DOCUMENTATION TECHNICAL AND ORGANIZATIONAL MEASURES

in acc. with article 32 GDPR

V 1.0

server4you

Host Europe GmbH

Hansestr. 111

51149 Köln

We are committed to protect our customers' information. Taking into account the best practices, the costs of implementation and the nature, scope, circumstances and purposes of processing as well as the different likelihood of occurrence and severity of the risk to the rights and freedoms of natural persons we take the following technical and organizational measures (TOM). When selecting the measures the confidentiality, integrity, availability and resilience of the systems are considered. A quick recovery after a physical or technical incident is guaranteed.

Data Privacy Program

Our Data Privacy Program is established to maintain a global data governance structure and secure information throughout its lifecycle. This program is driven by the office of the data protection officer, which oversees the implementation of privacy practices and security measures. We regularly test, assess and evaluate the effectiveness of its Data Privacy Program and Security Standards.

1. **Confidentiality**

"Confidentiality means that personal data is protected against unauthorized disclosure."

We use a variety of physical and logical measures to protect the confidentiality of its customers' personal data. Those measures include:

Physical Security

- Physical access control systems in place (Badge access control, Security event monitoring etc.)
- Surveillance systems including alarms and, as appropriate, CCTV monitoring
- Clean desk policies and controls in place (Locking of unattended computers, locked cabinets etc.)
- Visitor Access Management
- Destruction of data on physical media and documents (shredding, degaussing etc.)

Access Control & Prevention of Unauthorized Access

- User access restrictions applied and role-based access permissions provided/reviewed based on segregation of duties principle
- Strong authentication and authorization methods (Multi-factor authentication, certificate based authorization, automatic deactivation/log-off etc.)
- Centralized password management and strong/complex password policies (minimum length, complexity of characters, expiration of passwords etc.)
- Controlled access to e-mails and the Internet
- Anti-virus management
- Intrusion Prevention System management

Encryption

- Encryption of external and internal communication via strong cryptographic protocols
- Encrypting PII/SPII data at rest (databases, shared directories etc.)
- Full disk encryption for company PCs and laptops
- Encryption of storage media
- Remote connections to the company networks are encrypted via VPN
- Securing the lifecycle of encryption keys

Data Minimization

- PII/SPI minimization in application, debugging and security logs
- Pseudonymization of personal data to prevent directly identification of an individual
- Segregation of data stored by function (test, staging, live)
- Logical segregation of data by role based access rights
- Defined data retention periods for personal data

Security Testing

- Penetration Testing for critical company networks and platforms hosting personal data
- Regular network and vulnerability scans

2. **Integrity**

"Integrity refers to ensuring the correctness (intactness) 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."

Appropriate change and log management controls are in place, in addition to access controls to be able to maintain the integrity of personal data such as:

Change & Release Management

- Change and release management process including (impact analysis, approvals, testing, security reviews, staging, monitoring etc.)
- Role & Function based (Segregation of Duties) access provisioning on production environments

Logging & Monitoring

- Logging of access and changes on data
- Centralized audit & security logs
- Monitoring of the completeness and correctness of the transfer of data (end-to-end check)

3. **Availability**

"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."

We implement appropriate continuity and security measures to maintain the availability of its services and the data residing within those services:

- Regular fail-over tests applied for critical services
- Extensive performance/availability monitoring and reporting for critical systems
- Incident response programme
- Critical data either replicated or backed up (Cloud Backups/Hard Disks/Database replication etc.)
- Planned software, infrastructure and security maintenance in place (Software updates, security patches etc.)
- Redundant and resilient systems (server clusters, mirrored DBs, high availability setups etc.) located on off-site and/or geographically separated locations
- Use of uninterruptible power supplies, fail redundant hardware and network systems
- Alarm, security systems in place
- Physical Protection measures in place for critical sites (surge protection, raised floors, cooling systems, fire and/or smoke detectors, fire suppression systems etc.)
- DDOS protection to maintain availability
- Load & Stress Testing

4. **Data Processing Instructions**

"Data Processing Instructions refers to ensuring that personal data will only be processed in accordance with the instructions of the data controller and the related company measures"

We have established internal privacy policies, agreements and conduct regular privacy trainings for employees to ensure personal data is processed in accordance with customers' preferences and instructions.

- Privacy and confidentiality terms in place within employee contracts
- Regular data privacy and security trainings for employees
- Appropriate contractual provisions to the agreements with sub-contractors to maintain instructional control rights
- Regular privacy checks for external service providers
- Providing customers full control over their data processing preferences
- Regular security audits