boomi

Boomi Privacy

White Paper on Data Transfers

Published 08 December 2025

Content

Boomi: Data Transfers

Overview

This documentation provides information about the privacy and security of the Boomi Services, to help you, our customer, assess our privacy and security programs, including where required, privacy impact assessments. This document does not constitute legal advice, and you should consult with your own legal counsel.

As an integration tool, Customers may use Boomi to send data to various applications, databases or other endpoints. The Customer, not Boomi, is responsible for where it sends its data. The following describes the data transfers associated with the Boomi Services only, absent of considerations of where your destination applications are located.

Depending on your preference, a Boomi runtime can be deployed to Boomi's public runtime cloud, or some other agreed location, or to customer owned infrastructure (on-premise). It is important to note that business data that processes through an on-premises runtime, runtime cluster or runtime cloud does not by default flow through the Boomi data center. The resulting data and logs are stored on the customer owned infrastructure (either on-premises or in their cloud). For more information on the various deployment options please consult our detailed documentation at www.boomi.com/compliance.

Boomi shall process data, in accordance with the underlying customer Service Agreement and the product documentation and Boomi will not retain, use, or disclose that personal data for any purpose other than for the purposes set out in the Service Agreement. In no event will Boomi sell any personal data.

Boomi Services

Boomi takes the security and privacy of our customers and their underlying customers and data subjects seriously. We appreciate the trust our customers put in us. Our customer base is the biggest in the integration platform as a service (iPaaS) field, and includes various governmental (and quasi) governmental entities around the world, financial services, pharma and other companies, operating within regulated industries.

As one of the only iPaaS vendors that is FedRAMP Authorized, and a company with over 20 years in business, we are constantly working to ensure that our compliance meets the stringent standards set by governments, tens of thousands of customers, and all of their thoughtful security & privacy organizations. More details of our global compliance programs, not just privacy, can be found at www.boomi.com/compliance.

As a global business, Boomi pegs its Privacy Compliance Program to GDPR, as the foremost leading privacy regulation throughout the world. This means that to the extent that we transfer data internationally (ie outside the EEA, inc UK) as required to provide the services to you, such transfers are undertaken in accordance with the provisions of the GDPR, the new standard contractual clauses (inc the ICO data transfer provisions in the UK where applicable) and our Data Privacy Framework certification which allows Boomi to transfer personal data to the US without the need of additional contractual frameworks - which we will leave in place as a fallback though. This is all confirmed for you in your Service Agreements and the Data Processing Agreement.

Data protection laws require an element of partnership between vendor and customer - this document reinforces our commitment to you, our customer, to understand key parts of the Boomi Services (and to assist you in completing any PIA).

Boomi and Security

Overview

GDPR requires organizations (whether acting as controller or processor) to use appropriate technical and organizational measures to ensure a level of security appropriate to the risk, to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access. Boomi operates robust privacy and security programs to enable Boomi and our customers comply with applicable privacy laws. The Boomi Services include a variety of security controls, policies and procedures, which are described in the

Documentation (as defined in the Service Agreement) at https://help.boomi.com. Our services operate in a multi-tennant architecture, designed to segregate and restrict access to customer data based on business needs.Boomi has a collection of industry-standard third party certificates (ISO 27001, SOC2, etc.) and audit reports, details are set out on our Compliance Page.

Managing Security

Security is the joint responsibility of both Boomi and you, the Customer. While Boomi has robust policies and procedures to protect the security of the Boomi Services - details of which are available via the Compliance Page or the Boomi Documentation, the customer retains responsibility for configuring the relevant Boomi security controls and/or managing the processing of data under its control.

Technical and Organisational Measures

As a Platform, Boomi adopts a single standard of security for all its customers. The technical, administrative, and organizational security measures deployed by Boomi for the protection of customer data, including personal data submitted by customer to the applicable Boomi Service are set out in our Security Schedule, which forms part of the service agreements.

