Detailed assessment results

Audit report 2024

Certification of information security and data protection management system according to DIN EN ISO/IEC 27001:2022 and ISO/IEC 27701:2019

for

DATEV eG

Paumgartnerstr. 6 - 14

90429 Nürnberg, Germany

main location with all associated locations

CIS - Certification & Information Security Services GmbH

Headquarters

1010 Vienna, Salztorgasse 2/3/7

Phone.: +43 1 532 98 90
Fax: +43 1 532 98 90 89
office@cis-cert.com
www.cis-cert.com

This audit report must be treated as confidential. It may only be disclosed to third parties with the approval of DATEV.

Table of Contents

1. Explanatory notes on the audit

1.1 Initial situation

Standard references ISO/IEC 27001/27701: 4/5.2 Context of the organization

According to the published brief profile of DATEV eG, it is the third-largest provider of business software in Germany (IDC ranking 2023 and one of the major European IT service providers). Based in Nuremberg, DATEV eG provides software, cloud solutions and know-how that forms the basis for digital collaboration between small and medium-sized businesses and the tax consultants, who take care of the business management needs of the companies. Through this community, DATEV eG supports a total of 2.8 million businesses, self-employed persons, local authorities, associations and institutions. With more than 8,900 employees, the company supports around 620,000 customers as a partner with solutions for the digitalization of their commercial processes. Information security, data protection and tax compliance have the highest priority.

Since information security and data protection are inseparable topics, DATEV eG takes an integrated approach and had its information security and data protection management system (ISMS/DSMS) certified according to ISO/IEC 27001:2022 and ISO/IEC 27701:2019 by CIS – Certification & Information Security Services GmbH (following CIS). In addition to these certificates, other ISO/IEC certificates, such as for the disposal or for the quality and service management process, are available for retrieval on the company website.

1.2 Purpose of the audit

One building block for building trust and providing evidence of the high priority and effectiveness of the measures taken to ensure information security and data protection is the provision of the ISO certificates for the management systems acquired since 2006 on www.datev.de/datenschutz. DATEV eG would like to enable its members and other customers to fulfil the control obligations imposed on them in a simple and effective manner. Additionally, DATEV eG would like to be able to effectively fulfil any documentation obligations vis-à-vis external bodies and control bodies regarding the selection of its service provider.

With a voluntary information security and data protection audit, DATEV eG would like to demonstrate uniformly and across the board that information security and data protection are implemented appropriately, effectively and sustainably in an integrated management system. Furthermore, DATEV eG would like to demonstrate that the implemented processes ensure that the processing activities in the planning, implementation, testing and continuous improvement to

achieve the objectives of confidential externality, availability incl. resilience and integrity vis-à-vis existing data protection and information security risks are secure and designed in such a way that they comply with the principles of processing personal data.
DATEV eG would also like to demonstrate that its risk management process ensures that both information security risks and data protection risks to the rights and freedoms of natural persons are considered when processing their data.

The certificate also attests that the processes of the integrated ISMS/DSMS ensure that the technical and organizational measures are planned, implemented and maintained appropriately and effectively.

1.3 Scope of application of the IS/DS system

Standard references
ISO/IEC 27001/27701:
4.3/5.2.3 Determining the scope of the ISMS/DSMS 4.4/5.2.4 Information security management system

The audit for the assessment of the information security and data protection management system covers DATEV eG with all its locations in Germany. This, in particular, includes software development, data processing, the provision of services, training and consulting services, data centers in Nuremberg and Feucht as well as the Digital & Print Solution Centre and the 23 DATEV branches existing at the time of the audit.
The audit criteria are the standard requirements of ISO/IEC 27001 in combination with ISO/IEC 27701 and the required Statement of Applicability "Statement of Applicability: | Version 2.0 | 2024-09-19".

The Statement of Applicability is based on the applicable measures from the annexes of both standards and does not contain any exclusions. Furthermore, other internal and external requirements from procedures, instructions, contracts, etc., flow into the audit criteria.

The assessment of the locations and branches was carried out in the so-called sampling procedure, in which the number and selection of the locations to be assessed for the audit is determined in accordance with the certification rules.

Based on a holistic approach, DATEV eG has established an integrated management system that combines organizational, technical and location-related aspects and has an internal impact on structures and employees as well as an external impact on members, their clients, other customers and business partners.

