Public

IBODigital GmbH, Ammerthalstraße 9, 85551, Kirchheim

Technical and organizational measures (TOM)

MAPPING

Laws and regulations

- [x] K-2151 | GDPR - General Data Protection Regulation (DE: DSGVO)

PRELIMINARY REMARK

The Customer as Controller and IBODigital as Processor shall, pursuant to Art. 32 GDPR, take appropriate technical and organizational measures to ensure a level of protection appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons.

The customer is responsible for identifying and implementing its own appropriate measures in accordance with Art. 24 GDPR. IBODigital recommends introducing and implementing the recommended measures of relevant guidelines and standards, based on ISO/IEC 27002 and the Federal Office for Information Security.

In the following, those measures are presented that IBODigital itself has taken to ensure the security of processing. Where applicable, suitable measures taken by relevant subcontractors, in particular with regard to physical security by Infrastructure-as-a-Service providers (IaaS), are listed and marked or referred to accordingly.

TECHNICAL AND ORGANIZATIONAL MEASURES (TOM)

IBODigital has the following technical and organizational measures in place to ensure compliance with Art. 32 GDPR: encryption and pseudonymization, ability to ensure confidentiality, integrity, availability and resilience, recoverability and corresponding audit procedures.

CONFIDENTIALITY

Organizational control
The aim is to ensure that the internal organization meets the specific requirements of the data protection.

Measures

- [x] K-2358 | Internal organizational instructions
- [x] K-2359 | Appointment of a data protection officer
- [x] K-2360 | Restriction on personal and business use of communication devices
- [x] K-2363 | Obligation to maintain confidentiality and data protection
- [x] K-2364 | Data protection training
- [x] K-2365 | Personnel security

Encryption and pseudonymization of personal data
It is ensured that personal data is only stored in the system in a manner that prevents third parties from identifying data subjects.

Measures

- [x] K-2366 | Key management
- [x] K-2367 | Database and storage encryption
- [x] K-2368 | Information transfer via encrypted data networks or tunnel connections
- [x] K-2369 | Encryption of mobile storage media
- [x] K-2370 | Encryption of storage media on laptops
- [x] K-2371 | Encrypted exchange of information and files
- [x] K-2372 | Email encryption

Physical access control
Access by unauthorized persons to the IT system and processing facilities, by means of which the processing is carried out, is prohibited.

- [x] K-2373 | Closed entrance doors
- [x] K-2374 | Controlled key allocation
- [x] K-2375 | Monitoring and escorting third parties
- [x] K-2376 | Securing of rooms with increased protection requirements
- [x] K-2377 | Locked windows and doors
- [x] K-2378 | Clear desk
- [x] K-2379 | Clear screen
- [x] K-2380 | Physical and environmental security of server systems

Authorization check
The use and processing of data protected under data protection law by unauthorized persons is prevented.

Measures

- [x] K-2381 | Secure authentication
- [x] K-2382 | Authorization determination and assignment following approval by administration
- [x] K-2383 | Secure passwords
- [x] K-2384 | Prohibition of the disclosure of passwords and the use of "shared accounts"
- [x] K-2385 | Anti-virus software
- [x] K-2386 | Public wireless networks via VPN connection

Access control
It shall be ensured that persons authorized to use an automated processing system only have access to the personal data for which they have access authorization.

Measures

- [x] K-2387 | Roles and authorization concept
- [x] K-2388 | Control of access rights to customer systems by contracting entity
- [x] K-2389 | Assignment of access rights
- [x] K-2390 | Host-based threat detection
- [x] K-2391 | Network security
- [x] K-2392 | Logging of processes relating to logging in and logging out

Separability

It is ensured that personal data collected for different purposes can be processed separately and separated from other data and systems in such a way as to prevent unplanned use of such data for other purposes.

Measures

- [x] K-2393 | Separation of development, test and production environment
- [x] K-2394 | Separation of networks
- [x] K-2395 | Single-tenancy architecture

INTEGRITY

Transfer control
It is ensured that the confidentiality and integrity of personal data are protected during the transfer of information.

Measures

- [x] K-2396 | Transfer encryption
- [x] K-2397 | Prohibited disclosure to unauthorized third parties
- [x] K-2398 | Logging of data transfer

Input control
The aim is to ensure that it is possible to subsequently check and determine which personal data has been entered or changed into processing systems at what time and by whom.

Measures

- [x] K-2399 | Logging of system activities within the admin and customer system as well as evaluation

AVAILABILITY

Availability control
Ensure personal data is protected against accidental destruction or loss.

Measures

- [x] K-2400 | Data protection procedures / backups
- [x] K-2401 | Geo-redundancy with respect to the server infrastructure of the productive data and

- [x] K-2402 | Capacity management
- [x] K-2403 | Warning systems to monitor the availability and condition of server systems
- [x] K-2404 | Information security event management
- [x] K-2405 | Datacenter climate control
- [x] K-2406 | Datacenter fire and water damage protection

Restorability
It is ensured that systems can be reliably recovered in the event of a physical or technical failure.

Measures

- [x] K-2407 | Data recovery tests
- [x] K-2408 | Disaster recovery concept

REVIEW AND EVALUATION

Contract monitoring
It is ensured that personal data processed on behalf of a client can only be processed according to the client's instructions.

Measures

- [x] K-2409 | Data processing pursuant to Art. 28 GDPR
- [x] K-2410 | Careful selection of suppliers
- [x] K-2411 | Carrying out regular reviews / collection of evidence

Assessment of management system
Description of the procedures for regularly reviewing, assessing and evaluating the effectiveness of technical and organizational measures.

Measures

- [x] K-2412 | Risk assessment
- [x] K-2413 | Carrying out internal audits
- [x] K-2414 | Verification of compliance with security policies and standards
- [x] K-2415 | Verification of compliance with technical specifications
- [x] K-2416 | Process for continuous improvement of the management system

Date

04-2023