Data protection and information security at DATEV
DATEV – Where data protection is a top priority

At DATEV, data processing is built right into our name. As a service provider for the tax consulting and legal professions, we process sensitive personal data and business information. In this context, ensuring its availability and protecting it from unauthorised access is our top priority.

In this document, we would like to provide you with some insights into how data protection and information security are implemented at DATEV. Our aim is not only to provide information, but also help you comply with applicable data protection law.

This is because according to Article 28 of the EU’s General Data Protection Regulation (GDPR), principals who act as controllers pursuant to Article 4(7) of the GDPR can only work with processors who offer sufficient guarantees that processing is carried out in accordance with the legal requirements.
1 Sensitive data is in good hands with DATEV

As a cooperative for more than 40,000 tax consultants, lawyers and public accountants, DATEV is a leading expert when it comes to sensitive data. Our approximately 7,500 employees generated more than 970 million euros of turnover in 2017. This makes DATEV one of the largest service providers for software and data processing in Europe.

“As a professional IT service provider, data security and data protection are top priorities for DATEV and are of fundamental importance. DATEV stands for exceptional standards in this field. This particularly applies to personal data, but also to business data. All employees have a special responsibility in this context and observe the strict confidentiality of member and client data, in particular commissioned data. DATEV requires all business partners to fulfil their privacy and data security obligations and to maintain confidentiality.”

(Code of Business Conduct, Article 2: Data Protection and Data Security)
Working with sensitive data – the foundation of our business

We not only protect our members’ professional interests. Software and IT have been our core area of expertise for more than 50 years, and now around 12.5 million payslips are created every month using DATEV software. The majority of them are processed via the DATEV print, logistics and service centre. In addition, more than 700 million accounting documents were processed at the data centre.

We transfer accounting data to numerous institutions such as tax authorities, social security institutions and banks on a daily basis on behalf of member’s offices. In our line of business, data protection and information security are indispensable.

Compliance – a clear commitment to data protection

From the moment they sign their employment contract, our employees are aware of the fact that if you work with confidential personal and business data, you assume a great deal of responsibility. We set particularly high standards in this respect. Every employee must know and adhere to applicable legal regulations and our internal data protection policy. We ensure that this is the case through a mandatory, documented training process during hiring as well as through regular training seminars.

Our business partners must also adhere to their fiduciary duties with respect to data protection. Our Code of Business Conduct imposes far-reaching requirements on ourselves and our partners.
DATEV’s data protection organisation – awareness-raising, advise, monitor compliance

At DATEV, data protection is a holistic duty that the company fulfils at all levels. The data protection officer reports directly to the CEO. This individual works to ensure that DATEV always complies with the applicable legal provisions of the GDPR, Germany’s Federal Data Protection Act, as well as other data protection regulations, such as those governing electronic communication.

In this process, they are supported by their data protection and information security department, which advises them, among other things, when technical requirements have to be implemented throughout the company. In addition, the division officers for data protection in the business units and defined contacts at DATEV branch offices ensure that data protection is observed. They repeatedly draw our employees’ attention to their responsibility and monitor compliance with regulations. They provide assistance when it comes to implementing the stringent requirements governing the protection and security of the data we process on a day-to-day basis.
Questions relevant to data protection and information security are also discussed in internal bodies from various departments. They ensure that standardised solutions are implemented throughout the company.

Every employee on our data protection staff is specially trained and has the necessary expertise in the field of data protection law. Through advanced training and active involvement in specialist bodies and working groups, they are always up to date on the latest data protection issues. They are particularly active in the following organisations in Germany:

- Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. (AWV) (Working Group for Economic Management)
- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (bitkom);
  (Federal Association for Information Technology, Telecommunications and New Media)
- Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. (Professional Association of German Data Protection Officers)
- Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD);
  (Association for Data Protection and Data Security)

Awareness-raising, advising, monitoring – these are our strategies for implementing comprehensive data protection measures.

**DATEV as a controller – wide-ranging data protection measures**

DATEV’s data protection officer monitors where and how personal data is processed within the company. According to the provisions of the General Data Protection Regulation (Articles 38 and 39 GDPR), the departments must regularly inform the data protection officer of what data is being processed and for what purpose.

As the controller with respect to its websites (in accordance with Section 13 of the German Telemedia Act, TMA), the information pursuant to Articles 13 and 14 GDPR as well as DATEV’s data protection policy can be viewed online at www.datev.de/datenschutz.

