d.velop

Technical and Organizational Measures (Security Concept for Information Security, Data Protection and Confidentiality) of the d.velop Group

Contents

1 Change History

Version	Date	Changed by	Comment
1.0.0	3/29/2018	SOCH/SKRE	Created pursuant to GDPR
1.0.1	3/14/2018	SOCH	Adjusted organization
1.0.2	8/22/2018	SOCH	Adjusted "Encryption of Radio Networks" section
1.0.3	6/6/2019	SOCH	Revision, title changed to "Annex: Technical and Organizational Measures (IT Security and Data Protection Concept)"
1.0.4	10/25/2019	SOCH	Revision, adjustments to formatting and section 2.2.2 "Password Policy"
1.1.0	4/30/2020	SOCH	Revision, reformatting, special protection measures divided into on-premises and d.velop cloud, subsections of 2.1.1 updated, company name added to title
1.1.1	5/6/2020	SOCH	Tenant isolation moved to separate section: 4.1.3.1
1.1.2	07/20/2020	SOCH	Added section 2.1.6 "Telework and Remote Work" and sections 2.3.7/4.3.6 "Vulnerability and Resilience Tests"
1.1.3	09/02/2020	SOCH	Adjusted product area in Section 4.3.3, added Section 4.3.5 "Change Management Process"
1.2.0	04/27/2021	SOCH	Update, confidentiality added, data protection officer changed
1.2.1	06/08/2021	SOCH	Added section 2.1.6 "Telework and Remote Work"
1.2.2	10/21/2021	EWIN	Adjusted DPO
1.2.3	02/02/2022	EWIN	Converted to new contract template
1.2.4	08/02/2022	EWIN	Added section 2.1.4.3 "Deep Learning"
1.2.5	09/05/2022	EWIN	Stylistic adjustments
1.2.6	09/12/2022	EWIN	Section 88 of the German Telecommunications Act (TKG) replaced by Section 3 of the German Telecommunications and Telemedia Data Protection Act (TTDSG)
1.2.7	11/06/2023	EWIN	Removed section 2.1.4.3 "Deep Learning"
1.2.8	11/21/2023	EWIN	2.4.1.9 German Act against Unfair Competition (UWG) = German Act on the Protection of Business Secrets (GeschGehG)
1.3.0	03/22/2024	SOCH/SBEN/NMOE	Restructuring, adjusted the current technical and organizational measures
1.3.1	14/11/2024	SOCH	Section 3 of the German Telecommunications and Telemedia Data Protection Act (TTDSG) replaced by Section 3 of the German Telecommunications Digital Services Data Protection Act (TDDDG)

2 Information Security Management System

d.velop has implemented an information security management system that is certified according to ISO/IEC 27001 and tested according to TISAX. The scope, certificates and further details can be found on the following website: https://www.d-velop.de/ueber-d-velop/zertifizierungen

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

Within its internal IT systems, d.velop AG processes data in a central data center certified in accordance with ISO 27001.

Data that customers store in d.velop cloud products is processed not in the data centers of d.velop AG but rather in separate data centers. These can be found in the service descriptions of the respective products.

3.1 Physical Access Control

3.1.1 d.velop campus

The d.velop campus in Gescher, Germany is the headquarters of d.velop AG.

3.1.1.1 Physical Access Control System

All buildings on the d.velop campus have an electronic physical access control system, which is linked to motion detectors and alarm systems. Alarm notifications are sent to an external security service.

The building's facade is mainly glass, allowing rooms to be seen from the outside. The support and remote maintenance facilities are located on the first floor above ground level and have an additional privacy screen inside the building. All employees have a personalized ID card that allows them access to locked buildings.

3.1.1.2 Reception and Visitor Policy

Visitors to the d.velop companies are received in the main building. The reception desk is constantly manned during our business hours. The reception staff member registers visitors and accompanies the visitors into the meeting rooms. Visitors are permitted to independently cross over into the other buildings only in exceptional cases and only when accompanied by d.velop employees.

