Data Protection Management System: Certification of Compliance Kit 2.0

On August 6, 2019, IITR Datenschutz GmbH received confirmation that Compliance Kit 2.0 comprehensively and correctly satisfies the regulations of the GDPR. This confirmation was issued by the state-certified and sworn civil engineers Dr. Peter Gelber (Dipl.-Ing.) and Wolfgang Fiala (Dipl.-Ing.) and is equivalent to an official examination.

According to an Austrian provision, civil engineers (source: https://www.ziviltechniker.at/) are authorized as "persons of public trust" to check conformity with legal requirements and to issue certification on this matter.

Compliance Kit 2.0 (source https://www.iitr.us/products-services/compliance-kit.html) was submitted for examination. The review is documented in a report (source: https://www.iitr-cert.com/), as well as the corresponding certificate (source: https://www.iitr-cert.com/). Compliance Kit 2.0 has therefore received its official recognition.

Compliance Kit 2.0 is designed as a data protection management system.

Certification on the basis of a data protection management system

In the literature, it is often pointed out that a data protection management system is the suitable instrument in order to fulfil the requirements of the GDPR and here in particular the requirements of accountability (see "Handreichung zum Stand der Technik" [Assistance on State of the Art] by TeleTrust, p. 71, quote at the end and "Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO" [Data Protection (Compliance) Management Systems: Verification and Accountability Duties Pursuant to the GDPR] by Alexander Jung in "ZD," 2018, p. 208, quote at the end).

European Data Protection Board

The European Data Protection Board has decided that Art. 42 GDPR does not provide for certification of management systems according to its interpretation. As a result, the German certification authority DAkkS has now published guidelines which deal exclusively with the certification of products and services (see "Die Zertifizierung nach der GDPR: Innovatives, aber hochkomplexes Instrument" [Certification under the GDPR: Innovative but Highly Complex Instrument"], in "DuD," 8/2019, Dr. Natalie Maier, LL.M. and Tamer Bile, LL.M., Scientific Center for Information Technology Design at the University of Kassel, https://link.springer.com/article/10.1007/s11623-019-1147-x).

The article by Oliver Schonschek provides a further overview of the facts (source: https://www.computerwoche.de/a/welche-datenschutz-zertifikate-passen-zu-dsgvo-und-gdpr,3545410).

Compliance Kit 2.0 as basis

We have decided to offer our clients a data protection management system and the possibility of our own certification. This certification will be carried out by IITR Cert GmbH, established as an independent examination body for this purpose (source: https://www.iitr-cert.com/).

Due to the certification by civil engineers (as an authorized body), Compliance Kit 2.0 provides companies with a qualified tool to establish compliance with the GDPR and to obtain confirmation.

Certification bodies

According to an EU norm (Regulation (EC) No. 765/2008, Article 4 (1), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:de:PDF), the national certification bodies were solely responsible for certifications within their respective countries until the GDPR came into force (in Germany this is DAkKS). The GDPR has created a new situation by claiming certain processes in the area of certifications for itself. Since then, the data protection authorities of a country have been additionally involved in the sovereign certification process for the area of data protection. Germany has data protection authorities in its states which coordinate their activities internally. Germany is represented at the EU level in the European Data Protection Board by the Federal Commissioner for Data Protection and Freedom of Information.

Alternative option for large companies

Currently, the assessment of a company is only possible indirectly via a certification of its own IT security according to ISO 27001/27002 (“Information Security Management”), on which a corresponding certification according to ISO 27701 (source: https://www.iso.org/standard/71670.html) can be added in the future (whereby this also ultimately does not represent “certification” in the sense of Article 42 GDPR).

This procedure can only be carried out by large companies or by units whose business activities are extremely data sensitive and for this reason have the considerable resources to have them checked in accordance with these standards.

For the majority of companies, this approach is simply out of the question for many reasons. First of all, it is much too expensive at an additional cost of tens of thousands of euros. Furthermore, sufficient numbers of experts who could carry out such certifications are not even available.

Accountability and data protection management system

There should be no doubt about the need to use a data protection management system based on the requirements of the GDPR (accountability). This is also the view of management consultants KPMG (source: https://klardenker.kpmg.de/datenschutz-managementsystem-pruefung-bringt-sicherheit/). In the event that a company wants to employ software-driven strategies for coping with data protection requirements – which cannot be avoided above a certain company size – a data protection management system will become necessary at the same time. After all, management is liable for the actual implementation and will not want to rely on whether software has been correctly installed and operated.

Scope of services of Compliance Kit 2.0

The Compliance Kit 2.0 is based on a privacy manual reflecting the ISO High Level Structure. Compliance Kit 2.0 resembles, for example, a BS 10012 of the BSI British Standard Institution. The similarity is not surprising, as both are based on the same GDPR, but BS 10012 also includes some British special features.

Beyond that a data protection management system must make it possible to satisfy the demands specified in the GDPR regarding the documentation of descriptions as well as the storage of contracts to be entered into and must be able to archive these conceptions in a traceable manner, i.e., one that is version-controlled. An eLearning platform is integrated in order to be able to meet the existing obligation of educating all employees about data protection by the company's data protection officer. Completed training courses must be verifiable and are documented by the management system.