**Legal persons’ data also protected**

DATEV does not only protect personal data. Our internal company guidelines stipulate that DATEV’s information security measures also apply to data relating to legal persons – such as companies, institutions or associations.
Classification of data protection requirements

The level of protection data requires depends on the parameters of confidentiality, availability and integrity. DATEV takes into account the level of resilience required in accordance with the GDPR when assessing availability objectives. DATEV assesses the appropriate level of protection on the basis of the risk to the rights and freedoms of data subjects, among other factors. The name and address of a company, for example, which can be found on the Internet or in the telephone directory, are by no means as sensitive as payslips. Classifying the protection requirements for specific types of data determines how such data is processed and what measures of data protection are required.

Competent supervisory authority

The Data Protection Authority of Bavaria for the Private Sector (www.lda.bayern.de) in Ansbach is the supervisory authority responsible for data protection at DATEV. It monitors compliance with data protection provisions and helps to ensure that our protection measures meet the high standards imposed on us by legislators and ourselves.

Customer service – products and services for data protection

The law also stipulates that our customers must take great care when handling sensitive data. With our experience and expertise, we can help you meet your obligations when dealing with customer and client data.
To this end, we offer various products and services for data protection and IT security: DATEVnet is used to ensure that Internet access and e-mail traffic are secure. This creates the conditions necessary to encrypt your e-mails with DATEV E-Mail Encryption. DATEVnet also ensures that access to your e-mails, contacts and calendar on your mobile devices is secure. And the DATEV VIWAS antivirus program is ideal for protecting local member’s office PCs.

Customers who do not protect their Internet access with DATEVnet and DATEV E-Mail Encryption can still encrypt, decrypt and electronically sign their e-mails using the certificate-based DATEV SmartCard or DATEV miDentity.

DATEV-Consulting advises and trains you on all aspects of data protection and IT security, carries out risk assessments and audits and, if you wish, can also provide you with an external data protection officer.
Data processing – DATEV as a processor

Data processing on behalf of clients is a matter of trust. Article 28 of the GDPR provides the legal framework for processing personal data on behalf of a controller. Non-compliance by the principal and the contractor (processor) is punishable by a fine.

Legal basis of processing on behalf of a client
If a company transfers personal data to a service provider such as DATEV for processing, it remains responsible for compliance with data protection provisions as the principal (i.e. the controller as defined in Article 4(7) of the GDPR). As a result, the principal must carefully select the processor and explicitly designate them by written mandate or in electronic format. Article 28(3) of the GDPR DS-GVO sets forth what this agreement must stipulate.

When selecting the service provider, the principal must, in particular, verify the suitability of the technical and organizational protection measures taken to protect the ceded data. In particular, processing must be carried out in accordance with the requirements of the GDPR and ensure that the rights of data subjects are protected. In addition, the principal is advised to verify compliance with these measures and document the result before the start of data processing and regularly thereafter. To this end, the commissioned data processor must provide the controller with all of the information necessary to demonstrate compliance with the obligations set forth in Article 28 of the GDPR.

DATEV wants to help its customers obtain detailed information as to whether their data is in good hands with DATEV. This is why independent institutions regularly audit the effectiveness of DATEV’s data protection and information security measures and its information security management system in accordance with ISO/IEC 27001.

On the basis of the certificates and seals of approval – which are also enclosed in section 3 of this brochure – the principal can fulfill its auditing obligations without having to carry out an onsite inspection at DATEV (the GDPR does not mandate such an inspection). Instead, Article 28(5) of the GDPR stipulates that an approved certification procedure may also serve as evidence of sufficient guarantees. Until GDPR certification is offered that meets the requirements of Article 42 of the GDPR in conjunction with Section 39 of Germany’s Federal Data Protection Act, DATEV will continue to rely on a seal of approval issued by DQS BIT GmbH which confirms that DATEV has effectively implemented data protection in a management system via technical and organisational protection measures in accordance with the requirements of the GDPR.

Contractual bases
As a processor, DATEV may only process data ceded to it within the scope of the principal’s instructions and must take appropriate technical protection measures to protect the data from destruction, loss, alteration, or unauthorised disclosure or access. The obligations that DATEV and its principals must meet when it comes to data protection, in particular the instruction framework (see Article 28(3)(a) of the GDPR), are set out in the following documents applicable to the parties’ contractual agreement:

- DATEV eG Terms and Conditions
- Agreement on Commissioned Data Processing
- Service descriptions of applications and services
- Individual assignments
The Agreement on Commissioned Data Processing is the primary contractual document. It specifies the data protection obligations that DATEV and its principals must fulfil. The agreement applies to all assignments in which our employees or other processors may come into contact with personal data from the principal.

