

DORA Addendum

This DORA Addendum (“Addendum”) supplements the terms and conditions described in the Contract Documents (collectively the “Agreement”) that apply to Customer’s or Partner’s use of Company Service . This Addendum applies only if Customer is subject to the Digital Operational Resilience Act (DORA), (Regulation (EU) 2022/2554), commonly known as DORA. This Addendum sets forth the terms of the parties’ agreement to follow DORA.

Notwithstanding anything contrary in any other Contract Document, where this Addendum applies, the Contract Documents also apply.

I. Defined Terms

Capitalized terms used but not defined in this Addendum shall have the same meaning as provided in the Agreement. The following definitions are used in this Addendum:

“Applicable Law” means any law, rules or regulation applicable to Company or Customer.

“Business Unit Terms” means a Company operating unit supporting a specific Product for which additional Product specific terms are defined and stated at <https://www.cloud.com/content/dam/cloud/documents/legal/business-unit-terms.pdf> as referenced in the Agreement.

“Cloud Service Terms” means software-as-a-service offerings made available via a remote network provided in accordance with the terms located at <https://www.cloud.com/content/dam/cloud/documents/legal/cloud-services-usage-terms-and-conditions.pdf> as referenced in the Agreement.

“Company Service” means Company’s generally available Products accessed via a remote network and Updates.

“Contract Documents” means the Order, End User Agreement, MPA where applicable, Cloud Service Terms, Business Unit Terms, Data Processing Addendum, Security Exhibit, contents of the Trust Center located at <https://www.cloud.com/trust-center> and this Addendum.

“Customer” means, for the purpose of this Addendum, the Customer or Partner and any of its Affiliates (as defined in the Agreement) who are subject to DORA and are using Company Services.

“Customer Data” has the same meaning as Customer Content in the Agreement and includes both personal and non-personal data.

“DORA Regulation” or “DORA” means the Digital Operational Resilience Act (DORA), (Regulation (EU) 2022/2554), commonly known as DORA, and is a European Union (EU) financial regulation that requires financial institutions, and their suppliers to implement regulatory requirements to address digital resiliency against cyber attacks. This Addendum is an agreement between the parties to follow DORA as part of the licensing of Products.

“Data Processing Addendum” or “DPA” means the data processing agreement between Customer and Company governing the processing of personal data by Company on behalf of Customer located at

<https://www.cloud.com/trust-center/cloud-software-group-data-processing-agreement>, as incorporated in the Agreement.

“ICT-related Incident” has the meaning defined under the DORA Regulation.

“ICT Services” has the meaning defined under the DORA Regulation.

“Order” means a document or combination of documents memorializing Customer’s purchase of Company Service (including an order form, quote, Purchase Order, on-line Order, or other form of an ordering document) submitted by Customer to (i) Company, (ii) a Company Authorized Reseller, and/or (iii) through Company Product websites as defined in the Agreement.

“Regulator” means any European financial service regulator or national competent authority that has the monitoring or supervisory rights, as specified in Art. 26 (Competent Authorities) of the DORA Regulation, over Customer and/or Company as the provider of Company Service to Customer.

“Security Exhibit” means the manner in which Company develops and delivers Company Service, in accordance with the Services Security Exhibit at <https://www.cloud.com/trust-center/services-security-exhibit> as incorporated in the Agreement.

“Service Levels” means the service levels set forth under the Business Unit Terms of the Agreement that describe the delivery of Maintenance Services and Updates under the Agreement.

“Threat-led Penetration Testing” or “TLPT” has the same meaning as used in Art. 26 and 27 of the DORA Regulation.

II. Key Contractual Provisions for ICT Services

1. Allocation of Rights and Obligations

Pursuant to Art. 30(1) of DORA, the respective rights and obligations of the Customer and Company are set forth in the Contract Documents, available as a single electronic file upon written request.

