boomi

DORA Mapping for Boomi Services

This document is designed to help EU financial entities assess how their use of Boomi's services aligns with the requirements of the EU Digital Operational Resilience Act (DORA). Specifically, it maps the Article 30 DORA requirements and how Boomi addresses these requirements to provide our customers with adequate provisions to comply with DORA.

This document is for informational purposes only. While the information provided is reliable, it should not be the sole basis for any purchasing decisions. It does not constitute legal or professional advice, and Boomi may update the content of this DORA Mapping Document as regulatory or security requirements evolve. We recommend that customers seek independent legal and compliance advice to support their own DORA compliance efforts.

For the purposes of this document:

"Contract" means the MSA, the DPA, the FSA.

"DPA" means Boomis' Data Processing Addendum, as amended from time to time, available at www.boomi.com/dpa.

"Documentation" has the meaning given to it in the MSA, as amended from time to time.

"FSA" means Boomi's Financial Services Addendum, as amended from time to time.

"MSA" means Boomi's Master Services Agreement, as amended from time, available at www.boomi.com/msa.

"Securityy Schedule" means the Boomi Security Schedule attached to the DPA.

"Services" has the meaning given to it in the MSA.

"SLA" means the Service Level Agreement for the Boomi Services (www.boomi.com/sla) or Managed Cloud Services (www.boomi.com/mcs_sla),as amended from time.

boomi

DORA requirement (Art. 30)	Context	Boomi provision
1. The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing. The full contract shall include the service level agreements and be documented in one written document which shall be available to the parties on paper, or in a document with another downloadable, durable and accessible format	The rights and obligations of the parties are set out in the Contract, which incorporates the Documentation, the Compliance Page and the SLA.	Documentation, incorporated into MSA Compliance Page SLA
2a: a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting;	The clear and complete description of our services can be found in the Documentation, including Boomi Compliance Page. Boomi's DPA specifies our Subprocessors for transparency. Further info on Boomi's privacy program is included on the Compliance Page at https://help.boomi.com. Boomi's list of subprocessors is found at https://boomi.com/sub-processors.	MSA section 1.3 and section 8.1 DPA section 3 FSA section 2
2b: the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity in advance if it envisages changing such locations;	These locations are referenced at https://boomi.com/sub-processors. The customer can subscribe to updates to be informed about any changes. The DPA and the FSA provide for objection rights and termination in the event the Boomi Services, cannot be provided without the updated subprocessor.	DPA section 3 FSA section 3

2c provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;	Our Security measures for ensuring availability, authenticity and integrity are described in our Security as an Annex of our Data Processing Agreement This is part of the DPA. Availability is addressed by our SLA.	DPA Annex 1 SLA
2d provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements;	Customers can export their integrations via our platform (see here or via the API here). As the documentation at https://help.boomi.com is part of the MSA, this is addressed there.	MSA section 1.3 and section 8.1
2e service level descriptions, including updates and revisions thereof;	Boomi's SLA provides an above market standard 4 9s (99.99%) availability. Updates will be published via the website.	SLA
2f the obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex-ante, when an ICT incident that is related to the ICT service provided to the financial entity occurs;	As a SaaS provider Boomi, will notify, remediate and report on security incidents resulting in the destruction, loss, alteration, unauthorised disclosure of, or access to the data of a Financial Institution.	FSA section 2 DPA section 5
2g the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them;	The FSA sets out our duty to cooperate with any competent authority in exercising the information, audit and access rights.	FSA section 5

2h termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities;	The FSA provides for additional termination rights, necessary to comply with DORA.	FSA section 8
2i the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6).	Art. 13 (6) requires third-party vendors to be part of trainings "where appropriate". Art. 13 (6) stipulates that these are aimed at "all employees" (incl. The management) of the Financial Institution to ensure that the staff is aware of ICT related risks. Customers generally operate the services independently of Boomi. Given the 'one to many' nature of a SaaS platform Boomi does not have personnel dedicated to delivering services to an individual customer. Boomi does provide implementation services and all Boomi staff are provided training.	Not Applicable
3. The contractual arrangements on the use of ICT services supporting critical or important functions shall include, in addition to the elements referred to in paragraph 2, at least the following:		