3.1.1.3 Workflow for Granting Physical Access Permissions

Access permissions are assigned via a workflow-based system. d.velop employees must submit an electronic application for access permission.

3.1.1.4 Security Zones

There are individual security areas within the company buildings. These security areas are secured by further technical measures. The security zones are not recognizable to outsiders and are only listed in an internal document about the IT security concept. The security areas include the equipment rooms, and the rooms belonging to the company management, HR and IT administration.

3.1.2 Other Locations of d.velop AG or Affiliated Subsidiaries

In addition to the headquarters on the d.velop campus in Gescher, there are further locations that fulfill at least the following minimum requirements:

- Electronic physical access control system or central physical locking system
- Locked buildings
- Visitor policy (if visited by customers/partners)

3.1.3 Physical Security for d.velop Cloud Products

d.velop operates its cloud products exclusively in the data centers of operators who have a valid certification according to ISO/IEC 27001. These data centers therefore have the following technical and organizational measures to ensure physical security (not exhaustive):

- Defined physical security zones
- Electronic physical access control systems exclusively for authorized personnel

- Visitor policy
- Trained security staff
- Video surveillance

3.2 System Access Control

3.2.1 User Name & Password

d.velop AG operates a central directory service for all d.velop companies, which is used for logging on to all live endpoints and servers. Employees are always assigned their own personal user account.

3.2.2 Password Policy

An internal policy for access and password management specifies the password requirements. The password policy is in line with the current state of the art and follows the recommendations of recognized authorities (including NIST and BSI).

3.2.3 Multi-factor Authentication

d.velop uses multi-factor authentication. Whether users are asked for a second authentication factor depends on which endpoint they are using to access the IT system as well as the security level of the particular system.

3.2.4 Single Sign-On

If IT systems support single sign-on, this mechanism is permanently enabled. For systems without such a mechanism, an internal policy for prescribed access and password management mandatory requirements.

3.2.5 Authorization Process for System Access Permissions

System access permissions to the IT systems are always assigned on a personalized basis. New user accounts are created for d.velop employees as part of an onboarding process, which is initiated by the internal HR department. Where possible, data access permissions (including additional permissions) are assigned on a role-specific basis and always in writing.

3.2.6 System Access to d.velop Cloud Products

Cloud products are accessed using personalized accounts and under the security measures described above. Restricted service accounts are used for the automated provision of updates and infrastructure.

3.2.7 Authorization Process for System Access Permissions for Cloud Products

System access permissions for cloud products are granted exclusively according to the “least privilege” principle. Permissions are granted to employees by a regulated and traceable workflow in the internal ticket system.

3.2.8 Logging System Access Attempts for Cloud Products

Both successful and failed attempts to access cloud products with administrative access are logged. The logs are reviewed randomly and as necessary.

3.2.9 System Access to Customer Systems (On-Premises Remote Maintenance)

Common remote maintenance procedures include active connection using a remote maintenance solution (e.g. TeamViewer) in the presence of the customer, or using a client VPN software followed by a remote session (remote desktop). d.velop follows the customer’s specifications in all cases. In all procedures, access to the customer’s systems is controlled by the customer himself.

3.2.10 Firewall Systems

Firewall systems with IDS and IPS functionality are used to protect against unwanted intrusions. In IT systems that can be reached over the Internet, only the necessary interfaces are enabled.

d.velop cloud products are protected by firewalls against external attacks. The firewall configuration is adapted according to the level of protection required for the data being processed. The IT systems operated behind the firewall are open to external connections only to the extent necessary (e.g. port 443 for enabling HTTPS for communication between the front end servers and the customer).