2. Description of the Company Services and Subcontracting

- (a) Pursuant to Art. 30(2)(a) of DORA, a description of the Company Services is included in the Contract Documents. See specifically the Order and Business Unit Terms.
- (b) A list of subcontractors and changes thereto can be found on the list of sub-processors located at: <https://www.cloud.com/trust-center/sub-processor-list/>. Subject to Customer registering for the RSS notifications in accordance with the DPA, and pursuant to Art. 6 (1-3) of the Subcontractor Supplement, as defined below, if Customer establishes that material changes to the subcontracting arrangement expose the Customer to unreasonable risk, Customer may object to such change(s) within ten (10) days of the notification. In the absence of an objection, Customer is deemed to have accepted such change. Company may charge Customer on a time and materials basis for any costs associated with responding to Customer requests with respect to subcontracting under Parts 2(b-c) of this DORA Addendum.
- (c) Company’s obligations Pursuant to COMMISSION DELEGATED REGULATION (EU) 2025/532 adopted on 24.3.2025 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the elements that a financial entity has to determine and assess when subcontracting ICT services supporting critical or important functions (“Subcontractor Supplement”), include the following,
 - (i) Pursuant to Art. 4(1)(a) of the Subcontractor Supplement, Company is responsible for the provision of Company Services by the subcontractors;
 - (ii) Pursuant to Art. 4(1)(b) of the Subcontractor Supplement, Company shall monitor all subcontracted ICT services supporting a critical or important function to ensure compliance with the Agreement,
 - (iii) Pursuant to Art. 4(1)(c) of the Subcontractor Supplement, upon written request from Customer, Company shall provide a summary of findings from monitoring subcontractors relevant to the Company Services deployed by Customer;

- (iv) Pursuant to Art 4(1)(d) of the Subcontractor Supplement, Company shall assess all risks associated with the location of the current or potential subcontractors providing ICT service supporting a critical or important function or material part thereof, and its parent company and the location where the ICT service is provided from;
- (v) Pursuant to Art. 4(1)(e) of the Subcontractor Supplement, Company shall specify the location of data processed or stored by the subcontractor, where relevant;
- (vi) Pursuant to Art. 4(1)(f) of the Subcontractor Supplement, Company shall include in its subcontractor agreements monitoring and reporting obligations of the subcontractor towards Company.
- (vii) Pursuant to Art. 4(1)(g) of the Subcontractor Supplement, Company shall ensure the continuity of the Company Services supporting critical or important functions throughout the chain of subcontractors in case of failure by a subcontractor to meet its contractual obligations, that subcontracts include the requirements on business contingency plans as set out under Article 30(3)(c) of Regulation (EU) 2022/2554, and subcontracts meet the service levels necessary in relation to these plans;
- (viii) Pursuant to Art. 4(1)(h) of the Subcontractor Supplement, Company shall ensure that subcontracts meet the requirements of Art. 30(3)(c) of the DORA Regulation in relation to business continuity and security measures;
- (ix) Pursuant to Art. 4 (1)(i) of the Subcontractor Supplement, Company shall ensure that subcontracts meet the requirement of Art 30(3)(e) in relation to access, inspection and audit;
- (x) Pursuant to Art. 4(1)(j) and Art. 5 of the Subcontractor Supplement, Customer shall be notified of material changes to subcontracting arrangement subject to Customer registering for the RSS notifications in accordance with the DPA.

3. Data Locations

Pursuant to Art. 30(2)(b) of DORA, Customer Content that Company processes on behalf of the Customer shall be processed, transferred, and stored as stated in the DPA located at <https://www.cloud.com/trust-center/cloud-software-group-data-processing-agreement>. The locations (i.e., the regions or countries) where the Company Services will be provided and where Customer Content is to be processed, including the storage location, are set out in the sub-processor list located at <https://www.cloud.com/trust-center/sub-processor-list>.

