Data Processing Agreement 2023 - Trinity Sales B.V.

To protect your data, we will take appropriate technical and organizational measures that are in accordance with applicable data security legislation. Depending on the state of the art, the costs of implementation and the nature of the data to be protected, we take technical and organizational measures to prevent risks such as destruction, loss, modification and unauthorized disclosure of or access to your data. This with the aim of providing sufficient protection to the customer's personal data in accordance with Article 32 of the GDPR. The technical and organizational measures ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with this Processor Agreement.

1. Access control

Trinity Sales B.V. takes various measures to prevent unauthorized persons from gaining physical access to data processing systems on which Personal Data are processed or used (physical access control), such as:

- Access control
- Access authorization concepts
- Regulations regarding the provision of keys
- Supervision of visitors by staff
- Security outside office hours by means of an alarm system
- Compartmentalization with controlled access
- Entrance security
- Security measures for the building and grounds (alarm system)
- Secure access to server room
- Server room housed in lockable rooms/data centers
- Back-up data stored on location with limited access

2. Access control

Trinity Sales B.V. has implemented the following measures to prevent unauthorized use of data processing systems:

- Use of two-factor authentication when logging in from outside the own network
- Restriction for logging in from verified & approved fixed IP addresses of employees when logging in to SFTP connections
- Lockable data processing systems
- Security of computer workstations
- Regulation of user authorization
- Use of individual passwords
- Automatic blocking of user accounts after entering multiple incorrect passwords

- Automatic, password-protected, screen saver of computers after inactivity
- Password policy with minimum requirements for password complexity:
    - At least 8 characters
    - At least two of the following: Upper and lower case letters, special characters, numbers
- Processes for assigning access rights to new employees
- Processes for withdrawing access rights from employees who change departments
- Processes for withdrawing access rights from employees who leave the company
- The obligation to comply to data confidentiality provisions under the GDPR
- Recording and analysis of system usage
- Confidential destruction of data

3. Editing control

Measures aimed at ensuring that persons who have the right to use a data processing system can only access those data for which they have a specific authorization.

- Personal data cannot be read, copied, changed or deleted without permission during processing, use or after storage.
- Trinity Sales B.V. works with business software where employees can only request and view 1 (one) set of contact details at a time.
- Exporting datasets (more than 1 set of contact details) is impossible for individual employees.

4. Transmission control

Trinity Sales B.V. uses the following measures to ensure that Personal Data cannot be read, copied, changed or deleted without authorization during electronic transfer or transport or during storage on data carriers:

- Where possible, in consultation with the customer, we use an SFTP server from which the data files can be retrieved
- The leads are sent in advance via a two-step e-mail verification
- Files that are sent to a customer by e-mail will always be protected with a password.
- Passwords are provided separately (preferably via another electronic medium) to the recipient.

5. Input control

Measures to ensure that it can be retroactively investigated and determined whether and by whom personal data has been entered, changed or deleted from a data processing system. A log date and time is kept in all customer-related processes.

- Identification/labeling of entered data
- Definitions of the responsibilities regarding data entry
- Recording of entry/deletion
- There is a procedural, program and workflow organization

- Control of data entry
- The obligation to comply with the Personal Data Protection Act
- Control over access permissions

6. Task control

Task control is required to ensure that personal data processed on behalf of others is processed strictly according to the instructions of the Customer.

Measures:

- Trinity Sales B.V. uses control mechanisms and processes to monitor compliance with the contracts between Trinity Sales B.V. and its customers, subprocessors and other service providers. Personal data require at least the same level of security as confidential information under the GDPR legislation.
- All employees and contractual sub-processors of Trinity Sales B.V. are contractually obliged to respect the confidentiality of all sensitive information, including trade secrets of customers and partners.
- Trinity Sales B.V. employees cannot gain access to a customer system or customer-specific data without the knowledge and consent of the customer.

7. Availability control

Measures to ensure that personal data is protected against arbitrary destruction or loss:

- Data backup plans (a full backup is made daily, with 1 backup per week stored externally encrypted)
- Access rights to server space are limited to necessary personnel
- Fire alarms & Air conditioning are present in the server room
- Backup systems are in a separate location
- CO2 fire extinguishers are present in the server room

8. Data separation control

Personal data collected for different purposes can be processed separately.

Measures:

- Trinity Sales B.V. uses appropriate technical control mechanisms to ensure separation of customer data at all times. Each customer/project has its own folder.
- We use an authorization concept for the separate processing of data from different customers.