3.2.11 Endpoint Detection and Response Solutions

An endpoint detection and response (EDR) solution is used to protect against malware. The signatures are updated automatically. This virus protection is set up and activated on all live internal endpoints (servers, desktop computers, notebooks).

d.velop cloud products use EDR solutions where technically feasible. These serve primarily to protect the d.velop infrastructure and are not explicitly part of the service description.

3.2.12 Anti-spam Solution

An anti-spam solution is installed to protect against unwanted e-mails (phishing and spam) and malware. All incoming e-mails are automatically scanned for spam.

3.2.13 Password-Protected Screen Savers

A password-protected screen saver is activated when a workstation is left inactive. The password-protected screen saver is automatically activated after 10 minutes at the latest. An organizational guideline instructs employees to always lock their screen immediately when leaving their workstation.

3.3 Data Access Control

The d.velop companies are given access to data on the IT systems exclusively as needed and according to the "need to know" principle. All employees of the d.velop companies receive data access to only the IT systems that are absolutely necessary for their daily work.

3.3.1 Management and Assignment of Permissions

For applications and systems that support a detailed permission concept with roles or permission profiles, access to data is restricted by a permission concept within the software. Here, again, users are granted data access to only the applications and systems that are absolutely necessary for them to complete their work.

Additional data access permissions are assigned exclusively in writing.

3.3.2 Classification of Information

An information classification policy defines the minimum requirements for classifying digital and analog information by confidentiality level, and prescribes rules for labeling and correctly using the information in accordance with its classification.

3.3.3 Destruction of Files and Disks

Secure destruction containers and document shredders are set up in designated areas for the disposal of disks and documents. Disposal is carried out on behalf of d.velop AG by certified companies in compliance with data protection regulations. Documents disposed of in the secure destruction containers are destroyed by machines that function in accordance with DIN 66399.

3.4 Separation Control

To ensure that IT systems are separated, d.velop separates its systems both physically and logically.

3.4.1 Separation of Development, Test and Production Environments

All IT systems are divided into development, test and production environments. Needs-based access permissions are used to control data access to the individual environments. New product versions are always installed in a multi-stage process whereby functional testing is first carried out in test environments. The number of employees authorized to access test and production environments of d.velop cloud products is limited to those people for whom access is absolutely necessary to fulfill their tasks.

3.4.2 Tenant Isolation Within d.velop Cloud Products

Within the cloud products, each tenant has its own technical identifier. A tenant usually constitutes a company with multiple employees. The tenant identifier is verified each time data is called in order to ensure data separation between tenants.

3.4.3 Use of Test Data

Only anonymous or anonymized test data is used in development and test environments. Access to live data is not permitted. Permission concepts prevent unauthorized employees from accessing live data.

3.5 Pseudonymization (Art. 32 Para. 1 Lit. a GDPR; Art. 25 Para. 1 GDPR)

Wherever possible, pseudonyms are used in place of real names when processing personal data, e.g. to identify documents stored in cloud products. As user of the cloud products, the customer is additionally responsible for pseudonymizing any personal data they disclose for processing, if necessary.

3.6 Employee Training

All employees complete annual mandatory training on IT security and data protection. Additional measures are instituted as needed to promote further awareness. New employees complete the training courses during their onboarding process.

3.7 Telework and Remote Work

Telework and remote work are only permitted in accordance with a mandatory IT policy. This policy ensures that the workplace complies with the confidentiality requirements of the d.velop Group, that the use of private hardware (Internet connection, peripheral devices, monitors) is kept to a minimum, that documents and disks are not disposed of at home or while traveling, and that endpoints are always stored securely. In addition to this, special requirements or prohibitions from our clients are also observed.

3.8 Secure Software Development and Operation

d.velop uses a shift-left strategy to ensure a secure software development lifecycle (SSDLC). Key aspects of this strategy are defined in an internal policy for information security and data protection in software development and operation. Compliance with this strategy is regularly verified.