Advantages of certification

Particularly in the area of data protection, the prerequisites for cross-company cooperation and contract awarding have been subjected to rigid conditions when exchanging personal data. In some cases, a de facto reversal of the burden of proof has been introduced; liability for the correct conduct of a contractor can be traced back to the management of the client.

Who wouldn't want to have recourse to a statement and evaluation of the data protection structures of a potential contractor that was as accurate as possible?

For a potential contractor, on the other hand, it could be advantageous to present a certificate to the future client in order to be able to prove their own efforts towards data protection law-compliant structures.

Certification also has an internal effect: the certainty of being properly set up in this area. Standards are being followed that correspond to those which the business partner also adheres to.

Customers like to be supported by well-structured companies. There is hardly a customer who would prefer a company because it does not have a certificate.

The same applies to their own employees. Certification in data protection has both a protective and a signaling effect both internally and externally.

Position of the EU Commission

Official certifications for management systems are currently not available, as described. Only products and services are certified. On July 24, 2019, the EU Commission writes: (source: https://ec.europa.eu/commission/sites/beta-political/files/communication_from_the_commission_to_the_european_parliament_and_the_council.pdf):

> "Businesses are adapting their practices (…)
>
> Finally, certification can also be a useful instrument to demonstrate compliance with specific requirements of the Regulation. It can increase legal certainty for businesses and promote the Regulation globally. The certification and accreditation guidelines recently adopted by the European Data Protection Board will enable the development of certification schemes in the EU. The Commission will be monitoring these developments and, if appropriate, will make use of the empowerment provided under the Regulation to frame the requirements for certification. The Commission may also issue a standardisation request to EU standardisation bodies on elements relevant for the Regulation."

Conclusion

We would like to thank Dr. Peter Gelber (Dipl.-Ing.) (source: http://www.dsgvo-zt.at/) and Wolfgang Fiala (Dipl.-Ing.) (source: http://www.dsgvo-zt.at/). As civil engineers, it was their task to review and evaluate an extensive data protection management system. We would also like to thank Mr. Zlamal, Managing Director of IITR Cert GmbH (source: https://www.iitr-cert.com/), for his extraordinary commitment.

We are convinced that a data protection management system provides the appropriate tools for companies and related business structures to meet the complex requirements of the GDPR. This conviction stems from our own experience in the companies we support.

In our view, the fact that we are currently unable to have recourse to state certifications in accordance with the GDPR for data protection management systems should not lead to certified data protection management systems being withheld from the market.

Compliance Kit 2.0 is available to all interested parties as the basis for a qualified determination of compliance with the provisions of the GDPR.

Author: Eckehard Kraska

Contact: Dr. Sebastian Kraska, Attorney at Law, External Data Protection Officer

Internet: www.iitr.de

Telephone: 089-18 91 73 60

Email: email@iitr.de

Status: August 7, 2019

Sources/quotations:

TeleTrust, "Handreichung zum Stand der Technik," p. 71, Source: https://www.teletrust.de/fileadmin/docs/fachgruppen/2019-02_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf

Context of data protection

The implementation of a management system – more precisely: a data protection management system (DPMS) – is also an appropriate way of checking the effectiveness of measures in connection with the requirements of the GDPR. The GDPR does not expressly prescribe such a system. Nevertheless, it indicates the necessity of a DPMS in many places. For example, Art. 32 (1d) GDPR requires a "procedure for the regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing."

Since such a procedure requires a planned and structured method within the organization, i.e., an implementation of the classical PDCA model, the establishment of a DPMS is an ideal solution. If this is aligned with the elements of the ISO high-level structure, it can also be integrated into an existing ISMS based on ISO 27001.

Just like an ISMS, the DPMS can then also be audited and the degree of maturity of the system determined successively. Based on the ISO 19011 guideline, audits can be carried out on the basis of an audit program and an audit plan. Audits can be carried out by the data protection officer. In larger organizations, audits can also be carried out by employees of the organization who have received expert training or by consulting firms specializing in data protection.

"Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO," by Alexander Jung in "ZD," 2018, p. 208, Source: https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzd%2F2018%2Fcont%2Fzd.2018.208.1.htm&anchor=Y-300-Z-Z-ZD-B-2018-S-208-N-1

Compliance management systems (CMS) are almost obsolete in today's world. This is solely due to the fact that there are various standards that specify the structure of a corresponding system including its components. This looks different in relation to data protection management systems (DPMS), where the controller is indeed assigned corresponding accountability obligations for its data processing operations by the General Data Protection Regulation (GDPR), but it remains open how it needs to concretely prove compliance with the data protection regulations. The article aims to illustrate the necessity of a DPMS or at least the systematic proof of proper data processing, whereby reference is also made to the "old" legal situation prior to May 25, 2018. Here, approaches are to be shown as to how, in the absence of clear standards, a reasonable approach can be chosen in order to comply with the burden of proof demanded by the GDPR.