2. Description of the integrated IS/DS management system

2.1 Responsibility of the management

Standard references
ISO/IEC 27001/27701:
5.1/5.3 Leadership and commitment 5.2/5.3.2 Policy 5.3/5.3.3 Organizational roles, responsibilities and authorities 6.2/5.4.2 Information security objectives and planning to achieve them

The Board of Directors of DATEV eG supports the information security and data protection management system by approving the information security and data protection strategy and the associated directives and by providing sufficient resources. The information security and data protection management system are fully integrated into DATEV eG's target and control system. The Board of Directors receives information on the achievement of objectives and current issues via the regular report of the Information Security and Data Protection Officer. In accordance with the requirements of a management system, the Board of Directors is involved in important issues relevant to information and data protection. Important changes to the IS/DS management system are dealt with and approved by the Executive Board via decision papers.

The defined directive "Corporate Security and Data Protection" provides overarching guiding principles with DATEV-wide validity for planning, implementing and constantly maintaining the legal, regulatory, customer-oriented and other requirements.
The requirements for data protection and corporate security are documented in policies and standards in the Security Privacy Framework (SPF) based on the requirements of the standards, e.g. ISO/IEC 27001 and ISO/IEC 27701.

The integrated information security and data protection management system of DATEV eG combines the aspects and requirements of the ISO/IEC 27001/27701 standards and the data protection-specific requirements from the regulatory requirements for data protection, in particular the General Data Protection Regulation and the Federal Data Protection Act.

2.2 Risk management

Standard references
ISO/IEC 27001/27701:
6.1/5.4.1 Actions to address risks and opportunities 6.1.2/5.4.1.2 Information security risk assessment 6.1.3/5.4.1.3 Information security risk treatment

DATEV eG uses a risk-based approach that considers both information security risks and data protection risks for the rights and freedoms of natural persons.
Upstream of the IS/DS risk assessment, in the case of services with personal data, the notification of the information for the maintenance of the register of processing activities is carried out. The established tool-supported risk management process, which all services (processing activities with or without personal reference) must undergo, enables the identification, assessment, treatment or minimization and monitoring of risks. In the risk assessment, the probability of occurrence and the amount of damage for the IS and DS risks are evaluated based on the elementary threats of the BSI and the derived data protection threats of the GDPR. Depending on the result of the relevance test for carrying out a data protection in the event of a positive assessment, this is implemented on a project-oriented basis using detailed working aids.

2.3 Information security and data protection guidelines

Standard references
ISO/IEC 27001/27701:
A.5.1 Information security policies and guidelines 7.5/5.5.5 Documented information

The design of processing procedures for personal data is carried out methodically using the requirements of the Security Privacy Framework (SPF), both for processing as a controller and on behalf of the controller, considering the measures to be implemented. The focus is on the treatment of information security and data protection risks ensuring secure operations and compliance with the processing principles provided for by the GDPR, such as lawfulness and transparency.

Appropriate processes are defined to ensure the rights of data subjects, such as access, rectification, erasure, restriction, transfer and objection. These include, among other things, the identification of the data subject, compliance with deadlines, the involvement of responsible employees and the provision of evidence. The handling of information security and data protection

incidents is controlled by processes. This includes various sub-processes that define how to report within DATEV eG when a possible incident occurs, how to report incidents with data protection relevance to the supervisory authority within the specified period and how to notify those affected.

2.4 Internal and external communication

Standard references
ISO/IEC 27001/27701:
7.4/5.5.4 Communication

The central element of the information security and data protection management system is internal and external communication. Within the framework of the annual marketing and sales planning, the measures of the communication and marketing concept are determined. The aim is to provide information about the current security situation and measures to raise awareness to the respective target group. Numerous communication media are available for this purpose.

Internally, the company news, department news, data protection blog, information events, training courses, directives and guidelines are particularly worth mentioning. The need for communication with external stakeholders exists with all members, customers, clients and other interested parties, which is fulfilled via the DATEV magazine with focus topics, the blog in cooperation with DifÜ – digitaler Führerschein (digital driver license), the Trialog magazine, events, trade fairs and congresses etc.

DATEV's website offers members and interested parties' comprehensive information on DATEV's products and services. The web pages 'Data Protection and Data Security at DATEV' include a wide range of information on the data protection principles at DATEV, on order processing agreements, technical and organizational measures as well as data protection checklists and detailed service descriptions of the DATEV products incl. the respective regulations on order processing and much more.

2.5 Document management

Standard references
ISO/IEC 27001/27701:
7.5/5.5.5 Documented information

The Organization Handbook (OHB), a collection of organizational instructions, was replaced by the DATEV Set of rules, the new binding set of rules of DATEV eG. It is a graduated procedure for

setting rules that distinguish between the Code of Business Conduct, Directives, Policies and Standards.

