consent manager

consentmanager

Technical and organizational measures (Art. 32 GDPR)

Technical and organizational measures (Art. 32 GDPR)

consentmanager will use the following technical and organizational measures for our product and services. Please note that not all measures apply to consentmanager directly but are listed here because consentmanager will impose the relevant measures on its sub-processors. Example: consentmanager does not own or operate a datacenter, therefore CO2 fire extinguishers are not a measure that applies to consentmanager itself. Anyhow, as we are using sub-processors that operate datacenters for us, we will require these measures from those sub-processors.

1. Confidentiality (Art. 32 Para. 1 (b) GDPR)

1.1 Physical access control

- Alarm system
- Securing of building shafts
- Specially glazed windows
- Roller blinds with anti-lift devices
- Motion detector
- Manual locking system
- Video surveillance of system accesses
- Security locks
- Key control (e.g. key issue)
- Entitlement Passes
- Electronic access code card/access transponder
- Access authorization concept
- Security also outside working hours through factory security
- Grades security areas and controlled access
- Separately secured access to data canter
- Server storage in locked rooms
- Storage of data media under lock and key or in enclosed rooms
- Storage of data backups (e.g. tapes, CDs) in the access protected safe
- Visitor policy: personal checks at reception
- Visitor policy: Visitor passes
- Visitor policy: Accompaniment of visitors by own employees
- Visitor policy: Attendance records of visitor accesses
- Careful selection of cleaning personnel
- Careful selection of security personnel
- Specially secured server cabinet
- Notebook locks
- Instructions for the proper handling of end devices
- Prohibition of passing along the mobile devices

1.2 System access control

- Management of user authorizations
- Restrictive assignment of user accesses
- Password assignment
- Authentication with username/password
- Automatic deactivation/deletion of inactive accesses
- Measures in case of failed login attempts
- Two-factor-authentication
- Provisions that only company-owned and encrypted USB sticks are used
- Use of VPN technology
- Use of anti-virus software
- Use of a software firewall
- Encryption of data carriers
- Encryption of IT systems
- Prevention of unauthorized access to IT systems by third parties

1.3 Data access control

- Creation of an authorization concept, Definition of the access authorization
- Data recovery policy from backups (who, when, at whose request)
- Regular checking of authorizations
- Restriction of the free and uncontrolled query possibility of databases
- Partial access options to databases and functions (Read, Write, Execute)
- Administration of user rights by system administrator
- Number of administrators reduced to the ‘bare minimum’
- Logging of accesses to applications, especially during input, modification and erasure of data
- Use of service providers for the proper destruction of data carriers (DIN 66399)
- Use of service providers for document destruction
- Logging of destruction of data
- Regular evaluation of logs (log files)
- Virus scanner
- Firewalls
- SPAM-Filter
- Intrusion prevention (IPS)
- Intrusion detection (IDS)
- Anti-spy programs
- “Full scans” and “quick scans” at periodic intervals
- Software for Security Information and Event Management (SIEM)
- Encrypted storage of data
- Key algorithms used
- AES/RSA
- Hash function used
- SHA2 (256, 384, 512 bit)
- SHA3
- Hashes are "salted" (Salt) or "peppered" (Pepper)
- Identity Management System (IDMS)

1.4 Separation control

- Separation of production and test systems
- File separation for databases
- Logical data separation
- Separate processing of data collected for different purposes
- Separate processing of data of different customers
- Prevention of customers from accessing data of other customers
- Processing of the data of the Principal and other customers by different employees of the Contractor
- Data backup of Principal data on separate data carriers (without data of other customers)
- Processing of the data of the principal and other customers by different employees of the Contractor

1.5 Pseudonymization and encryption (Art. 32 Para. 1 (a) GDPR)

- Implementation of data record pseudonymization
- Implementation of data encryption
- Encrypted data transmission to third parties

2. Integrity (Art. 32 Para. 1 (b) GDPR)

2.1 Data transmission control

- Transmission of data via Citrix connection (128 bit encrypted)
- Data exchange via https connection
- Use of encryption algorithms
- Use of hash functions (salted or peppered)
- Installation of leased lines or VPN tunnels
- E-mail encryption (transport, e.g. ZIP files)
- E-mail encryption (E2EE)
- TLS encryption
- IPsec
- Secure Shell (SSH)
- Use of electronic signatures
- Secured entrance for incoming and outgoing deliveries
- Documented management of data media, inventory control
- Definition of the areas in which data media must be located
- Encryption of confidential data media
- Encryption of laptop hard disks
- Encryption of mobile data carriers
- Controlled destruction of data
- Automatic deletion in case of certain event
- Automatic deletion concepts
- Physical destruction
- Overwriting of tapes and hard disks
- paper disposal
- Sealed metal containers (so-called data protection barrels)

