobe shall reasonably cooperate with the Regulator, including with persons appointed by the Regulator, for requested information regarding the Cloud Services provided to Customer, so long as Customer does not otherwise have access to the relevant information.

3.8 **Termination Rights and Minimum Notice Period.** In addition of termination rights mentioned in the Agreement, Customer may terminate the Agreement, in whole or in part:

- 3.8.1 In any of the circumstances set forth under Art 28, par. 7 DORA;
- 3.8.2 if the Regulator requires with a formal request to do so;
- 3.8.3 if Customer is entitled to exercise its termination right pursuant to the service level agreement (see section 3.6 of this Addendum);
- 3.8.4 if Adobe is unable to demonstrate compliance with the requirements concerning the security of network and information systems standards as defined by DORA Regulation;

provided, however, (1) the aforementioned termination rights are limited to Cloud Services that are subject to this Addendum, and (2) that Customer must give written notice describing the nature and basis of the breach to Adobe and Adobe has failed to cure the breach within 30 days after receipt of Customer´s breach notice.

3.9 **Adobe Security Awareness Programs.** Adobe personnel complete security awareness training, which

includes annual updates about relevant policies, standards, and new or modified attack vectors and how to report security events to the appropriate response team. Records of annual training completion are documented and retained for tracking purposes.

4 Confidentiality

The existence and terms of this Addendum and any information, responses and documentation provided by Adobe or by Customer in connection with this Addendum will be treated as Confidential Information of the party owning it, unless (1) it has become public knowledge through no fault of the receiving party; (2) was known to the receiving party, free of any confidentiality obligations, prior to disclosure by the disclosing party; (3) becomes known to the receiving party, free of any confidentiality obligations, from a source other than the disclosing party; (4) is independently developed by the receiving party without the use of Confidential Information ("Confidential Information"). Confidential Information will not be disclosed by the receiving party, except that Confidential Information may be disclosed to the Regulator, provided that the disclosing party obtains confidential treatment or similar protections, and (b) to the affiliates and advisors of a party provided he disclosing party and affiliate(s)/advisor(s) enter into confidentiality terms ensuring the same level of confidentiality protection as defined in this Addendum.

5 Miscellaneous

Customer's sole and exclusive remedy for any breach by Adobe in relation to this Addendum is to terminate this Addendum and the applicable Agreement for the affected Cloud Services. For the purposes of this Addendum, the rights and obligations of the parties in this Addendum are in addition to, and not in re placement of, the rights and obligations of the parties in the Agreement, except that this Section will prevail over any conflicting term in the Agreement. Except as amended by this Addendum, the Agreement will remain in full force and effect.

Except to the extent otherwise mandated by Applicable Laws, this Addendum will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.