The overarching guidelines on corporate security and data protection as well as data ethics are regulated as documents in the form of directives. In contrast, the contents of policies and standards, derived from norms, laws and internal guidelines, are mapped with the help of a SharePoint solution, the Security Privacy Framework (SPF). The SPF represents the binding framework for action for all employees of DATEV eG and must be implemented by them in their area of responsibility in accordance with the risk-oriented procedure.

During the restructuring, the original OHB regulations were assigned to the persons responsible in the specialist departments and checked by them for relevance and topicality Subsequently, the specialist managers drew up the standards, supported by training material. The approval process for these standards provides for coordination of the content with the person responsible for the domain of the regulatory area as well as approval of a further person responsible in the corresponding specialist area. These quality assurance measures ensure a coherent and consistent framework of specifications. In total, more than 350 OHB specifications have been replaced by more than 230 SPF standards.

2.6 Planning and control of information security and data protection processes

Standard references
ISO/IEC 27001/27701:
8.1/5.6.1 Operational planning and control

The information security and data protection management system bring the responsibilities, resources, processes and methods for compliance with the requirements from the information security and data protection area into a homogeneous structure and thus enables transparent and systematic planning, implementation and continuous improvement of the processes. The defined specifications from the Security Privacy Framework have been incorporated into the design of the processes and their operational implementation.

2.7 Organization of information security and data protection

Further standard references ISO/IEC 27001/27701: 5.3/5.3.3 Organizational roles, responsibilities and authorities A.5.2 Information security roles and responsibilities A.5.3 Separation of duties A.6.3 Information security awareness, education and training A.7 Physical controls

2.7.1 Three-Lines-of-Defence-Model

DATEV eG follows the model of the three lines of defence for a systematic approach to risks that may occur in the company. These must be recorded, identified, analyzed and evaluated at an early stage and communicated within the company.

The 1st line consists of the operational IT security and privacy teams responsible for providing ongoing advice to the specialist departments. They are supported by the divisional data protection officers, data protection coordinators and security engineers.

The 2nd line, as a governance unit, is responsible for creating guidelines and conducting internal audits to monitor and support the 1st line. The Governance unit consists of the Strategy & Certifications and Management Systems & Governance teams.

The 3rd Line is carried out by the Audit Department. It monitors risk management as an independent body.

A data protection officer (DPO) has been appointed and acts independently in the performance of his data protection tasks. Due to the thematic proximity and the associated integration of the management systems for information security and data protection, he also fulfils the role of the Information Security Officer (ISO). In his dual role, he develops and trains specifications, monitors their implementation and assumes central control for all information security and data protection management processes.

The Information Security Officer and Data Protection Officer is supported in the fulfilment of his tasks by competent, full-time employees and by numerous other data protection, security and control bodies of the institution. These include, for example, the overall security committee, the divisional officers for data protection or physical security. The special position of the information security or data protection officer from the point of view of DATEV eG is documented, among other things, by his membership of the group of senior executives.

2.7.2 Organization of the DATEV branches

The DATEV branches are managed according to central guidelines regarding information security and data protection. This includes, among other things, the definition of information security/data protection obligations and tasks.
All branches are included in the scope of the technical and organizational measures published on www.datev.de. The management of the respective branch plays a central role. It is responsible for the operation and security of one or several branches.

The regulations on information security and data protection for branches are described in the specifications of the Security and Privacy Framework (SPF). In principle, all regulations apply to branch offices in the same way as to DATEV locations in Nuremberg. Branch-specific characteristics for branch management and employees are defined accordingly in the SPF. All employees who visit or work in branch offices must familiarize themselves with the different regulations that apply locally.

The requirements for physical security in the branches cover the areas of access control, visits, technical room and fire protection.

Access to the branch is divided between the training area and the internal area. Access to the internal area is restricted by physical security measures and is, among other things, monitored by video. No confidential external information or personal data is processed in the training area.

Employees in the internal areas of the branches MUST check and document the identification of all visitors. All visitors must identify themselves with a valid, official photo identification. The person visited is obliged to pick up visitors or have them picked up at the reception or at the entrance of the branch or the internal area of the branch and to carry out a short safety briefing. During the entire stay within the internal area of the DATEV branch office, visitors must be accompanied.

Technical rooms in branch offices are explicitly designated as security areas and secured by a technical access system that is controlled by the central security department in Nuremberg. Access is only possible by dedicated employees, such as the branch office's security officer, and is notified and logged with company security.

Sealed aluminum containers from an external service provider are provided for the collection and disposal of paper data carriers. When the fill level of the security containers is reached, the branch office arranges for the disposal partner to pick them up. The security containers are transported in closed and GPS-monitored box vehicles. At the disposal company, the containers are tipped and opened after passing through the security gate, so that the collected material can be fed directly into the shredding plant and destroyed without being inspected by external parties.

