A1 Digital International GmbH Lassallestraße 9, 1020 Vienna

Offensity Security Monitoring & Reporting

Data protection and data processing attachment

Version: 1.0

Date: 24th of June 2021

1. Data protection and data security

The service is operated at data centres within Europe.

Further information can be found on our website:
https://www.a1.digital/at/ueber-a1-digital/datenschutzerklarung/.

A1 Digital International GmbH's General Terms and Conditions for processing of personal data on behalf of customers (GTC DPA) including the Data Processing Annex, which is an Annex to this Service Description/Terms of Service shall apply. The GTC DPA are published under https://www.a1.digital/at/ueber-a1-digital/agbs/.

2. Data processing attachment

In the framework of the services A1 Digitals provide, A1 Digital will process your personal data as a contract processor pursuant to Art. 28 of the General Data Protection Regulation (GDPR).

2.1 Subject of the order

1.1. The order for the person responsible for processing to the contract processor includes the following products or services: **"Offensity"**

1.2. The following data types can be the subject of regular processing:

- ☒ Personal master data
- ☒ Personal IDs
- ☐ Special personal data
- ☒ Marketing/sales data with reference to a person
- ☒ Personal roles/associations
- ☒ Customer inventory
- ☒ Customer interactions
- ☒ Traffic data
- ☐ Movement data | Geolocation data
- ☒ Content data
- ☒ Financial data
- ☒ Login, passwords

1.3. Group of persons affected by the data processing:

☒ Customer of the client - natural person

☒ Customer of the client - legal entity

☒ User of the enterprise customer

☒ Employee of the client

☒ Contract partner of the client

☐ Children or persons requiring protection

2.2 List of commissioned subcontractors

Name	Company address	Type of processing	Processing location
Akenes SA (Exoscale)	Boulevard de Grancy 19A 1006 – Lausanne Switzerland	Hosting Services	Switzerland, Germany, Austria, Bulgaria
Google Ireland Ltd. (Branch of Google LLC)	Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland	Hosting Services	Ireland, Frankfurt
Elasticsearch B.V.	Rijnsburgstraat 11, 1059 AT Amsterdam, the Netherlands	Hosting Services	Frankfurt

2.3 Technical organisational measures

The contract processor shall ensure security in accordance with Art. 28 (3) lit. c, (32) of the GDPR, in particular, in conjunction with Art. 5 (1), (2) of the GDPR. Overall, the measures to be implemented are measures to secure data and guarantee a level of protection commensurate to the risk with respect to the confidentiality, integrity, availability and capacity of the systems. The state-of-the-art, the implementation costs and the type, scope and purpose of the processing and the various occurrence probabilities and severity of the risk to the rights and freedoms of natural persons pursuant to Art. 32 (1) of the GDPR must be taken into account. Unless stipulated in more detail in the performance agreement, the contract processor is responsible for ensuring that a protection level appropriate for the respective processing is ensured, in particular, by means of a combination of the technical organisational measures specified below. The contract processor is permitted to implement adequate, alternative measures. The protection level of the defined measures must be reached.

A. CONFIDENTIALITY (ART. 32 (1) LIT. B OF THE GDPR)

- **Admission control:** Protection against unauthorised access to data processing systems, e.g. using magnetic or chip cards, keys, electrical door openers, factory security or gatekeeper, alarm systems, video systems.

- **Access control**: Protection against unauthorised system use e.g. (secure) passwords, two-factor authentication.

- **Login control**: No unauthorised reading, copying, modification or removal within the system, via e.g., authorisation concepts and need-based access rights, documentation of logins.

- **Separation control:** Separate processing of data collected for different purposes, e.g., by means of standard authorisation profiles on a "need to know basis", client-capability.

- **Pseudonymisation**: If possible for the respective data processing, the primary identification properties of the personal data in the respective data processing will be removed and stored separately.

- **Classification scheme for data:** Based on statutory obligations or self-assessment (secret/confidential/internal/public).

B. DATA INTEGRITY[1] (ART. 32 (1) LIT. B OF THE GDPR)

- **Transfer control**: No unauthorised reading, copying, modification or removal during electronics transmission or transport, e.g. as a result of encryption.

- **Entry control**: Determination of whether and from whom personal data has been entered into, modified or removed from data processing systems, e.g. by means of logging.

C. AVAILABILITY AND CAPACITY (ART. 32 (1) LIT. B OF THE GDPR)

- **Availability monitoring**: Protection against random or deliberate destruction or loss, e.g. by means of a backup strategy (online/offline; on-site/off-site), uninterrupted power supply (UPS), firewall, reporting channels and contingency plans.

- **Restorability**

D. PROCEDURE FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION (ART. 32 (1) LIT. D OF THE GDPR; ART. 25 (1) OF THE GDPR)

- **Data protection management, including regular employee training**
- **Incident response management**
- **Data protection-friendly defaults**:
- **Order monitoring:** No contract-based data processing pursuant to Art. 28 of the GDPR without corresponding instructions from the client

[1] Prevention of (unintentional) destruction/deletion, (unintentional) damage, (unintentional) loss, (unintentional) modification of personal data.