Detailed Audit Results

DATA PROTECTION AUDIT
GENERAL DATA PROTECTION REGULATION (GDPR)

DATEV EG
DATEV BRANCH OFFICES IN GERMANY

June 8, 2018
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 standardised 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.\(^{(1)}\)

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) und 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
- Agreement on commissioned data processing
- Effective and appropriate implementation of the agreed-upon technical and organisational measures
- General data security measures
- Records of processing activities Art. 30 (1) GDPR
- Records of processing activities Art. 30 (2) GDPR
- Lawfulness of handling personal data
- Compliance with principles to processing of personal data Art. 5 (1) GDPR
- Compliance with accountability requirements Art. 5 (2) GDPR
- Evaluation and treatment for data protection risks and data protection impact assessment
- Risk response plan based on ISO 29151
- Commitment to confidentiality of data and to professional secrecy
- Training and sensitisation of employees
- Rights of the data subject
- Data protection in special areas
  - General control of access
  - Product development
  - Production
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