Boomi and your Personal Data

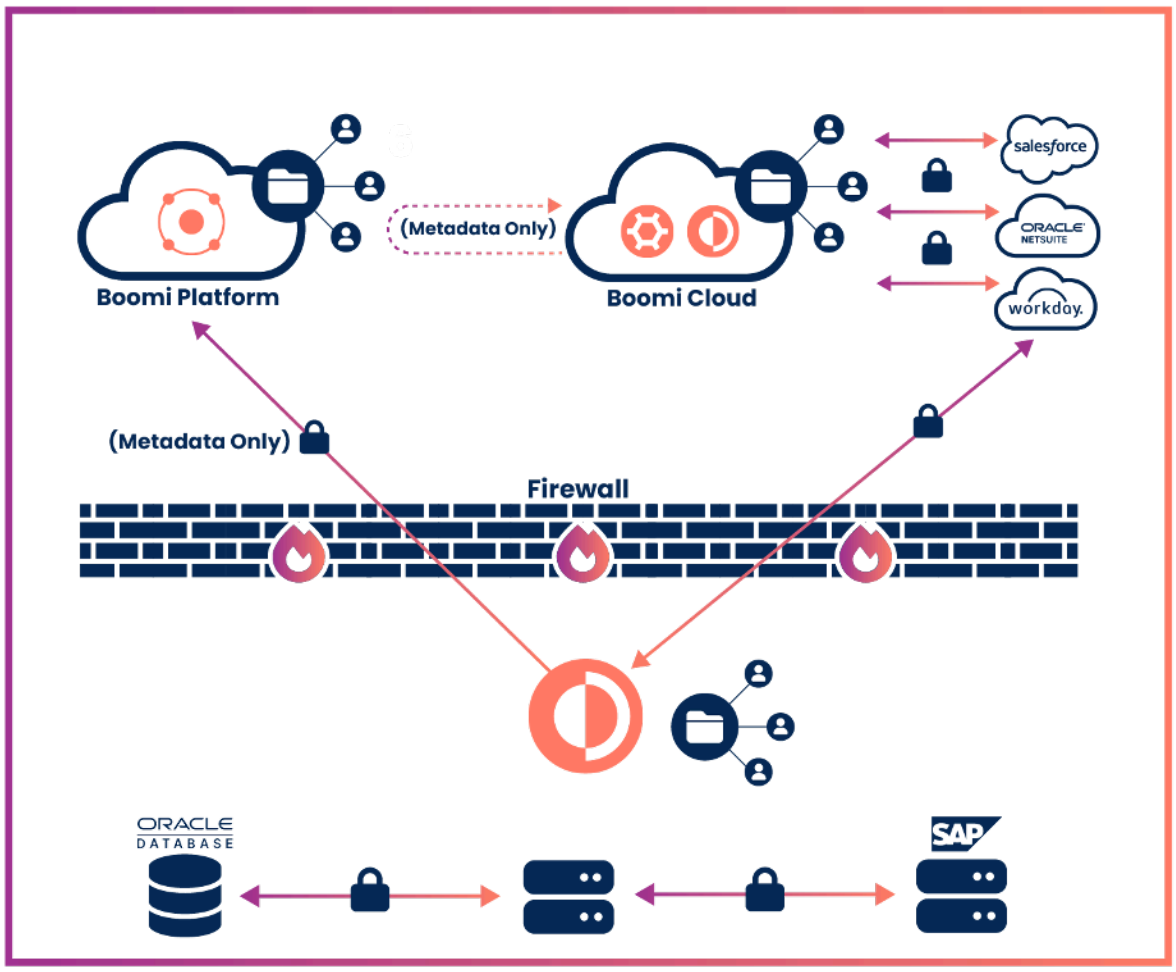
Description of Personal Data

Customers retain control over their data, and choose what data is processed by them through the Boomi Services. This will depend on your use case and application of the Boomi Services, but may include customer / employee names, email addresses or other personal data so selected by you, the Customer.

Where Customers choose “special categories of personal data” or other sensitive data (such as financial account number of health information), they remain responsible for ensuring that any such data submitted and/or processed via Boomi Services compiled with the applicable laws and any contractual restrictions which may be in place.

Data Flows

Further information on Boomi data flows is set out at https://boomi.com/compliance.