4 Integrity (Art. 32 Para. 1 Lit. b GDPR)

4.1 Transfer Control

4.1.1 Transport Encryption

All IT systems and d.velop cloud products that can be accessed from outside the company use transport encryption (e.g. HTTPS). They can only be accessed via encrypted communication channels. Data is encrypted according to the state of the art (including BSI Technical Guideline 02102).

4.1.2 Encryption of Disks

Disks within mobile devices (notebooks, smartphones, tablets) and external disks are encrypted. Data is encrypted using the methods integrated in the operating system (Microsoft BitLocker, Apple FileVault, Apple iOS device encryption).

4.1.3 Encryption of Wireless Networks

All wireless networks (WLAN) that reach internal systems communicate exclusively in encrypted form. The networks are separated for different interest groups (employees, trainees). Internal IT systems cannot be accessed from networks that allow external access (training, guests).

4.2 Input Control

Audit logs ensure that all inputs and changes can be traced.

4.2.1 Document Management System (DMS)

Policies are defined that oblige all employees to archive documents that are subject to retention and archiving requirements in the DMS. This includes records and electronic data that are necessary to ensure the correctness and traceability of all business processes. The DMS enables change histories and audit-compliant archiving of stored documents.

5 Availability and Resilience (Art. 32 Para. 1 Lit. b GDPR)

5.1 Contingency Plans

Central contingency plans and specific instructions are updated on an ongoing basis and take current risks into account (including ransomware, natural disasters, failure of individual IT systems). Regular exercises ensure that all persons involved are familiar with the plans and know how to use them.

5.2 Backup Concept

Live data and IT systems are backed up regularly. The frequency of the backups and the duration of storage depend on the sensitivity of the backed-up data. Backup intervals for d.velop cloud products can be found in the service descriptions of the respective products.

5.3 Importing Security Updates

All live IT systems are updated regularly. Security updates for live endpoints are installed as soon as they are released. Upstream tests ensure that the updates can be installed without any problems.

Central IT systems and d.velop cloud products are regularly updated within planned maintenance windows. If critical security gaps are detected outside of scheduled maintenance windows, appropriate patches are applied immediately.

5.4 Deployment Process

The d.velop Group has established a deployment process for all d.velop cloud products. All changes to cloud products are documented and versioned. The development and introduction of new functions always follows a controlled multi-stage process, in which changes are first tested in development and test systems. Functions are introduced into production environments only after an internal quality review.

5.5 Vulnerability and Resilience Tests

Regular vulnerability and resilience tests are carried out both internally and by external contractors. These tests ensure that vulnerabilities or other deficiencies are identified and corrected in good time.

5.6 Monitoring of IT Systems

d.velop uses various monitoring and alarm systems to monitor its IT systems. Defined alarms provide immediate notification when operation deviates from normal. This allows us to detect malfunctions immediately and shorten the time to restoring normal operation.

5.7 Redundancies

Critical IT systems and supply devices (e.g. power supply, UPS) have a redundant design to ensure uninterrupted operation. The IT systems are divided such that individual fire compartments / availability zones can fail.

5.8 Technical Monitoring of Data Centers

The data centers commissioned by d.velop use measuring instruments for the early detection of natural hazards (fire, water). Systems such as uninterruptible power supplies (UPS) and fire extinguishing systems prevent extensive destruction in the event that damage does occur.

6 Procedure for Regular Review, Assessment and Evaluation (Art. 32 Para. 1 Lit. d GDPR; Art. 25 Para. 1 GDPR)

6.1 Data Protection Management

The d.velop Group has a data protection management concept with clearly defined responsibilities and workflows. A status team at d.velop AG meets regularly to discuss all measures and developments necessary for data protection and information security. It also monitors the implementation of these measures in the d.velop companies and suggests necessary or recommended changes to the management board of d.velop AG and, if necessary, the management of other d.velop companies.

