DOCUMENTATION OF TECHNICAL AND ORGANISATIONAL MEASURES

according to Art. 32 GDPR

V 1.6

domainfactory GmbH

Oskar-Messter-Strasse 33

85737 Ismaning

1. Preamble

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (TOM). These apply to the IT services defined in the main contract, which are provided in the data centres defined in section 2.

When selecting these measures, the four protection objectives of art. 32 paragraph 1 b) GDPR, namely the confidentiality, integrity, availability, and resilience of the systems, were taken into account. A quick recovery after a physical or technical incident is guaranteed. All technical and organisational measures are regularly checked for their effectiveness in accordance with art. 32 paragraph 1 d) GDPR.

In general, the following must be observed:

DomainFactory GmbH rents out the data processing system to the customer. This includes the rental of hardware and software, as well as the provision of connections to the Internet and other services in accordance with the respective agreement. The customer alone and exclusively decides which personal data are processed and how ("master of the data"). The systems required for data processing are created and used by the customer. DomainFactory ensures the technical operational readiness of the system in accordance with the contractual agreements and keeps a record of which systems are used by the customer and to what extent. Data processing is carried out by the customer. DomainFactory has no influence on the data processing operations carried out by the customer.

2. Confidentiality capability

Confidentiality means that personal data must be protected from unauthorised access.

Measures
Defined security areas
Individual assignment of access authorisation
Electronic access control systems and personnel monitor and guarantee access to the respective data centre for authorized persons only
Documentation of access authorisations
Access documentation
Authorized security personnel[1] - During business hours - 24/7 - Visual inspections
Role-dependent access rules for employees (administrators, assistants, cleaning personnel, etc.)
Visitor Regulations
Regular patrols by security personnel outside the data centre area
Automatic closing and locking of doors
Locking of all building entrances, such as windows and doors
Additional mechanical protection measures for the ground floor
Offices are locked outside working hours
Protection and restriction of access routes
Locking system based on transponders or key cards
Video cameras as well as intrusion and contact detectors monitor the outer facade of the building
Alarm messages can be viewed by personnel on site
Fenced area including video surveillance
Access control system with access cards
Additional access restrictions for server rooms
Change of the default passwords of all system and infrastructure components

[1] Not DC Cologne (CGN1)

Measures
Logging of user relevant activities (logon, logoff, denial of access, etc.)
Demilitarised zones
Protection of the infrastructure through alarm signals on windows and doors
Access restrictions for certain IP address ranges
VPN restrictions
Blocking of unnecessary ports
External access only via secure connections (VPN, RDP or similar)
Wi-Fi encryption
Regular software updates
User authentication required for system access and/or application access
Limitation of the validity period of user accounts
Automatic deactivation of users after several failed logins
Forced or mandatory change of passwords after the first login
Expiration of user passwords
Required minimum complexity for passwords
Password history to prevent multiple use of the same password
Appropriate user account recovery in the event of a lost or forgotten authentication record
Encrypted storage of user passwords
User login history
Destruction of physical media according to DIN 66399
Use of a document shredder (according to DIN 66399)

3. Integrity capability (Applies to all data centre locations)

Integrity means ensuring the correctness (integrity) of data and the correct functioning of systems. When the term integrity is used in connection with the term “data”, it expresses that the data is complete and unchanged.

Measures
Role-based authorization concept (read / write / change / copy / delete)

Measures
Documentation of the assignment of access rights
Strict administrative separation of tasks
Logging of external support processes
Documentation of the transfer of physical storage media
Logical data separation: Separate databases or structured file storage
Separate instances for development and production systems (sandboxes)
Specific approval rules for the database and application access / authorization concept

4. Availability capability

The availability of services and IT systems, IT applications, and IT network functions or of information is guaranteed, if the users are able to use them at all times as intended.

Measures
Infrastructure protection through hardware firewalls
Software firewall
Antivirus software
Monitoring and logging of administrative system access and configuration changes
Controlled access to e-mails and the Internet
Separation of application and administration accesses
Monitoring and logging of general user activity
Logging of external support processes
Logging of administrative changes
Access rules and access management
Overvoltage protection of the building exterior against lightning strike
Uninterruptible power supply (UPS)
Fire and/or smoke detector has a direct connection to the local fire department or local security personnel
Cooling system in data centre / server room

Measures
Automatic fire extinguishing system[2]
Disaster recovery mechanisms for data recovery, protection against accidental destruction and loss
Daily incremental data backup
Weekly complete data backup
Weekly backups on separately stored physical media or on physically separate systems
The fuel supply is sufficient for at least 16 hours at full load. Refuelling is possible while the generator is running
Devices for monitoring temperature and humidity in data centres
Contingency plan
External audits and security tests
Clearly defined administrative tasks for controllers and processors

5. Regular review procedures (Applies to all data centre locations)

How is it ensured that the above-mentioned data backup measures are regularly checked?

Measures
Regular review of system access authorizations
Internal and external audits
Disciplinary measures in the event of data protection violations
Regular safety checks
Regular control of external service providers
Regular meetings with the data protection officers appointed with regard to operational processes relating to the processing of personal data

6. Protection against unlawful access to personal data (applies to all data centre locations))

Which measures are taken to prevent that personal data is available and accessible to unauthorized persons?

[2] DC Limburg (OVH): early fire detection system.

Measures
Controlled access to e-mails and the internet
Separation of application and administration accesses
Regular security updates
Monitoring and logging of general user activity
Prohibition of the use of private data carriers
Role-dependent access restrictions
Application-based check of input authorization

7. Processing of personal data only according to instructions (Applies to all data centre locations)

How is it ensured that personal data will only be processed in accordance with the instructions of the data controller?

Measures
confidentiality reminders
Written obligation of all employees to maintain confidentiality
Regular data protection training of employees
Controlled erasure / disposal of data carriers such as hard disks, CDs, DVDs, USB sticks
Data transfer and transfer in accordance with the instructions of the controller
Written guidelines for data transmission and dissemination
Binding rules for the disclosure of sensitive data
Data protection-compliant deletion of all data copies and data backups after completion of the order
Processing of personal data is carried out exclusively in accordance with the instructions of the client
Defined contact persons for change requests
Control rights of the controller during ordered data processing
Subcontractors will be bound by the same rules and regulations as DomainFactory itself

8. Anonymisation / pseudonymisation / encryption

Anonymisation, pseudonymisation or encryption of the client's data shall in principle not be the subject of the service to be provided by DomainFactory, unless separate agreements have been made in the main contract.

9. Resilience of systems

DomainFactory takes the measures described in Section 4 to ensure the resilience of the IT systems. In principle, penetration tests of the client's IT systems are not the subject of the service to be provided by DomainFactory, unless separate agreements have been made in the main contract.

10. Data centres of OVH SAS

For products that are provisioned in data centres of our subcontractor OVH SAS, the above TOMs might differ. This is noted accordingly in the document.