The individuals authorised to process such personal data are bound to confidentiality or are subject to an appropriate legal secrecy obligation.

It is only possible to extend the instruction framework provided beyond the scope described here by mutually agreeing to modify the agreement. In the Agreement on Commissioned Data Processing, DATEV and the principal expressly agree to comply with applicable data protection laws.
Data processing at the DATEV data centre
The DATEV data centre guarantees the privacy of your and your clients’ data. All of the data transferred through the DATEV data centre is protected by encrypting technologies to ensure maximum data security.

Use of commissioned data processors
DATEV is authorised to have certain services provided by third parties (i.e. subcontractors) if this is deemed necessary for the completion of an assignment (DATEV Terms and Conditions, Section 7.1).

Under our Agreement on Commissioned Data Processing, the client authorises DATEV to avail itself of commissioned data processing as defined in Article 28(2) of the GDPR. The commissioned data processors currently used by DATEV are listed in the info database document “Overview of commissioned data processors” (doc. no. 1000192), available here: www.datev.de/info-db/1000192.

We notify our customers when DATEV intends to accept or use additional commissioned data processors.

If DATEV commissions other data processors, DATEV ensures that its data protection obligations under the Agreement on Commissioned Data Processing are imposed on the other processor.

The provision of services by DATEV also requires DATEV to ensure that operations run smoothly at all times. As a result, in the event of maintenance or malfunctions, it may be necessary to engage service providers who must be granted permission to analyse error logs or similar system states. Under certain circumstances, it may not be possible to completely rule out the possibility that these service providers may access personal data when maintaining and troubleshooting DATEV’s systems. In these individual cases, personal data can only be viewed by these service providers – including in a third country, if necessary – in compliance with the mandatory statutory provisions.

Regular service processes with suppliers do not foresee commissioned data and, in particular, data protected by professional law being transferred outside the EU.

Secrecy obligation
DATEV, as a service provider, is involved in the professional activities of customers who are subject to an obligation of professional secrecy. The third-party secrets revealed to DATEV in the process are kept confidential by the cooperative in accordance with Section 203 of the German Criminal Code and any other applicable professional regulations. Section 16 of DATEV eG’s General Terms and Conditions contains more detailed provisions regarding this special secrecy obligation. We enter into appropriate confidentiality agreements with our members and customers.

DATEV binds all of its employees to confidentiality in a proper manner; this also applies to subcontractors to the extent that they might gain knowledge of third-party secrets in the course of their activities.
Depending on the area of responsibility, further confidentiality obligations may also apply. This applies to the privacy of communications (under Section 88 of the German Telecommunications Act) and postal secrecy (under Section 39 of the Postal Act), among others. This means that the content and circumstances of our customers’ communication processes remain confidential. Furthermore, we only grant user rights for remote access to DATEV or customer networks with personal data to employees who have agreed to implement appropriate technical and organisational measures.

Employees tasked with administrative duties are also particularly bound to observe the associated confidentiality requirements. We ensure that our employees are familiar with the applicable legal safeguards through the use of training seminars and informational events. We are committed to continuously reminding our employees how important this discretion is, which is why they are required to regularly participate in online training sessions with subsequent tests and seminars on the subject.

**Holistic information security concepts**

At DATEV, information security is implemented systematically. Because regulations, technology and organisational structures can change, we constantly strive to adapt and improve our information security measures.

We operate an ISO/IEC 27001-certified information security management system – certification covers DATEV’s data centre as well as DATEV’s print, logistics and service centre, which are located in the greater Nuremberg area.

In addition, we enhance our protection measures in a continuous improvement process in accordance with legal, technical and organisational requirements.

Our information security concept encompasses structural, human resource-related, organisational and technical protection measures to guarantee the security of the properties and data they contain. The technical and organisational protection measures are intended to prevent unauthorised access to data and to ensure data and data media are handled in a due and proper manner.

We review the effectiveness of these measures through independent internal and external audits as well as through unannounced emergency exercises with alternating focal points. The results of these reviews form the basis for targeted improvement measures.
Exchange of data with the DATEV data centre

DATEV has developed various solutions to guarantee data confidentiality and integrity as well as its unique identification and authentication. These include the DATEV SmartCard, DATEV miDentity and DATEV SmartLogin. With the help of these security mechanisms, users can access their data at the DATEV data centre and use associated online services.