4. Protection of data

Pursuant to Art. 30(2)(f) of DORA, Company's obligations with regard to the availability, authenticity, integrity, and confidentiality in relation to the protection of data, including personal data, as well as the terms ensuring access, recovery, and return of personal data, are stated in the DPA and Agreement. Pursuant to Art. 30(3)(c) of DORA, a list of certifications for the Cloud Services are available in the Trust Center, located at <https://www.cloud.com/trust-center>.

5. Access, recovery and return of Customer Data

Pursuant to Art. 30(2)(d) of DORA, Customer controls access to its Customer account, and Customer Data, including upon termination or expiration of Company Services, or in the unlikely event of Company insolvency, as stated in the Cloud Service Terms incorporated in the Agreement.

6. Service level descriptions

(a) Pursuant to Art. 30(2)(e) and 30(3)(a), Service Level Descriptions (hereinafter "SLD") for Company Services, are defined in the Agreement, or if not specifically agreed, are located at:

(i) As to Citrix Company Services, SLD are described at <https://docs.citrix.com/en-us/citrix-cloud/overview/service-level-agreement.html>;

(ii) As to TIBCO, Spotfire, ibi, and Jaspersoft, Company Services SLD are described at <https://www.cloud.com/content/dam/cloud/documents/legal/service-level-guide.pdf>.

(b) Pursuant to Art. 30(3)(b), and in accordance with Section 11 of the Security Exhibit, Customer will be notified of any development that may result in a material impact on Company's ability to provide the Company Service.

7. ICT-related Incident Support

(a) Pursuant to Art. 30(3)(b), where Company Service is a critical service, Company will promptly and without undue delay notify Customer upon becoming aware of any developments that may cause a material impact to Company's ability to provide the Company Service.

(b) Pursuant to Art. 30(2)(f) of DORA, Company shall provide required assistance to Customer regarding ICT-related Incidents. The DPA, Security Exhibit and applicable Business Unit Terms further describe Company's response and obligations should such incident arise. Customer is responsible for the costs of any such investigation unless Company Services are found to be the source of the incident.

(c) Where Company incurs costs for ICT-related Incident Support unrelated to Company Services, Company shall invoice Customer for such costs at a rate determined to be commercially reasonable.

8. Cooperation with Regulators

(a) In the event a Regulator initiates an onsite audit or inspection, or requests information from Company, pursuant to Art. 30(2)(g) of DORA, Company shall fully cooperate as it relates to access to such information for the purposes of determining compliance with DORA.

(b) Upon 30 days' prior written notice to Company that Company Services support critical or important functions for Customer, as such term is used in DORA, pursuant to Art. 30(3)(e), Customer may have unrestricted rights of access, inspection, monitor and audit Company and the right to take copies of relevant documentation on-site if they are critical to the operations of the Company, as determined by Company.

(c) Pursuant to Art. 30(3)(e), and to the extent required to cooperate with Regulators, this Addendum shall not impede or limit Customer right to take copies of relevant documentation on-site if they are critical to the operations of the Company.

(d) The following guidelines shall apply to each audit, inspector or monitoring event:

(i) Such events shall be conducted in a manner that avoids any unreasonable or unnecessary disruption to Company's operations and shall be limited to one audit or inspection per year, unless Customer determines that a greater frequency of audits is necessary on the basis of a risk-based approach Pursuant to Art. 28(6) of DORA and incorporates such frequency at the time it enters the Order for Company Services.

(ii) Such events shall be conducted in accordance with Company security-related policies and procedures to ensure the safety of the persons involved and to protect the security and confidentiality of Customer Content.

(iii) Any information and documentation provided by Company or its auditors in relation to such an event shall be treated by Customer, its Affiliates, Customer Auditors, and the Regulator as Confidential Information of Company.

(iv) Customer shall provide Company with a copy of any final report unless prohibited by Applicable Law, shall treat the findings as Confidential Information in accordance with the terms of the Agreement (or confidentiality agreement entered into between Customer and Company), and use it solely for the purpose of assessing Company's compliance with the terms of the Agreement, this Addendum and Applicable Law.

