Acquia Customer Data Platform

Last revision of this Product Notice: *[v1.1 – 17 May 2021 – hyperlinks updated]*
Prior version(s) of this Product Notice: *[v1.0 – 05 March 2021 – initial version]*

This Product Notices describes the privacy relevant aspects of the above-mentioned Acquia product/services.

About the Product
Acquia Customer Data Platform ("CDP") is a subscription cloud service that creates a persistent, unified database of shoppers, visitors, and other customers ("Third Party Users") Acquia's Customer, i.e. the subscriber to Acquia Customer Data Platform. CDP's database is accessible to other systems of Acquia's Customer (Customer as used in the respective Order Form or other relevant services agreement with Acquia), specifically data stored in the CDP can be used by other systems for analysis and to manage Third Party User interactions. CDP creates a comprehensive view of each Third Party User by capturing data from multiple systems, linking information related to the same Third Party User, and storing the information to track the Third Party User's online shopping, visiting, and browsing behavior over time. The stored information may be used to target marketing messages and track individual-level marketing results.

For details about this Product, please refer to the Product Description available online at https://docs.acquia.com/guide

1. Processing Operation(s)

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

- Processing of Personal Data to deliver its core functionalities required: ☒ yes ☐ no
- Optional features processing Personal Data: ☐ yes ☒ no
  - The optional features are deactivated by default: ☐ yes ☒ no ☐ n/a*
- Processing of sensitive Personal Data: ☒ yes** ☐ no ☐ n/a*
- Profiling of individuals based on personal characteristics: ☒ yes ☐ no ☐ n/a*
- Automated decision making that produces legal or other significant impacts on individuals: ☐ yes ☒ no ☐ n/a*

** (n/a = not applicable)*
*** (optional; depends on the Customer's configuration of the system, the connection to other systems, and the categories chosen by the Customer to be collected from Third Party Users)*

2. Details of Personal Data being processed

Categories of Personal Data	Categories of Data Subjects	Purpose of Processing	Categories of Data Recipients	Needed for Core Features	Processing Location	Acquia Inc. acts as Processor
Through the configuration, design, and administration of their own CDP instance, Customer in its sole discretion determines and controls the categories of data subjects collected by their CDP instance. Customer has full access and autonomy over what types of data is tracked and has access to this data and can manipulate it in various ways. Primarily, the categories of Personal Data could be individual identifiers, contact details, online identifiers, network activity, location data, travel data, expense and financial data, browsing information, and any sensitive data categories.	Through the configuration, design, and administration of their own CDP instance, Customer in its sole discretion determines and controls the categories of data subjects collected by their CDP instance. Customer has full access and autonomy over what types of data is tracked and has access to this data and can manipulate it in various ways. Primarily, the categories of Data Subjects could be Customer's end-users including visitors to Customer's website, online shop, or physical store.	Provision of the Services by Acquia to Customer	Customer's personnel	yes	Depends on the data center location chosen by customer; data collected in a given region will exist only within that region. Subprocessors, Support: see Acquia Affiliates	Yes

3. Privacy Enhancements

Objective	Technology / Measure	Data at Rest	Data in Transit
Anonymization and	Data anonymization at Customer level optional for	Yes	Yes

Pseudonymization	Customer		
Data confidentiality	Access control measures Encryption at customer level Encryption at Acquia level (see Security Annex and Product Description)	Yes No Yes	Yes No Yes
Data integrity	Ant-tampering technology (see Security Annex)	Yes	Yes
Data availability including restoring availability, restoring access to personal data, and data resilience	Business continuity and disaster recovery measures (see Security Annex)	Yes	Yes
Regular testing, assessing and evaluating of TOMs	Regular security and process reviews (see also Security Annex)	Yes	Yes

4. Certifications

- SOC 2 Type II

5. Data Subject Rights

n/a

6. (Personal) Data Retention Cycles

Personal data is retained at the Customer's discretion. By default data retention cycles exist only for time series data (e.g. transactions and events), but not other personal data (e.g. email address and name).

7. Sub-Processing

The specific list of sub-processors is available from: www.acquia.com/about-us/legal/subprocessors

Any current Acquia customer with a data processing agreement in place with Acquia may subscribe to receive notifications of new or changed sub-processors through above website.

8. Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached)

Data importer has implemented and will maintain appropriate administrative, physical, and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Acquia Security Annex (available from https://www.acquia.com/about-us/legal/gdpr) applicable to the specific Services purchased by data exporter, as updated from time to time, and made available by data importer upon request. The data exporter is wholly responsible for implementing and maintaining security and data administration within any data exporter applications, configuration settings, or log settings used by data exporter in conjunction with the Services.