Outsourcing data processing

We offer the DATEVasp and DATEV-SmartIT products for customers who want to outsource their IT infrastructure to the cloud. In this context, the customer’s software and data are stored at the DATEV data centre and can be accessed via remote desktop services (formerly also known as terminal servers). Secure communications with the DATEV data centre are guaranteed through the use of suitable, state-of-the-art encryption procedures.

The support and service network for DATEVasp and DATEV-SmartIT is operated separately from DATEV’s internal office communication to guarantee data security and confidentiality. DATEV uses a clearly defined user rights policy and assigns service staff to a separate role group whose access rights and settings are subject to special supervision.
Technical and organisational protection measures

DATEV has processed data on behalf of professional groups that are subject to professional secrecy since its founding in 1966. At DATEV, information security measures are not just cost factors, but the cornerstone of its business. All of DATEV’s services are designed to guarantee maximum data protection and information security with a focus on efficacy and cost-effectiveness.

Appropriate technical and organisational protection measures are implemented at DATEV in such a way that processing is carried out in accordance with the requirements of the GDPR and that the rights and freedoms of the data subject are protected. Within its sphere of responsibility, DATEV takes all the necessary measures pursuant to Article 32 of the GDPR. The following provides an overview of our technical and organisational protection measures. The information contained in this overview largely corresponds to the content of the agreements DATEV has included in the information database in document number 1000562 www.datev.de/inodb/1000562) since 2018. For security reasons, we cannot describe the security measures in detail here.
The security measures are regularly audited as part of data protection and ISO/IEC 27001 audits. DATEV reserves the right to change the technical and organisational protection measures it has implemented, provided they do not fall below the level of protection stipulated in the GDPR.

Measures to pseudonymise personal data
As a commissioned data processor, DATEV implements measures resulting from the service descriptions of its products or services or which are taken by the controller within the scope of the assignment. DATEV does not take any further measures to pseudonymise personal data beyond this.

Measures to encrypt personal data
DATEV defines rules governing the selection of suitable cryptographic processes and products as well as the organisation of their use that correspond to the state of the art. DATEV implements key management measures and regular reviews of these procedures, e.g., to detect weaknesses in encryption procedures or products.

Measures to guarantee integrity and confidentiality
DATEV implements suitable and state-of-the art technical and organisational protection measures to reduce risks from unauthorised disclosure or unauthorised access to personal data as well as unintentional or unauthorised modification of the data processed on behalf of the controller.

This particularly include the following measures:
- Monitoring, imposing obligations on, raising the awareness of and training employees
- Protection against unauthorised physical access (access control), including mobile device security
- Protection against unauthorised system access (user rights policy and authentication)
- Operational reliability measures (IT fault management, event monitoring)
- Communication security measures (network security management, use of encryption procedures)
- Secure, irreversible deletion of data or destruction of data storage devices

Measures to guarantee availability and resilience
DATEV reduces the risks that could arise from the destruction, loss, alteration, unauthorised disclosure, or unauthorised access to processed data by taking appropriate measures against system overloads or crashes. To this end, when it comes to data processing at the DATEV data centre, DATEV ensures a level of system stability sufficient for the large number of reliable and timely data processing operations.

This particularly include the following measures:
- Measures to ensure availability (structural measures, fire protection, human resource-related measures, emergency power, air conditioning)
- Protection against external influences (prevention of attacks through the use of firewalls, virus scanners, contingency plan)
Restoring availability and access after a physical or technical incident

DATEV implements the necessary technical protection measures to reduce the risk of physical, material or immaterial damage. Safeguards are in place to minimise the occurrence of a physical or technical incident.

This particularly include the following measures:

- IT emergency manual including restart planning
- System load monitoring
- Redundant infrastructure design

Procedures for the regular review of implemented measures

To guarantee that processing is secure, DATEV regularly reviews, appraises and evaluates the implemented measures.

This particularly include the following measures:

- Information security strategy and certification
- Continuous enhancement of protection measures in accordance with legal, technical and organisational requirements
- Management of information security incidents
- Maintaining information security in the event of unplanned system statuses
- Conducting internal or external security audits

Other measures

DATEV ensures that its software applications process personal data in accordance with the GDPR.

Within the scope of providing its products and services (service descriptions), DATEV ensures that data is only processed for the intended purpose (purpose limitation). When processing data on behalf of controllers, it implements appropriate technical and organisational protection measures to protect the rights of the data subjects.