3a: full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow effective monitoring by the financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met;	Our SLA sets out measurable performance targets for the services. Customers can monitor availability on an ongoing basis via https://status.boomi.com. Customers can subscribe to updates via our status page. If the services do not meet the SLA, Customers may claim service credits in accordance with the SLA.	MSA section 8.1 FSA section 2 SLA Boomi's Support Services https://www.boomi.com/legal/service
3b: notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material impact on the ICT third-party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels;	We provide real time information to our customers via https://status.boomi.com, about material impacts to our services. Boomi shall promptly notify Customer in writing of becoming aware of any security incidents that can reasonably be expected to have a material impact on Customer and affect the Customer's Data.	FSA section 2 and section 3
3c: requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the financial entity in line with its regulatory framework;	Boomi's MSA, FSA and DPA provides appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity and resilience of processing systems as part of the Boomi Services.	DPA section 4 Security Schedule FSA section 3

	Boomi has in place and tests Disaster Recovery and Business Continuity Plans, as set out in FSA. Summary of our DR / BCP are provided via our compliance page Business continuity is part of the ISO 27001 standard (control A.17.1 and A.17.2) under which Boomi is certified together with multiple other frameworks which can be found at https://boomi.com/compliance.	
3d: the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27;	Boomi's platform is subject to regular penetration tests (e.g., as part of our ISO 27001 certification) and security reviews. These penetration tests are only performed by sufficiently qualified personnel to ensure that our products meet the highest security standards. As our runtimes can be deployed within customers premises, our FSA provides customers with the right to conduct penetration testing on such locally deployed runtimes. As our platform is provided to all of our customers, a TLTP by a customer can negatively impact our other customers. In these cases, we will use external testers to perform pooled testing in accordance with Article 26 (4).	FSA section 3
3e: the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which	The FSA provides for monitoring and audit of Services in accordance with Dora.	FSA section 5

entails the following: (i) unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;	Our Status page provides real-time information on service performance. As a cloud services provider, we rely on 3rd party service providers to provide our services to our customers (e.g., cloud hosting providers). Due to the nature of our product, we can't provide access to all of our subprocessors' premises, but we follow the "alternative assurance levels" approach (see below).	
(ii) the right to agree on alternative assurance levels if other clients' rights are affected;	Due to the nature of our Service, we provide additional assurances through certifications and 3rd party audits. Boomi provides compliance documentation issued by accredited third parties who produce certifications and attestations, including, but not limited to, ISO 27001 / 27701, SOC Reports (type 2), Cyber Essentials Plus, and other standards. To learn more about which compliance offerings are available visit our compliance page These "alternative assurance levels" will help our customers to comply with DORA.	FSA section 5

(iii) the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and	See above (section 2g). Boomi will fully cooperate with authorities and/or other auditors and will provide information in compliance with the FSA.	FSA section 5 / 6
(iv) the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;	Details of the scope, procedures to be followed and frequency of any such audit are set out in the FSA. Customers must ensure that any such audit is conducted accordingly.	FSA section 5
3f: exit strategies, in particular the establishment of a mandatory adequate transition period: (i) during which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring;	Exit strategies are the responsibility of the Customer. Boomi as a service provider can't oversee the complete business of the customer which might require the customer to terminate the relationship. Under the FSA Boomi will provide (i) access to the services for a pre-determined additional period (ii) commercially reasonable support in relation to such exit planning - the scope and cost of which to be agreed between the parties. Boomi's Documentation provides customers with information on how to migrate to another service provider.	FSA section 9

(ii) allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.	See above	FSA section 9
26(4) Without prejudice to paragraph 2, first and second subparagraphs, where the participation of an ICT third-party service provider in the TLPT, referred to in paragraph 3, is reasonably expected to have an adverse impact on the quality or security of services delivered by the ICT third-party service provider to customers that are entities falling outside the scope of this Regulation, or on the confidentiality of the data related to such services, the financial entity and the ICT third-party service provider may agree in writing that the ICT third-party service provider mdirectly enters into contractual arrangements with an external tester, for the purpose of conducting, under the direction of one designated financial entity, a pooled TLPT involving several financial entities (pooled testing) to which the ICT third-party service provider provides ICT services. That pooled testing shall cover the relevant range of ICT services supporting critical or important functions contracted to the respective ICT third-party service provider by the financial entities. The pooled testing shall be considered TLPT carried out by the financial entities		

participating in the pooled testing. The number of financial entities participating in the pooled testing shall be duly calibrated taking into account the complexity and types of services involved.		