The selection, inspection and control of disposal partners is carried out centrally. A framework agreement exists for a well-known waste management company. Important selection criteria

include certifications and certificates, including ISO 9001:2015 quality management and ISO 21964/DIN 66399 data destruction process.
The control includes an annual on-site audit of the disposal partner based on a checklist and a site inspection to assess building security, access systems, etc.
Electronic data carriers for disposal are rarely found in the branches and are passed on to internal IT for disposal by the responsible security officers at the branches.

The principle of mobile working is equally applicable to working in the branch office. For example, during mobile working, personal data is only processed on behalf of a controller, using mobile devices provided by DATEV with a remote connection to DATEV networks. The hard disks of the mobile workstation computer are fully encrypted. The electronic transfer of data to the data center takes place via an encrypted connection with two-factor authentication.

The annual training of employees in fire safety regulations and the use of portable fire extinguishers, as well as evacuation drills, are an integral part of the branches' fire safety concept.

The implementation of technical and organizational safety measures is supported by topic-specific self-assessments, which are provided centrally.

The handling of data protection in the branch office has an exemplary function, as the numerous training participants can experience the various data protection measures and their interaction on site.

2.8 Monitoring and improvement

Standard references
ISO/IEC 27001/27701:
9.1/5.7 Monitoring, measurement, analysis and evaluation 9.2/5.7.2 Internal audit 10.1/5.8.2 Continual improvement 10.2/5.8.1 Nonconformity and corrective action

DATEV eG's integrated information security and data protection management system is subject to a continuous monitoring and improvement process.
The monitoring of IT systems about their secure and data protection-compliant design is given just as much priority as the information security and data protection organization itself.
Information security and data protection are continuously reviewed by the Privacy & Information Security and IT Audit departments as part of an annually defined audit program through the adopted internal audit measures. Any deviations or potential identified are incorporated into an improvement plan, which is regularly updated and monitored.

In addition to these multi-stage internal controls, DATEV eG also commissions independent certified assessors and certification bodies to conduct external audits of the information security and data protection management system.

2.9 General information security and data protection measures (technical and organizational measures)

The priority given to information security and data protection in connection with the size of DATEV eG enables comprehensive and effective information security and data protection measures. As part of its complex security system, DATEV eG has taken all important precautions in terms of construction, personnel, organization and technology. This ensures the high security for the IT infrastructure, process environments, data and the operations.

Many specifications and measures, ranging from the distribution, transport and storage to the disposal or dispatch of data and information, serve to ensure unauthorized access and proper handling.

DATEV eG provides its customers and interested parties with its general description of the technical and organizational measures for pursuing the data protection and information security objectives of confidential externality, availability including resilience and integrity at www.datev.de/datenschutz. Furthermore, DATEV eG publishes the white paper "Data Protection and Corporate Security at DATEV".

3. Overall result of the audit

The assessment showed that DATEV eG has implemented an appropriate, effective information security and data protection management system on a sustainable basis and meets the requirements of the ISO/IEC 27001 and ISO/IEC 27701 standards.

In particular, the assessment showed that, in addition to information security risks, the risks to the rights and freedoms of natural persons are sufficiently considered in the context of risk management and that DATEV eG has very diverse, comprehensive and complex information security and data protection measures in place that ensure a high level of precaution and secure data processing operations.

DATEV eG continuously reviews the technical and organizational measures in the form of regular internal checks and audits for their appropriateness and effectiveness and derives corrective and preventive measures from this, which contribute to the continuous improvement of the system as a whole.

Successful certification according to ISO 9001 Quality Management and ISO/IEC 20000-1 Service Management for the Digital & Print Solution Center and for the disposal of particularly sensitive data according to ISO 21964/DIN 66399-1 also results in high synergies for the effective verification and control of technical and organizational measures. This means that members and customers can refer to this information security and data protection certificate at www.datev.de/datenschutz to fulfil their audit obligation (Art. 28 and 32 GDPR).

The assessment of management systems involves a random inspection of the requirements of the set of rules regarding implementation and its documentation. Based on the audit and the evidence provided therein, it can be assumed that the management system fulfils the requirements at the time of the audit. However, CIS does not assume any guarantee or liability for a complete and permanent fulfilment of the set of rules during the term of the certificate, as this is the sole responsibility of the company.

Vienna, December 31st 2024

CIS - Certification & Information Security Services GmbH

Headquarters

1010 Vienna, Salztorgasse 2/3/7

Phone.: +43 1 532 98 90
Fax: +43 1 532 98 90 89
office@cis-cert.com
www.cis-cert.com