Furthermore, DATEV also implements the following measures:

- Measures to uphold the principle of purpose limitation with respect to personal data
- Privacy by design and by default and measures to protect the rights of data subjects
- Measures to ensure transparency for data subjects, controllers and supervisory authorities
Certification, seal of quality and documentation obligations

When it comes to processing personal data, the principal remains responsible for compliance with appropriate technical and organisational protection measures, including by the processor. Controllers are not required to conduct on-site inspections to ensure compliance with the agreed upon data protection measures, however. Certification by independent experts can also be used for this purpose.

Product certifications
DATEV’s products and services are audited at regular intervals by an auditing company. This is how we ensure that processing data with DATEV applications makes bookkeeping, the preparation of annual financial statements and transaction processing in compliance with the principles of proper accounting possible.

An overview of the available audit reports and certifications can be found in the info database at www.datev.de/info-db/0908286.

Certification according to ISO/IEC 27001
The international ISO/IEC 27001 standard defines the requirements for the installation, implementation, operation, monitoring, maintenance and continuous improvement of a documented information security management system. We have had our information security management system audited in accordance with the ISO/IEC 27001 standard. On December 8, 2016, the German Association for the Certification of Management Systems (DQS GmbH) once again confirmed that DATEV has implemented and operates an ISO/IEC 27001-compliant system.

Certification was issued for the DATEV data centre and the services provided by the DATEV print, logistics and service centre including digital scanning. A copy of it can be found on page 21.

Disposal of data storage devices according to DIN SPEC 66399
We dispose of test prints and misprints from the production department using our own technical equipment which meets the requirements of protection class 3 and security level 4 of DIN 66399-1 (very high protection requirements, particularly sensitive data). A copy of the certificate issued on November 21, 2017 can be found on page 22.

Data protection seal
DATEV had its data protection management system reviewed by the renowned company DQSBIT GmbH on the basis of the procedure for auditing information security management systems in accordance with ISO/IEC 27001. The appraisal was based on the GDPR as of April 27, 2016, with corrections as of March 13, 2017. In order to ensure a sufficient level of evaluation, the review was carried out taking into account the requirements of ISO/IEC 29151:2017 “Guidelines for Protecting Personal Data.”

The assessment demonstrated that DATEV has effectively implemented technical and organisational protection measures within the scope of a management system to protect privacy in accordance with the requirements of the GDPR, whereby the principles governing the processing of personal data pursuant to Article 5(2) in conjunction with Article 5(1) of the GDPR apply. Within the framework of risk management, DATEV sufficiently respects the rights and freedoms of natural persons.

DQSBIT GmbH subsequently awarded DATEV a data protection seal that is valid from May 25, 2018 to May 24, 2021. It applies to DATEV’s headquarters in Nuremberg, including the DATEV I-IV sites, and the DATEV branch offices listed in the appendix to the seal.
This is to certify that

DATEV eG
Paumgartnerstraße 6-14
90429 Nürnberg
Germany

has implemented and maintains an
Information Security Management System.

Scope:
DATEV computer center
DATEV print-, logistic- and service center
Statement of applicability: V4.0

Through an audit, documented in a report, it was verified that the management system fulfills the requirements of the following standard:

ISO / IEC 27001 : 2013

Certificate registration no. 337181 ISMS13
Valid from 2016-12-08
Valid until 2019-12-07
Date of certification 2016-12-08

DQS GmbH

Frank Graichen
Managing Director

Attestations

ISO/IEC 27001
DIN SPEC 66399
Data protection audit
Data protection brief report
This is to certify that

DATEV eG
Paumgartnerstraße 6-14
90429 Nürnberg
Germany

has introduced and applies a Management System in accordance with the set of regulations indicated below.

Scope:
Disposal of paper in the security area of the Printing, Logistics and Service Centre.

Verification was provided by means of an audit, documented in a report, that the regulations of the specification below are met. Spot checks carried out within the scope of the audit demonstrated that the process is implemented in practical applications accordingly.