6.1.1 Data Protection Mission Statement

All d.velop companies take the protection of personal rights and personal data very seriously. The d.velop Group employs a group-wide data protection management system to meet these needs. The data protection management system is based on the IT Baseline Protection (IT-Grundschutz) Compendium of the Federal Office for Information Security (BSI), on the recommendations of the German Association for Data Protection and Data

Security (GDD), and on the recommendations of the overarching industry association, bitkom. It is reviewed and updated regularly and as required.

6.1.2 Data Protection Policy

d.velop AG has adopted a group-wide policy from the management board that defines the importance of data protection and information security for the entire d.velop group. This policy is the basis of the data protection measures and business processes implemented by the d.velop Group and documented in this document.

6.1.3 Nomination of a Data Protection Officer

Where required by law, the d.velop companies have appointed an external data protection officer. As of 10/01/2021, the external data protection officer for d.velop AG is Mr. Nils Möllers. The external data protection officer of d.velop AG has the expertise necessary to carry out the duties of the company data protection officer. He is a certified data protection officer and has several years of experience in data protection consulting.

Contact details of the data protection officer:

Nils Möllers
Keyed GmbH
Siemensstrasse 12, 48341 Altenberge
datenschutz@d-velop.de

The external data protection officer of d.velop AG reports directly to the management board of d.velop AG and thus reports directly to the highest management level of the controller in accordance with Art. 38 Para. 3 Sentence 3 of the GDPR. d.velop AG also ensures that the external data protection officer is exempt from instructions in the exercise of his data protection activities in accordance with Art. 38 Para. 3 Sentences 1, 2 of the GDPR.

6.1.4 Reporting

The external data protection officer has the opportunity to report directly to the management board of d.velop AG in bimonthly status meetings. The information security officer and, if necessary, the management board and the legal department also participate in these meetings.

In addition to the status meetings, reports and inquiries are communicated directly by e-mail. Important decisions are also recorded in an activity report produced by the external data protection officer.

6.1.5 Activity Reports

The external data protection officer keeps activity reports that record individual actions and events relating to data protection. These activity reports are also submitted to the management board (see Reporting). The activity reports are confidential and intended only for the external data protection officer and the management board.

6.1.6 Record of Processing Activities (Art. 30 GDPR)

In accordance with statutory regulations, the d.velop Group keeps a list of its own processing activities pursuant to Art. 30 Para. 1 GDPR as well as a list of processing activities that it carries out on someone else's behalf (e.g. for d.velop cloud apps) pursuant to Art. 30 Para. 2 GDPR.

6.1.7 Quality Management System

d.velop operates a quality management system that contains a multitude of work instructions, procedural instructions, policies and datasheets. These are considered binding for data protection management in all d.velop companies.

6.1.8 IT Security and Data Protection Team

d.velop AG has a team for IT security, confidentiality and data protection (see above). It meets regularly every two weeks.

6.1.9 Employee Obligations

All employees of the d.velop companies are bound in writing to confidentiality (formerly: data secrecy according to Section 5 of the German Federal Data Protection Act (BDSG)), social secrecy (Section 35 of the German Social Code Volume I (SGB I)), business secrecy (German Act on the Protection of Business Secrets (GeschGehG)) and professional secrecy (Section 203 of the German Criminal Code (StGB)), and if necessary telecommunications

secrecy (Section 3 of the Telecommunications Digital Services Data Protection Act (TDDDG)) and banking secrecy. This secrecy declaration is an integral part of the employment contract and is placed in the employee's personnel file. The secrecy declaration is accompanied by an information sheet that describes the meaning of these individual paragraphs.

6.1.10 Training

Instruction in data protection matters is part of the onboarding procedure for new employees. During onboarding, employees are instructed in both data protection according to the GDPR and social secrecy according to the SGB. In addition to these training sessions, employees are made aware of current topics in data protection via the d.velop Group intranet. All employees can also use the e-mail address datenschutz@d-velop.de to address questions and data protection incidents to the external data protection officer.