International Transfers

Under GDPR, personal data cannot be transferred outside of the EEA unless (i) the recipient country has been deemed adequate (which is the case for Boomi due to its Data Privacy Framework certification) or (ii) suitable safeguards have been put in place to ensure the personal data transferred is afforded the same level of protection.

Where transfers of personal data are required in order to provide the Boomi Services as set out in the Service Agreement, Boomi utilizes Standard Contractual Clauses - a suitable safeguard - as a fallback. This will ensure GDPR compliance of our customers even if other measures (like our Data Privacy Framework) can't be used.

Our DPA includes not just the EU Commission's new 2021 Standard Contractual Clauses, but also the ICO's international transfer addendum to the SCCs, to facilitate the transfer of personal data from the UK. Due to the length of the SCCs and the ITA, we have chosen to incorporate these by reference by way of Annex 3 to the DPA, with all the relevant information (and options) set out there.

Given the nature of our services, and in order to provide you the Customer with utmost flexibility, our DPA incorporates both Module 2 (Controller to Processor) and Module 3 (Processor to Processor) of the SCCs. These will apply depending on the relationship between Customer and Boomi (e.g., when using Boomi in a group of companies), and there is no need to make any amendments to the DPA should the underlying classification of you, the Customer, change.

Support Services

Boomi operates a 24-7 follow the sun support model, with support teams in Australia, Japan, India, Israel, UK, Ireland, Canada, and US, which benefit from the same privacy measures (e.g., adequacy decisions or standard contractual clauses) to ensure privacy compliant transfer of personal data.

Third Parties and your Personal Data

Where personal data is processed via the Boomi Services, it may be further processed by Boomi (its affiliates) or its subprocessors. Our list of subprocessors is set out at www.boomi.com/legal/sub-processors. Customers can subscribe for updates, in line with the general authorisation principle set out in the DPA.

Processing by Boomi and transfer of customer personal data for further processing by these subprocessors is subject to the Service Agreements (and in particular the Boomi DPA). As set out in the Service Agreement, in connection with the DPA, Boomi (i) takes responsibility for the actions of its Subprocessors; and (ii) has entered into a written agreement with each Subprocessor containing data protection obligations materially similar to those in our customer agreements.

Boomi's subprocessors are infrastructure subprocessors, which are required to deliver the Boomi Services to you, our customer - and including hosting providers (including AWS, as our platform and public cloud host and Azure for MCS deployments within Azure).

Storage of Personal Data

The underlying data which is processed by the customer is retained in the runtime database. As Boomi lets its users customize this element of the Boomi Services, the runtime may be (i) hosted by Boomi in an AWS or Azure Cloud (depending of the relevant service and deployment model), (ii) hosted by Boomi as part of a Managed Cloud Services or (iii) hosted on-premise by the Customer (whether behind their own firewall or in a chosen public/private cloud provider).

As a cloud based platform, personal data may flow between Boomi and various global locations (depending on your users and the specific hosting of your data inside your own applications).

Boomi's Services include Master Data Management, Data Integration, Managed File Transfer, API Management and other services, which are designed to allow the customer to maintain ownership of customer data, whilst providing state-of-the-art administration via Boomi's cloud.

Master Data Management (Master Data Hub)

Boomi's Master Data Hub allows customers to work with a master data solution, which provides one source for all of your data. The data hub can be hosted in one of our regions which are currently the US, EMEA and APJ.

Data Integration

Data Integration allows customers to transfer data via our Data Integration platform, which region depends on the customer's Rivery Console location. Whilst this data is integrated in real time, we allow the temporary storage of the data for up to 48 hours in our custom file zone for the further processing of this data. Customer data will only be accessed on specific request of the customer and the customer may also deploy the self-hosted custom file zone for the storage of their data (e.g., in the customer-owned S3 bucket). In case of self-hosting, access by Boomi to this data is not possible.

API Management

For API Management, personal data will not be stored unless you decide to upload it to our platform for debugging purposes. In these cases, personal data will be processed temporarily without permanent storage.

API Control Plane

The API Control Plane will allow you to discover, configure and govern your APIs. The traffic of the APIs, including its personal data, will not be transferred via Boomi's API Control Plane.