DIN SPEC 66399
Office machines and information technology – destruction of data carriers
Part 3: Process for data carrier destruction, February 2013
in accordance with protection class 3 and security level 4

Certificate registration no. 337181 KB
Valid from 2017-11-21
Valid until 2020-11-20
Date of certification 2017-11-21

DQS BIT GmbH

Andre Dubsky
Managing Director

Administrative Office: DQS BIT GmbH, Gartenstrasse 13, 86325 Bad Wörishofen
This is to certify that

DATEV eG
Paumgartenstraße 6-14
90429 Nürnberg
Deutschland
organisation
with the sites listed in the annex

for the scope
main site in Nürnberg, including the areas DATEV I-IV
as well as the DATEV branch offices listed in the annex

Data Protection in accordance with the requirements of the
EU General Data Protection Regulation (GDPR)
as of April 27, 2018
with addendum from March 13, 2017
to be used from May 25, 2018

regarding the technical and organisational measures in a management system
has effectively implemented the principles for processing personal data
in accordance with Article 5 Section 2 in combination with Section 1 GDPR find application.
As part of the risk management, the rights and freedoms of natural persons are sufficiently considered.

A voluntary data protection audit, documented in a report, provided evidence
that the management system satisfies the requirements of the GDPR.

The company is entitled to use the following data protection Mark of Quality in accordance with
the established rules.

Reg. No. 337181 GP
Audit date 2018-04-18
Valid from: 2018-05-25
Valid until: 2021-05-24

DQS BIT GmbH

Andre Dubsky
Managing Director
Annex to
Reg. No. 337181 GP

DATEV eG
Pauwgartnerstraße 6-14
90429 Nürnberg

This annex (dated: 2018-05-25) is valid only in combination with the Mark of Quality referenced above.

Certificate: Data protection audit (annex)
Attestations

ISO/IEC 27001
DIN SPEC 66399
Data protection audit
Data protection brief report

Detailed audit results (brief report)

Data protection audit general data protection regulation (gdpr)
- DATEV eG
- DATEV branch offices in germany

1 Explanatory Notes to the Audit
1.1 Starting Point

Since its founding on February 14, 1966, the Nürnberg-based DATEV eG has evolved into the leading software and IT services provider for tax consultants, public accountants and lawyers, as well as their clients. Its range of services encompasses accounting, business consulting, taxes, office organisation, Enterprise Resource Planning (ERP), IT services as well as training and consulting.

Based on a change of the corporate statutes from February 18, 2005, DATEV may also work directly for a member’s clients, if the member so desires. Additionally, specific services are also available for non-members (IT sourcing).

According to its 2017 business report, on December 31, 2017, DATEV had 7,292 employees, as well as 40,555 members for whom, inter alia, more than 12.5 million payroll accounts are processed. Additionally, more than 700 million booking vouchers were processed at the computer center.

Considering the type and volume of the data processed, data protection as well as the security of both the data and the IT systems processing them, as well as an appropriate design of the programs, trainings and consulting services are of existential importance to the company; this is also the estimation of its members.

As the responsibility for commissioned data processing rests with the controller, he is obliged to ensure that the processor has implemented technical and organisational measures in such a manner that data is processed in accordance with the requirements of the GDPR (Art. 28 GDPR). The requirements for the contractual agreement on commissioned data processing (Art. 28 (3) GDPR) include, inter alia, the binding nature of the contract for the processor, that the persons authorised to process the personal data have committed themselves to confidentiality, as well as making available to the controller all information necessary to demonstrate compliance. This also includes the necessary technical and organisational measures, the obligation of the processor (e.g. DATEV) to exercise control, as well as the supervisory rights of the controller (e.g. a member) as well as regulations regarding the return or deletion of data stored by the processor.

For this purpose, DATEV provides its members, in addition to the Agreement on Commissioned Data Processing, with a description of the technical and organisational measures according to Art. 32 (1) GDPR for processors (Art. 30 (2) GDPR) according to the general description in the Information Database (Doc.-Nr. 1000562) – online as well as the information document „Data Protection and Information Security at DATEV“ (available via DATEV Shop Art.-Nr. 11992). The information document provides insight into measures implemented, but does not, by itself, allow an evaluation whether those measures are effective or compliant with the law.

Hence, DATEV is facing the task of enabling members to evaluate the level of data protection without requiring individual examination.
1.2 Purpose of the Audit

In the past, it was possible to achieve this aim to a large extent by making reference to the regular checks conducted by the supervisory authority for data protection. However, in the course of the amendment to the Federal Data Protection Act (BDSG) in 2001, the periodic check carried out on the Data Processing Center of DATEV by the supervisory authority has been dispensed with.

In order to replace this inspection, DATEV availed itself in 2006 for the first time of the possibility provided for by BDSG to commission independent and licensed experts to inspect and audit the data protection concept on a voluntary basis (statutory data protection audit pursuant to § 9a BDSG a.F.).