6.1.11 Intranet and Data Protection Portal

News and changes related to data protection, IT security and confidentiality in the d.velop Group are published in employee meetings as well as on the d.velop Group intranet. Employees can access all relevant documents regarding data protection via the intranet.

6.2 Data Breach Management

In the event of a suspected data protection violation, the d.velop Group has defined and described a notification workflow that ensures that the incident is immediately reviewed by the status team (see above). The incoming messages are always sent to incidents@d-velop.de so that the data protection officer, information security officer, head of IT and legal department are notified immediately. If the situation requires, these entities then initiate the necessary countermeasures, notify the relevant supervisory authorities and, if necessary, notify the data subjects in accordance with the legal obligations. This is followed by a comprehensive evaluation of the entire process to derive lessons learned and, if necessary, to make systematic or selective changes to avoid future data protection violations.

6.3 Privacy-Friendly Default Settings (Art. 25 Para. 2 GDPR)

The systems used by the d.velop Group are always pre-configured for data protection when provided internally or to the customer. Processing that is not necessary will only be carried out at the user's instigation or with his/her prior consent. Optional input fields in d.velop Group applications are marked as such; there is, of course, no obligation to fill them in.

6.4 Order Control

As the contractors, the data processing activities of d.velop AG and other d.velop companies are subject to Art. 28 GDPR and, if applicable, Section 80 SGB X. The client, as controller, is responsible for compliance with data protection regulations and laws. The d.velop companies actively assist the client in this responsibility through a multitude of technical and organizational measures. This document is part of these measures. If necessary, the d.velop companies shall conclude a data processing agreement with you, the customer, in accordance with the legal requirements.

6.4.1 Subcontractors

The d.velop Group is a group of companies consisting of d.velop AG and several subsidiaries.

The d.velop companies specialize in subareas of the ECM environment and are regularly used as subcontractors for data processing. In addition to corresponding partnership agreements and framework service agreements, the data processing agreement with each subsidiary forms an essential part of the data processing relationship. This data processing agreement always grants the main client within the d.velop Group the right of control, right of inspection and right of instruction.

In any data processing agreement concluded with a customer, the d.velop company acting as processor lists the subsidiaries used as subcontractors (further processors) as well as any additional third parties—which have been carefully selected for suitability—used as subcontractors along with the services they provide. The customer agrees to the subcontracting by signing the agreement or, if necessary, a separate agreement. The customer shall also be entitled to the control, inspection and instruction rights agreed with the subcontractors.

The d.velop companies are regularly audited by customers or external third parties (e.g. auditing companies). Any recommendations made during the audits are subsequently evaluated by the IT security, confidentiality and data protection teams (see above) and then implemented where necessary or useful to improve data protection.

All service relationships between the d.velop companies and their customers and subcontractors are transparently documented in the DMS (see above). This makes it possible to determine at any time for whom the d.velop companies provide which services and with which subcontractors.

7 Special Confidentiality Measures

Section 2 No. 1 Lit. b) of the Act on the Protection of Business Secrets (GeschGehG) requires that the lawful holder shall establish confidentiality measures appropriate to the circumstances to protect trade secrets. The following measures apply in addition to the aforementioned measures for all trade secrets and other confidential information which the d.velop Group uses and has access to.

7.1 Establishment of Binding Rules of Conduct

All d.velop companies have subjected themselves to binding rules of conduct regarding confidentiality, data protection and information security. This security concept is part of these rules of conduct, which are published in full on the d.velop AG service portal. The rules of conduct ensure that an equally high level of security is guaranteed in every company within the d.velop Group.

7.2 Conclusion of Non-disclosure Agreements

The d.velop companies have concluded non-disclosure agreements (NDA) among themselves. These are another part of the rules of conduct (see above). The d.velop companies also conclude non-disclosure agreements with their customers that are customary for the market and comply with the legal requirements of the Act on the Protection of Business Secrets, and pass these through to any subcontractors and third parties in the service chain.