9. Customer Termination Rights

Pursuant to Art. 28(7) of DORA, Customer may terminate a Company Service upon 30 days' prior written notice and Company's failure to cure a Company Service under the following scenarios.

a) Upon the formal request of a Regulator. Company's significant breach of Applicable Law or its obligations under this Addendum, that are identified in an audit and not promptly remediated;

b) Company's inability to demonstrate its compliance, or ability to follow the requirements of the DORA Regulation;

c) Any of the circumstances set forth in Art 28(7) of the DORA Regulation;

d) Company's failure to respond to an ICT-related Incident pursuant to the requirements of the DORA Regulation;

e) Any of the circumstances set forth in Art. 6 of the Subcontractor Supplement;

f) Pursuant to customer's rights under the DPA, if Customer does not approve of material changes to subcontracting arrangements, Customer may terminate any subscription for the affected Company Service without penalty or termination fee by providing, before the end of the applicable notice period, written notice of termination. Upon termination, Company shall remove payment obligations for any of the terminated subscriptions.

10. Business Continuity

(a) Pursuant to Art. 30(3)(f) of DORA, upon termination of the Company Services pursuant to Section 9 above, Company shall continue to provide such services for a commercially reasonable period of time, at Customer's expense, to reduce risk of disruption, facilitate resolution and restructuring, including migrating to a new ICT Services provider as needed.

(b) Pursuant to Art. 30(3)(c) of DORA, Company has in place and tests business contingency and continuity plans as provided in Section 10 of the Security Exhibit.

(c) Customer shall pay Company all amounts owed for the terminated Company Service, which will become immediately due upon Customer exercising this termination right. No portion of any prepaid amounts, including any annual fees (if applicable) shall be refunded.

11. Customer's Training

Pursuant to Articles 13(6) and 30(2)(i) of DORA, Company's personnel directly involved in Customer's implementation of the Company Service may participate in Customer's relevant security awareness programs and digital operational resilience training. In this case, the conditions for the participation of Company's personnel in such programs shall be agreed in advance between the Customer and Company, at no additional cost to Company.

12. Threat-led Penetration Testing

Pursuant to Articles 26, 27 and 30(3)(d) of DORA, Customer may run, at no cost to Company, Threat-led Penetration Testing (as defined in DORA; hereinafter referred to as "TLPT") against their own dedicated Company Service environment, but shall work with Company to ensure that the TLPT does not impact any other customer of Company. Company shall participate and cooperate with Customer as per the process required to be followed for a TLPT, available on the Company Trust Center in the Cloud Assurance section located at <https://www.cloud.com/trust-center/security-assurance>. Company further reserves the right, pursuant to Art. 26(4) of DORA, to engage an external tester for the purpose of conducting pooled TLPT if TLPT is reasonably expected to have an adverse impact on the quality or security of Company Services.

III. Miscellaneous

1. Confidentiality

This Addendum, any other Contract Document, any findings from an audit, inspection or monitoring, and all information regarding and provided by Company are Company Confidential Information. Notwithstanding the foregoing, Customer may disclose these items to a Regulator provided that (i) Customer first redacts all terms that are unrelated to regulatory oversight and approval, including pricing information and order quantities, and (ii) other than disclosures to a Regulator, Customer must comply with the Confidentiality terms of the Agreement as if the disclosure was a disclosure of Company Confidential Information by Customer.

2. Term and Termination

This Addendum shall terminate automatically upon termination of the Agreement.

3. Conflict

Notwithstanding anything contrary in this Addendum, the Agreement remains unchanged and in full force and effect. If there is any conflict between any provision in this Addendum and any provision in the Agreement, this Addendum shall control.

4. Remedy

Customer's sole and exclusive remedy for any breach by Company in relation to this Addendum is to terminate this Addendum and the applicable Agreement for the affected Company Services. For the purposes of this Addendum, the rights and obligations of the parties to this Addendum are in addition to, and not in place of, the rights and obligations of the parties to 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 the governing law and jurisdiction provisions in the Agreement.