1 Februar 2024

Technical and Organizational Measures

According to Article 32 GDPR

chemmedia AG
Parkstrasse 35
09120 Chemnitz, GER
VAT-ID
DE223357395

Contact
phone: +49 371 49370-370
fax: +49 371 49 370-201
www.chemmedia.de
sales@chemmedia.de

Management Board
Lars Fassmann,
Sandra Deyringer
Chairman Supervisory Board
Stefan Pickschneider

Bank Account
Volksbank Chemnitz
Innere Klosterstr. 15, 09111 Chemnitz
IBAN: DE88 8709 6214 0321 058922
BIC: GENODEF1CH1

Technical and organizational measures

chemmedia undertakes to implement appropriate technical and organizational measures to ensure that the processing of data is carried out in accordance with legal requirements and that the rights of data subjects are adequately protected. chemmedia will design its internal organization in such a way that it meets the special requirements of data protection.

Confidentiality

Access control of data processing centers

Unauthorized persons are not granted access to the data processing systems used to process personal data. This is ensured by the following measures, among others:

- Operation of infrastructure in high-security data centers (Knowledgeworker systems) with strict security measures
- Property security through locking systems and documented key management, burglar-proof glazing, fire doors
- Access authorizations for security zones

Access control of data processing systems

The following measures prevent unauthorized persons from accessing data processing systems:

- Security and data protection policy, incl. password policy
- Implementation of a central system for managing user identities (Identity and Access Management System)
- Two-factor authentication procedures
- Hard disk encryption of mobile devices
- Administration of server systems exclusively via protected, encrypted connection, only accessible via VPN, securing the administration interface with two-factor authentication
- Standardized offboarding process when employees leave the company

Access control of personal data in data processing systems

It is ensured that the persons authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, changed or removed without authorization during processing.

- Binding authorization assignment procedure (separation of functions)
- Authorization concept for IT applications / IT systems

- Logging and event-related evaluation of accesses
- Binding procedure for restoring data from backup (restore by administrators on the instructions of project management or management)
- Separate user accounts for security-critical authorizations (e.g. administrative access)

Separation control

The following measures ensure that data collected for different purposes can be processed separately.

- Separation of clients
- Separation of functions (authorization concept, need-to-know)
- Private instances of data processing systems only for the respective client
- Separation of functions between production and test environment

Integrity

Transfer control

Disclosure and transmission of personal data stored on the technical systems of chemmedia AG is only possible on the instructions of the client and is documented. Disclosure for the purposes of criminal prosecution is only possible if a court order has been issued. As far as legally permissible, the client will be informed promptly. chemmedia protects confidential data during transmission as follows:

- Company-wide guidelines for the transmission of confidential data (e.g. use of our own file sharing system)
- Encrypted transmission and storage of confidential data. The encryption technologies used correspond to the state of the art.
- Pseudonymization, anonymization and deletion of personal data where necessary
- Controlled destruction of data carriers

Input control

The following measures ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered into, changed or removed from data processing systems.

- Definition of responsibilities for the input of data
- Logging of entries, changes and deletions of personal data
- Contractual obligation of all employees to maintain data secrecy and confidentiality
- Regular training of all employees
- Contractual regulations on deletion periods for customer projects

Availability and resilience

Availability control

The following measures ensure that personal data is protected against accidental destruction or loss.

- Backup and recovery concept with daily backup of all relevant data and geographically separated storage
- Expert use of protection programs (virus scanners, firewalls, encryption programs, SPAM filters)
- Redundant design of the systems required to maintain business operations
- Monitoring of the operating parameters of the data centers by chemmedia and hosting providers
- Disaster and emergency plan (business continuity plan)

Procedures for regular review, assessment and evaluation

chemmedia has established procedures that enable regular review, assessment and evaluation of the effectiveness of the technical and organizational measures used. Company-wide internal guidelines are binding for all employees and are reviewed annually. Where technically possible, data protection-friendly default settings are made in the technical systems used in accordance with Art. 25 para. 2 GDPR. Incident response responsibilities are clearly defined and communicated. Our company data protection officer is integrated into all relevant processes and can be contacted at privacy@chemmedia.de for inquiries.

Order control

The following measures ensure that personal data processed on behalf of the controller is only processed in accordance with the controller's instructions.

- Clear contract design and formalized order placement by the client
- Documentation of the execution of the contract
- Contractually agreed written form for change requests and instructions from the client
- Careful selection of suitable service providers and obliging them to comply with the applicable data protection laws