Managed File Transfer

Where customers are using Boomi's Managed File Transfer, the customer can choose between different regions to store their respective data. These are (currently) the US, UK, Germany and Australia. Both, the configuration and the storage of the data will be performed in this region, while also giving you control over the duration of the storage. Where you decide to use our dedicated cloud, you can choose between the available data centers which are provided by AWS and Azure. Retention of Personal Data. Boomi does not control data retention for customer on-premises runtimes. For customers that deploy on a Boomi managed runtime, customer data is deleted based on the particular service offering. For certain products, retention periods can be altered / reduced or increased by the Customer.
As set out in our customer DPA, Boomi deletes Customer personal data upon request at the end of the Customer contract. You will find our DPA at www.boomi.com/DPA.

Encryption

Details of Boomi's encryption are set out in the Boomi Documentation. Customer processed data is encrypted at rest and in transit. Customer Data may be encrypted between Boomi's Enterprise Platform and the customer chosen endpoints, when the relevant connectors support encryption.

GDPR

Data Protection Officer

Where legally required, Boomi appointed a Data Protection Officer. Boomi does also have a CIO, who leads security and product technical compliance certifications, while responsibility for privacy is with Boomi's Global Privacy Lead, who also serves as Data Protection Officer where required, as a part of Boomi's legal team. We also undergo ISO 27001, SOC1, SOC2, HIPAA, and other compliance audits every year. Details can be found at www.boomi.com/compliance. For questions or concerns with regard to privacy please contact Privacy@boomi.com.

Data Transfer Mechanism

In response to the Schrems II decision and the EDPB Recommendations, Boomi, when transferring personal data to Third Countries, as set out in the Boomi DPA, uses its Data Privacy Framework certification and where this doesn't apply, standard contractual clauses, pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4th June 2021 ("**EU SCCs**") and the UK international Data Transfer Agreement adopted on March 21st, 2022 ("**UK IDTA**"). Our standard DPA (for both our customer and our vendors) includes both the EU SCCs and the UK IDTA. With our acquisition of Rivery in 2024, we purchased an Israelian business. When transfers to Israel are taking place (e.g., due to support cases for the Rivery products), these transfers are happening on the legal basis of the adequacy decision for Israel and therefore don't need additional contracts like the Standard Contractual Clauses.

EDPB Recommendations on Supplemental Measures

Our TIA considers the EDPB Recommendations, based on the specifics of the international transfers undertaken by Boomi. Our revised DPA includes detailed descriptions of our Supplemental Measures.

Data Subject Rights

Privacy laws afford individuals whose personal data is processed certain rights (Data Subject Access Requests - "DSAR"), depending on where they are resident. These rights require companies to have systems in place to respond to and effectively address individual data subjects' requests. Due to the nature of the Boomi Services, you, the customer, retain all access to and control of your data to address such a DSAR. To the extent that Boomi holds such information, we will assist you, in line with our services agreement.

For questions related to this topic, please contact Privacy@boomi.com.

Governmental Access Requests

The EDPB Recommendations enable a customer to take into account the processor's practical experiences "with relevant prior instances of requests received from public authorities."

Boomi's Annual Transparency Report shows that Boomi has not received any governmental (from a third country) access request for EU data subject data.

Due to the nature of the Boomi Services, Boomi is not an electronic communications service under FISA 702 and Executive Order 12333. While the Cloud Act may, subject to a warrant, facilitate access by the US Government to data in a criminal investigation, Boomi does not voluntarily provide personal information on its customers and Boomi may technically not be able (due to the infrastructure of our products - see also our data flow document at https://boomi.com/compliance) to access customer data within customer's systems.

Data Breach Notifications

As part of Boomi's privacy program, Boomi works closely to address any issues relating to an alleged security incident. In the event of a confirmed security incident affecting your underlying personal data, Boomi shall, as required under GDPR and codified in our Service Agreements, notify you without undue delay.

Boomi Employees and confidentiality

All Boomi employees are bound by confidentiality obligations in their service contracts. Boomi confirms in our DPA, that employees processing personal data are suitably trained and have suitable conditional agreements in place. Our employees undergo annual data protection, privacy and security training.