By undergoing a new and voluntary data protection audit under consideration of the requirements of the GDPR, DATEV wants to make it uniform to all its members and other customers in a standardized and comprehensive manner that data protection continues to be implemented appropriately and effectively through the use of technical and organisational measures. In addition, DATEV wishes to demonstrate that the principles for processing personal data according to Art. 5 (2) in combination with (1) GDPR are being applied and that the rights and freedoms of natural persons have been adequately considered as part of risk management. By way of verification, DATEV makes the applicable Mark of Quality available to its members, further customers and the public, which can, if necessary, be substantiated by the relevant audit report.

In particular, the quality mark confirms that the measures described in the data processing agreement, as well as the technical and organisational measures according to Art. 32 (1) GDPR described in the Information Database (Doc.-Nr. 1000562) and in the information document "Data Protection and Information Security at DATEV", are appropriate and effective. In this manner, DATEV enables its members and clients to fulfil the required supervisory duties as well as potential documentation requirements with regards to external supervisory or governing bodies simply and effectively.

As a result, DATEV enables its members and customers to meet the inspection obligation easily and effectively, and to satisfy any documentation obligations vis-à-vis external agencies and supervisory authorities.

1.3 Scope of the audit

The certificate based on the BDSG (most recently changed on October 8, 2015) ceases to be valid once the GDPR comes into effect on May 25, 2018.

As the criteria specific to data protection and the additional sector-specific accreditation requirements have not yet been agreed between the governing bodies for data protection of the Federal and federal states governments, corresponding certification processes by an accredited conformity assessment body cannot be provided before May 25, 2018.

The choice of an appropriate audit process is thus of decisive importance for the significance of any attestation regarding the data protection management system. Both the reputation of the provider and the underlying processes are essential.

Hence, DATEV has entrusted DQS BIT GmbH with conducting the voluntary data protection audit. DQS Group is a market leader in the field of certification for quality and other management systems, and accredited for numerous standards according to ISO/IEC 17021.1)

1) Overview at https://www.dqs.de/de/ueber-uns/dqs-gmbh/akkreditierungen/ (http://www.dakks.de)
As accreditation for the field of data protection is not yet possible, DQS BIT GmbH carried out the audit based on the process for auditing information security systems according to ISO/IEC 27001, taking into account the requirements of the ISO/IEC 29151:2017 guideline for the protection of personal data, in order to ensure an adequate standard of assessment.

Additionally, DATEV’s information security management system (ISMS) for the computer center was certified according to ISO 27001 in 2010. The certificate issued was renewed in December 2016. Furthermore, the print-, logistic- and service center was successfully certified according to ISO 20000-1 (Service Management) and ISO 9001 (Quality Management) in 2017. The certification of the waste disposal process according to DIN SPEC 66399 was successfully completed in November 2017. The certificate confirms the correct disposal of test prints and misprints from the production department according to protection class 3 and security level 4 of DIN 66399 (very high need for protection, particularly sensitive data).
These certifications, carried out by DQS BIT GmbH, create considerable synergies, particularly for an assessment of the data protection measures required by Art. 32 GDPR.

Within the framework of the voluntary data protection audit, DATEV’s entire data protection management system was assessed with respect to effective design and implementation. This was intended to uncover and use extant optimisation potential.

The initial certification was carried out in autumn of 2006 according to § 9a BDSG (old version) and confirmed in subsequent years by supporting assessments and re-certifications. The most recent supporting assessment was completed in autumn of 2017.

According to the certification regulations, certification needs to be repeated to its full extent after three years. The re-certification cycle according to § 9a BDSG (old version) in the fall of 2018 was interrupted by the new legislation, and the audit brought forward accordingly.

The data protection audit for assessing the implementation of the requirements of the GDPR in April 2018 starts the fifth cycle of assessing the implementation of data protection and the confirmation of effective implementation of the contractually agreed technical and organisational measures for the protection of personal data processed on behalf of the controller, the results of which are reported herein.

The audit of the branch offices is conducted using the so-called matrix procedure, involving a suitable sample is selected from branch offices which have not yet been audited.

1.4 Scope of application of the audit
The data protection audit covers all DATEV branch offices in Germany, i.e.

- The central branches in Nürnberg and
- The 24 DATEV branch offices existing at the time of the audit, whereby the former DATEV information center Nürnberg was merged into the headquarters and is thus no longer a branch office in its own right.

The data protection mark of quality is valid for three years, when maintained by annual supporting assessments.

