Acquia Edge

Last revision of this Product Notice: *[v1.1 – 17 May 2021 – spelling updated]*
Prior version(s) of this Product Notice: *[v1.0 – 04 March 2021 – initial version]*

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

About the Product
Acquia Edge consists of the following services which may be purchased jointly or individually:

1. Acquia Edge Security
2. Acquia Edge CDN

Acquia Edge Security provides comprehensive security to support Customers' digital transformation - against existing and emerging threats. The service includes a web application firewall (WAF) and distributed denial-of-service (DDOS) protection designed to help mitigate the effects of online threats and optimize legitimate visitor requests for protected websites.

Acquia Edge CDN supports Customers' digital transformation journeys, enabling them to provide users with superior experiences. It includes a massive global content delivery network (CDN) with 51 Tbps of capacity and web content optimization (WCO) service to accelerate the delivery of Customer website content to the visitor and decrease website load times. The Acquia Edge CDN service utilizes data centers in over 200 cities in more than 100 countries around the world, except mainland China, to accelerate the delivery of the Customer website content. If the Customer requires fast website load times within mainland China through the use of mainland China data centers, an optional Acquia Edge CDN China Network Access service is available. Use of the Acquia Edge CDN China Network Access service requires the Customer to have or obtain a valid Internet Content Provider (ICP) license from the Chinese government.

Acquia Edge is a service provided by Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA ("**Cloudflare**") and resold by Acquia to Acquia's customers. Cloudflare is a Sub-processor to Acquia.

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)*

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 the Service, Customer in its sole discretion determines and controls the categories of personal data by the Service. These may be names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or	Through the configuration, design, and administration of the service, Customer in its sole discretion determines and controls the categories of data subjects collected by the Service: Natural persons that (i) access or use the Customer's domains, networks, websites, application programming interfaces ("APIs"), and applications, or (ii) are authorized users such as the Customers' employees, agents, or contractors..	Provision of the Services by Acquia to Customer	Site administrators	yes	globally through Cloudflare's Anycast network as further describe here: https://www.cloudflare.com/network	Yes

localization data (including IP addresses).						

3. Privacy Enhancements (incl. CIA)

Objective	Technology / Measure	Data at Rest	Data in Transit
Anonymization and Pseudonymization	Data anonymization at Customer level optional for Customer	☐	☐
Data confidentiality (incl. encryption)	Access control measures Encryption at customer level Encryption at Acquia level Jurisdiction restrictions for (private) key storage and option to choose data center locations (see Security Annex and Product Description)	☒ ☒ ☒ ☒	☒ ☒ ☒ ☒
Data integrity	Ant-tampering technology (see Security Annex)	☒	☒
Data availability including restoring availability, restoring access to personal data, and data resilience	Business continuity and disaster recovery measures (see Security Annex)	☒	n/a
Regular testing, assessing and evaluating of TOMs	Regular security and process reviews (see also Security Annex)	☒	n/a

4. Certifications (on Sub-processor level)

- **SOC 2 Type II**
- **SOC 3**
- **ISO 27001:2013**

5. Data Subject Rights

Through the Product's administration console the Customer may manage, update, retrieve, and erase individual Personal Data.

6. (Personal) Data Retention Cycles

Customer Account Information - Customer Account Information includes customer registration and contact information, audit logs, and other logs and data about account configurations and settings. We store Customer Account Information as long as a Customer has an active account, and we set specific timeframes for retaining Customer Account Information following deletion of an account based on the reason for collection and applicable law. For example, we are required to keep information about contracts we have signed and subscription payment details for several years due to compliance obligations. In addition, upon deletion of an account or upon receipt of an individual's request to be forgotten, we may be required to retain the email address associated with the account for an extended period of time, and potentially block that email address from creating a new account in the future, in order to comply with legal obligations and our terms.

End User Log Data - We currently store detailed end user request traffic logs of the data we process on behalf of our Customers ("End User Log Data") for up to 7 days and may store such data longer if requested by the Customer and where technically possible. We store a small sample -- approximately 1% -- of all End User traffic logs for up to 12 months. We may store firewall event logs for up to 12 months. When a Customer terminates their account, End User Log Data is deleted in accordance with these retention periods unless other treatment is required to comply with our legal obligations.

Operational Metrics - We store server and network activity data and logs collected by Cloudflare in the course of operating the Service and our observations and analysis of traffic data (together, "Operational Metrics") up to 12 months or as long as we have a legitimate business purpose for retention. Examples of Operational Metrics include service uptime and service availability metrics, request volumes, error rates, cache rates, and IP threat scores.

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)

Acquia 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 applicable to the

specific Services purchased by Customer, as updated from time to time, and made available by Acquia upon request. Customer is wholly responsible for implementing and maintaining security and data administration within any Customer applications, configuration settings, or log settings used by Customer in conjunction with the Services.

In addition, Cloudflare's security program includes further security measures as detailed here https://www.cloudflare.com/gdpr/introduction/ (please also refer to Cloudflare's DPA as available under this link).