Last updated: September 2022

Data Processing Addendum FAQ

Treasure Data offers to its Customers a Data Processing Addendum ("DPA") as part of its standard terms of business. We have created this FAQ to answer some of the most common questions we receive.

All defined terms used in this FAQ document are as set out in the DPA or related Terms of Service.

This FAQ document is provided for informational purposes only. It is not intended to provide legal advice and will not form part of the contract between the parties.

A. GENERAL

Where can I find a copy of the DPA?
It is published on Treasure Data's website. Please visit this webpage: https://www.treasuredata.com/terms/

What does the DPA cover?
It sets out the responsibilities of both parties in respect of the Processing of Personal Data that Treasure Data receives from Customer for the purpose of providing its Service. The DPA sets out contractual obligations binding upon Treasure Data in relation to – among others - the following areas:

- purpose limitation for the use of Personal Data;
- compliance with Customer's instructions regarding the Processing Personal Data;
- confidentiality of Personal Data;
- assistance to Customer for compliance purposes;
- data security (see section B below)
- notifications of Personal Data Breaches;
- restrictions to the engagement of Sub-processors (see section C below);
- restrictions on data transfers from certain jurisdictions (see section D below);
- Customer's audit rights.

Do I need to request the DPA to be included in my agreement with Treasure Data?
No, the DPA is part of Treasure Data's standard terms of business. Customers do not need to expressly request it to be part of their "contract pack". The DPA is incorporated into the Terms of Service by reference (see Section 1.3 of the Terms of Service).

Why can my organization not use its own data processing addendum instead of the DPA made available by Treasure Data?
The DPA has been drafted specifically to reflect Treasure Data's processes and practices in respect of the Service provided. The Service is provided to Customers using a "one-to-many" model, meaning the same SaaS service is provided to all of Treasure Data's Customers. Treasure Data does not offer a customized service offering that would allow Treasure Data to treat one Customer's data differently from other Customers' data. This also applies to our security practices that are backed by third-party SOC2 and ISO27001 certifications. These standardized controls are reflected in the DPA.
Treasure Data's DPA has also been drafted to seamlessly interoperate with Treasure Data's Terms of Service.

Does the DPA support my organization's compliance with the GDPR and the CCPA?
The DPA addresses the contractual requirements prescribed under art. 28(3) of the GDPR. It also incorporates the latest version (2021) of the Standard Contractual Clauses adopted by the EU Commission (see section D below).

The DPA includes a clause (see Clause 10) expressly addressing the CCPA and clarifying that Treasure Data acts in the capacity of a "service provider" for the Customer.

Does the DPA offer any protection to the Personal Data if my organization is not based in the EU or California?
Most of the commitments in the DPA are not specific to the GDPR or the CCPA: they bind Treasure Data regardless of where the Customer is based, and regardless of whether the GDPR or the CCPA applies to the Customer. All Customers can therefore benefit from those stringent privacy-related commitments that are legally binding upon Treasure Data in respect of all Personal Data.

B. TECHNICAL AND ORGANIZATIONAL MEASURES

What technical and organizational measures does Treasure Data have in place to protect Personal Data?
Treasure Data maintains a comprehensive security program. The Security Measures in place are outlined at Schedule 2 of the DPA.

For more information, please also visit our website: https://www.treasuredata.com/security/

C. SUB-PROCESSORS

Does Treasure Data use any third-party for Processing Customers' Personal Data?
Yes. Treasure Data only engages a Sub-processor:
(i) after a careful assessment of their security posture;
(ii) under a written contract requiring them to comply with stringent privacy commitments; and
(iii) after prior notification to Customers.
Please refer to the process set out under Clause 6 of the DPA.

The list of Sub-processors used by Treasure Data is publicly available on Treasure Data's website: https://www.treasuredata.com/terms/

How does Treasure Data notify Customers about the engagement of any new Sub-processor?
The published list of Sub-processors is updated from time to time. Customers may subscribe to notifications of any update to that list here.

D. DATA TRANSFERS

What is the "transfer mechanism" under the GDPR that is used for data transfers between Customer and Treasure Data?
The DPA incorporates by reference Module Two (Controller-to-Processor) of the 2021 Standard Contractual Clauses.

Can Treasure Data support my organization in carrying out a "transfer impact assessment" regarding transfers of Personal Data to Treasure Data?

Yes, information will be made available to existing Customers and prospects upon request. For requesting it, please get in touch with your contact at Treasure Data.

What about data transfers from the United Kingdom and Switzerland?
The DPA expressly covers transfers from these jurisdictions. Specifically, it incorporates by reference:
(i) the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018, Version B1.0; and
(ii) adaptations to the 2021 Standard Contractual Clauses for their use under the Federal Data Protection Act of 19 June 1992 (Switzerland).