d.vinci

d.vinci HR-Systems, 37-39 Nagelsweg, 20097 Hamburg

# Technical and organizational measures (TOM) in accordance with Art. 32 GDPR

| | |
|---|---|
| Valid from | Oct. 10, 2024 |
| Owner | Information Security Officer |
| Classification | public |

d.vinci operates and administers systems for its customers in the pop-interactive data centre in Hamburg. d.vinci is certified according to ISO/IEC 27001, and the certification includes the services of the data centre. This document describes the technical and organizational measures for the protection of personal data in these systems.

To classify the technical and organizational measures, it is important to note that the systems are not operated in a traditional cloud but are a SaaS solution that is administered and operated solely by d.vinci. The data centre staff have neither physical nor technical access to the systems. d.vinci only uses the data centre infrastructure (extinguishing system, fire protection, emergency power supply, etc.).

Insofar as the measures listed here differ between the data centre and the d.vinci office, they are marked with an “RZ” (data centre) or “N37” (office).

## 1. Confidentiality (Art. 32 Par. 1 lit. b GDPR)

a) Physical access control: Measures to prevent unauthorized persons from physically accessing the data processing systems

- RZ: Solid building with steel doors, windowless server room on an upper floor
- Alarm system
- RZ: Backups in separate, locked fire protection area
- Physical access control/key management with documentation of key allocation
- N37: Physical access via transponder instead of mechanical key
- RZ: Assignment and withdrawal of access rights according to the need-to-know principle including documentation
- RZ: Logging of physical access
- RZ: Visitor regulation (access only for certain persons, ID card requirement, etc.)
- RZ: Video surveillance
- N37: Visitor regulations (documentation of visiting times, escorting visitors, etc.)

b) Technical access control: Measures to prevent unauthorized technical access to the data processing systems

- RZ: “data at rest” encryption
- N37: Encryption of the clients' hard disks
- Established patch management processes
- Deactivation of unneeded services and functions
- Access to the company network from outside via VPN
- Personal user login to the d.vinci system
- Procedures for granting and withdrawing user authorizations based on a role concept
- Approval procedure for changes to authorizations
- Regular checking of user accounts
- Automatic blocking of the user account after 5 failed login attempts
- Specification for passwords according to policy
- At least 25 characters long and randomly generated passwords for service accounts
- Access logging and evaluation (SIEM)
- Administration via VPN tunnel
- Partially multi-factor authentication based on the classification of information
- N37: Automatic blocking of clients when not in use
- Redundant firewalls

c) Access Control (Authorization): Measures to prevent unauthorized access to personal data

- Configurable roles and rights in the application (e.g. HR officers and specialist departments)
- Established roles and rights concept for d.vinci employees
- Change of access rights according to the need-to-know principle including documentation
- Regular review of user accounts including access authorizations
- Logging of access and administrative activities
- Encrypted communication channels
- Segmented networks
- Dedicated network for customer systems
- Firewall rules that are as restrictive as possible
- Tool-based vulnerability management
- Dedicated backup hardware and dedicated backup network
- Encrypted transmission of data backups
- Conclusion of contracts for commissioned data processing with service providers for the maintenance of data processing systems
- N37: Blocking of the clients' USB ports
- File and data carrier destruction in accordance with DIN 66399

d) Separation Control: Measures for the separate processing of personal data collected for different purposes

- Storage of data in databases separated by customer
- Separation of development, test and production environments, each with its own database
- Use of generic test data; no production data in development and test systems
- Use of separate systems depending on the purpose of data collection
- Access authorizations according to functional responsibility

e) Pseudonymization (Art. 32 Par. 1 lit. a DSGVO; Art. 25 Par. 1 DSGVO): Measures to process personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures

- Pseudonymization procedures are not used; instead, procedures for secure encryption and anonymization are used

## 2. Integrity (Art. 32 Par. 1 lit. b DSGVO)

a) Transfer control: Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during transmission or storage on data carriers and that it is possible to check which persons or bodies have received personal data

- Encrypted data transport with TLS at least version 1.2
- Administration of the infrastructure through a VPN tunnel
- Irreversible destruction of data carriers in accordance with DIN 66399
- Encryption of client hard disks
- Regulation on the restricted use of mobile storage media
- Encryption of offsite backups
- Logging of logins to the d.vinci system

b) Input control: Measures to ensure the possibility of checking who has processed personal data in data processing systems and at what time

- Temporary logging of IP addresses when applications are submitted
- Audit log for administrative changes that can be viewed in the d.vinci system
- Rights and roles concept

## 3. Availability and resilience (Art. 32 Par. 1 lit. b DSGVO)

Availability control and resilience control: Measures to protect personal data from accidental destruction or loss and to ensure that the data is always available to the client

- Daily data backups to an independent fire protection area
- Outsourcing of encrypted backups to a geographically remote location
- Regular testing of recovery from backups
- Regular disaster recovery exercises
- Operation in a professional data centre: structural fire protection, early fire detection, gas extinguishing system, UPS, video surveillance, flood protection, redundant air conditioning, redundant internet connection
- Established emergency management for the immediate handling and processing of acute faults
- Predefined measures for described emergency scenarios
- Established risk management
- Redundant network components
- Operation of virtual machines in a high-availability cluster
- Redundant services
- Installing security updates as required
- Checking all incoming files for viruses

- Monitoring the availability of relevant services and resources
- Use of exclusively up-to-date hardware with manufacturer support

## 4. Procedures for regular review, assessment and evaluation (Art. 32 Par. 1 lit. d DSGVO; Art. 25 Par. 1 DSGVO)

a) Data protection management: Measures to ensure an organization that meets the basic requirements of data protection law

- Established data protection management system
- Appointment of an external company data protection officer
- Established role of an internal data protection advisor
- Confidentiality obligation of employees
- Annual re-commitment of employees to confidentiality and relevant data protection guidelines
- Annual data protection training for employees
- Data protection training for new employees
- Keeping a register of processing activities
- Annual audit of technical and organizational measures by the company data protection officer
- Audit of technical and organizational measures as part of ISO 27001 certification

b) Incident response management: Measures for triggering reporting processes in the event of data protection breaches

- Established process for reporting data breaches to supervisory authorities and data subjects

c) Privacy-friendly default settings (Art. 25 Par. 2 DSGVO): Measures to ensure that only the necessary personal data is processed and the amount of data collected is minimized

- Privacy by design: Integration of data protection into the software development as early as the requirements gathering stage
- Opt-in instead of opt-out, wherever reasonably possible
- Limiting the amount of personal data collected to what is necessary
- Transparency about what data is collected, how it is used and with whom it is shared
- Automatic data deletion after a period of time that can be set by the customer

d) Order control: Measures to ensure that personal data can only be processed in accordance with instructions

- Agreement on order processing with regulations on the rights and obligations of the contractor and client
- Specification of persons authorized to issue instructions on the part of the client and recipients of instructions on the part of the contractor
- Possibility of access, information and control for the contractor, for example through pentests or audits
- Documentation of order execution subject to instructions
- Instruction of all authorized employees of the contractor
- Obligation of d.vinci employees to maintain confidentiality