1.5 Subject of the audit
Core subjects were the following topics of the General Data Protection Regulation:

- Scope of protection
- Data protection management
  - Context of the organisation especially requirements and expectations of interested parties.
  - Data protection and information security strategy
  - Requirements for data protection (e.g. guidelines, policies, concepts, etc.)
  - Company data protection officer (DPO) and other data protection bodies
  - Change management for the implementation of the requirements of the GDPR by Project DaGobert
- Data protection processes with special consideration of compliance with data protection principles
  - Data processing in compliance with data protection principles
  - Safeguarding the rights of data subjects
  - Handling data protection breaches
  - Continuous supervision, adaptation and improvement
- Agreement on commissioned data processing
- Effective and appropriate implementation of the agreed-upon technical and organizational measures
1.6 Implementation and criteria of the audit
The audit was carried out between April 18, 2018 and April 19, 2018 on the premises of the DATEV headquarter in Nürnberg. As part of the audit, DATEV presented the relevant organisational regulations, processes and procedures, which were audited using the appropriate premises and evidence.

The audit was based on the following:
- EU General Data Protection Regulation from April 27, 2016 with addendum from March 13, 2017
- Internal DATEV requirements and regulations on data protection and information security

1.7 Use of the results of the audit
With this new data protection audit, DATEV has yet again delivered an effective control evidence for its members and other customers from an independent auditor.

The data protection mark of quality is published in its open-access customer database on the DQS website (https://www.mydqs.com/kunden/kundendatenbank.html).

The data protection mark of quality from DQS BIT GmbH in combination with one’s own evaluation of the audit report can be used to document the legally required regular supervision.

These testimonials may also be forwarded to clients who wish to carry out their own control duties. For this purpose, the following documents are provided on the internet at www.datev.de/datenschutz.

1. Data protection mark of quality
2. Abridged version of the present report, i.e. without Section 3 “Annex: Detailed results of the Audit”. The full version is available on request from DATEV’s Data Protection Officer.
3. Proprietary DATEV supplements, particularly the technical and organisational measures according to Art. 32 (1) GDPR for processors (Art. 30 (2) lit. d) GDPR) in accordance with the General Description in the Information Database (Doc. Nr. 1000562) online as well as the information document “Data Protection and Information Security at DATEV” (in revised edition available at the DATEV-Shop Art.-Nr. 11992).
These testimonials enable controllers, as before, to confirm that DATEV’s technical and organisational measures are compliant.

2 Overall result of the audit

The audit has confirmed that DATEV has effectively implemented data protection in compliance with requirements of the General Data Protection Regulations through technical and organisational measures by using a management system. The principles for processing personal data according to Art. 5 (2) in combination with (1) GDPR are being applied.

In particular, the audit has confirmed that within the framework of risk management, the rights and freedoms of natural persons are adequately considered and that DATEV has implemented manifold, comprehensive and complex data protection and information security measures, ensuring a high degree of prevention and a secure processing of data.

DATEV is continuously evaluating the technical and organisational measures using internal monitoring with respect to their appropriateness and effectiveness and documents the results in a checklist or in the corresponding data protection monitoring report.

On this basis, the effective and appropriate fulfilment of the technical and organisational measures (TOM) referenced in the agreement on commissioned data processing can be confirmed.

Thus, members and customers may refer to the present data protection mark of quality to fulfil their supervision requirements (Art. 28 and 32 GDPR).

Beyond that, a high degree of synergy for the effective verification and monitoring of the technical and organisational measures results from the successful certification of the Information Security Management System (ISMS) according to ISO/IEC 27001 for the computer center and according to ISO 20000-1/ISO 9001 for the field of the print-, logistic- and service center as well as for the disposal of particularly sensitive data according to DIN 66399-1.

An audit of a management system is a sample testing method of the requirements regarding the documentation and its implementation. Based on the audit and the evidence provided during its execution, it is to be concluded that the management system fulfils the requirements at the time of the audit. DQS BIT GmbH cannot assume liability or guarantee for complete and permanent compliance with the standard throughout the validity of the mark of quality, this being exclusively the responsibility of the organisation.

Frankfurt/Main,
May 8, 2018
DQS BIT GmbH
Take action now!
Data protection and data security are essential business foundations – and therefore a management issue. Simply contact us with any queries. We will help you to find the best solutions for you.
Collaboration as partners

If you have any questions related to data protection, please contact DATEV’s data protection officer, Dr Jörg Spilker. You can reach him at this e-mail address: datenschutz@datev.de.