- Disposal by service providers
- Shredder according to DIN 66399
- Rules for making copies
- Backup copies of data carriers that need to be transported
- Documentation of the bodies to which transmission is envisaged and of the means of transmission
- Packaging and shipping instructions
- Completeness and correctness check
- Nondisclosure agreements with subcontractors
- Organizational requirements (prohibition of the use of private mobile devices)
- Technical separation of private and business communication

2.2 Input control

- Traceability of data input, modification and erasure by means of individual usernames (not user groups)
- Identification of collected data
- Definition of user authorizations
- Read, Change, Delete
- Partial access to data or functions
- Field access to databases
- Organizational definition of input responsibilities
- Logging of entries/deletions
- Protocol evaluation system
- Logging of data processing systems
- Document management
- Obligation of data secrecy
- Log concept going beyond OS standard
- Dedicated log server
- Regulation of access authorizations for log servers (LogAdmin)
- Regulation on retention periods for audit/proof purposes

3. Availability and resilience (Art. 32 Para. 1 (b) GDPR)

3.1 Availability control

- Data backup and backup concepts
- Implementation of data backup and backup concepts
- Ensuring the technical readability of backup storage media for the future
- Storage of data backup in a secure, outsourced location
- Agreement regarding the transfer of data backups
- Access limitation to necessary personnel in server rooms
- Server rooms not beneath sanitary facilities
- In flood-prone areas: server rooms above highest water level
- Air-conditioned server rooms
- Shielding attenuation
- Fire doors

- Water protection devices
- Sprinklers
- Presence of a fire and smoke detection system
- Presence of a fire and smoke detection system in server rooms
- Presence of a waterless fire-fighting system in the server rooms
- CO2 fire extinguishers in the immediate vicinity of the server rooms
- Server rooms in separate fire compartment
- Lightning/overvoltage protection
- Uninterruptible power supply (especially in server rooms)
- Electric generator
- Water sensors in server rooms
- Creation of an emergency plan and reporting channels (e.g. water, fire, explosion, threat)
- Regulations, which only allow access after training/instruction
- Regulations, which allow access only with accompaniment
- Weak point analysis (terrain protection, building protection, penetration into computers, computer networks)
- Storage of data in data safes, vaults
- Protected power strips in server rooms

3.2 Restorability (Art. 32 Para. 1 (c) GDPR)

- Installation of backup systems
- Backup data centers
- Redundant power supply
- Redundant power generators
- Redundant air conditioning
- Redundant fire fighting
- Hard disk mirroring
- Computer Emergency Response Team (CERT)
- Load balancer
- Data storage on RAID systems (RAID 1 and higher)
- Performance of penetration tests
- System hardening (deactivation of unnecessary components)
- Immediate and regular activation of available software and company software updates:
    - Identify the different devices that make up the network and determine your hardware version and your current software and firmware versions
    - Communication channel with the manufacturers to inform themselves about new updates and patches that have been released for the devices in their possession
    - Definition of time periods in which updates are to be implemented
    - Use redundant systems to maintain operation while main equipment is being updated
    - Progressive provision of updates / patches to detect problems early without affecting multiple devices
    - Determination of a test period to ensure correct implementation of the update Review and ensure that operations with the new updates continue to run smoothly
- Main consideration of safety during the design phase of the system:
- Definition of security measures to protect and validate communication between system components
- Restriction of authorizations to the need for authorization

- External contractors and maintenance personnel receive specific access that is only active during the intervention and deactivated for the rest of the time
- Periodic safety training and awareness-raising campaigns within the organization:
    - Awareness-raising campaigns to inform users about security concepts specific to both specific systems and traditional IT systems
    - Specific security training to teach how to apply security measures and behaviors to daily processes with the least possible effort
- Conclusion of a cyber insurance policy
- Identification of IT devices, assets and network systems in the organization's Infrastructure
- Perform a risk analysis of all these systems, equipment and assets identified to determine the threats, including their likelihood and impact
- Encryption of data backups
- Ability to restore data rapidly

4. Process for regular testing, assessment and evaluation (Art. 32 Para. 1 (d) GDPR)

4.1 Data protection concept

- Presence of a data protection management system
- Presence of a data protection risk management system
- Processing records held by the Processor
- Existence of data protection-friendly default settings

4.2 Order control

- Regular checks of the Contractor from a due diligence perspective (in particular with regard to data security)
- Drafting contracts in accordance with legal requirements (Art. 28 GDPR)
- Central registration of existing service providers (uniform contract management)
- Examination of the Contractor´s data security concept
- Regular controls of the Contractor
- Selection of Contractor from a due diligence perspective (in particular with regard to data security)
- On-the-spot checks at the contractor's premises
- Securing of existing IT security certificates of the contractors
- Obligation of the Contractor’s employees to maintain secrecy and confidentiality
- Guidelines and/or work instructions for data protection/data security
- Evidence of training completed by Contractor’s employees