Technical and Organisational Measures for jsDelivr CDN service

The following sections define Volentio JSD's current technical and organisational measures and are incorporated into Volentio JSD's Data Processing Agreement. Volentio JSD may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. PHYSICAL ACCESS CONTROL

Unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process or use Personal Data are located.

1.1. Measures

1.1.1. Volentio JSD protects its assets and facilities using the appropriate means based on the Volentio JSD Security Policy.

1.1.2. In general, buildings are secured through access control systems (e.g., smart card access system).

1.1.3. As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.

1.1.4. Access rights are granted to authorised persons on an individual basis according to the System and Data Access Control measures (see below). This also applies to visitor access. Guests and visitors to Volentio JSD buildings must register their names at reception and must be accompanied by authorised Volentio JSD personnel.

1.1.5. Volentio JSD employees and external personnel must wear their ID cards at all Volentio JSD locations.

1.2. Additional measures for data centres

1.2.1. All data centres adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms, and other measures to prevent compromised equipment and data centre facilities. Only authorised representatives have access to systems and infrastructure within the data centre facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

1.2.2. Volentio JSD and all third-party data centre providers log the names and times of authorised personnel entering Volentio JSD's private areas within the data centres.

2. SYSTEM ACCESS CONTROL

Data processing systems used to provide the jsDelivr CDN service must be prevented from being used without authorisation by taking the following measures:

2.1. Multiple authorisation levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorisations are managed via defined processes according to the Volentio JSD Security Policy

2.2. All personnel access Volentio JSD's systems with a unique identifier (user ID).

2.3. Volentio JSD has procedures in place so that requested authorisation changes are implemented only in accordance with the Volentio JSD Security Policy (for example, no rights are granted without authorisation). In case personnel leave the company, their access rights are revoked.

2.4. Volentio JSD has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed regularly and default passwords to be altered. Personalised user IDs are assigned for authentication. All passwords must fulfil defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

2.5. The company network is protected from the public network by firewalls.

2.6. Volentio JSD uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.

2.7. Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to Volentio JSD's corporate network and critical infrastructure is protected by strong authentication.

3. DATA ACCESS CONTROL

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorisation in the course of processing, use and storage. Volentio JSD takes the following measures:

3.1. As part of the Volentio JSD Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the Volentio JSD Information Classification standard.

3.2. Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. Volentio JSD uses authorisation concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the Volentio JSD Security Policy.

3.3. All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, Volentio JSD conducts internal and external security checks and penetration tests on its IT systems.

3.4. Volentio JSD does not allow the installation of software that has not been approved by Volentio JSD.

3.5. An Volentio JSD security standard governs how data and data carriers are deleted or destroyed once they are no longer required.