Certification procedure for data protection concepts and IT systems

TÜV NORD GROUP

Trusted Site Privacy

Privacy 2017 Trusted Site

Certificate ID: 00000.17

Contents

1 Introduction

1.1 Privacy of personal data

Collection, processing, transfer and use of data have become a universal everyday occurrence in the information society of today. If electronic services or networks are used for communication or transactional purposes, data regarding the use and the user are generated automatically. This personal data can be assembled to very detailed information on the users, reaching from the persons' real names to the content of very confidential data exchanges.

For a considerable time now, the right to protection of this information has no longer only been viewed as an individual right in the sense of the right to self-determination in relation to personal data. Companies and organizations are realising more and more that inadequate data protection endangers their reputation, which ultimately puts their existence at risk.

Therefore hardly anyone nowadays doubts the need to protect personal data. However, the way in which this protection should be achieved and implemented, and also the effectiveness of the protection, is the subject of some controversy. All too often, data protection is recognized as another tedious regulatory task one has to comply with. Most organizations are trying to solve this by adding data protection as a low-profile add-on to their IT security concepts.

1.2 IT security and data protection

The results of many different IT security inspections, such as evaluations of security products according to ITSEC[1] or CC[2] and security management audits according to ISO 27001 or inspections based on the IT-Grundschutz Catalogues of the BSI[3], are just as inadequate for the needs of data protection as individual IT security audits[4] are.

On the other hand, the evaluation of the data protection of IT systems and IT processes cannot be implemented based on legislation alone. It is absolutely essential - following determination of the privacy requirements and starting from the relevant legislation - also to investigate and assess the relevant organizational and technical measures involved. Data protection and IT security complement each other here and are directly dependent upon one another.

1.3 Goals

The ultimate goals of those who are responsible for questions of data protection are objective identification and suitable elimination of risks to the **personal rights** of the individual which result from information processing. For reaching these goals, a twofold approach is required:

1) All questions related to **data protection legislation** which are relevant for a particular IT system or IT infrastructure must be identified and answered thoroughly.

2) In order to ensure that collection and processing of personal data are fulfilling the requirements of data protection law, the technical implementation of the process or service has to be checked for compliance to the data protection requirements.

[1] Information Technology Security Evaluation Criteria
[2] Common Criteria
[3] Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
[4] e.g. the **S**ecurity **Q**ualification procedure of TUViT

1.4 Trusted Site Privacy

TUViT has developed a certification procedure in which evaluation of the privacy of a process is combined with evaluation of the security of the corresponding IT system.

Among others, the quid! criteria serve as a basis for assessment of data protection. Within the two-year EU quid! research project, common characteristics for ensuring quality of data protection in operational environments were worked out by more than 80 experts from industry and science, from state and private data protection organizations, from public administration bodies, consultancy organisations, from federations and trade unions and also from works councils and top company management. Objective and easy-to-use criteria for comparative assessment of data protection were developed. TUViT has the sole rights to perform certifications based on these criteria and for this purpose offers a standardised audit procedure which is combined with security-related inspection (see section 2.2).

The procedure takes all the factors which are decisive for data protection fully into consideration and focuses on the fundamental and critical points which are essential to data protection. The results of the data protection audit according to this procedure permit a differentiated and appropriate reaction to data protection problems that are recognised. A quality model which is suitable for use in practice ensures both universal applicability and specificity suited to the particular features of the item to be investigated.

The context of the item to be investigated is taken into consideration in the formulation of individual data protection requirements.

The prerequisite for successful data protection certification is that the content which is necessary for determination of the data protection requirements is identified and its boundaries established. Within the framework of the audit, this content is described based on the documentation available from the customer, and is later on discussed and agreed with the customer.

The item to be investigated, or target, which is laid down from this content (Target of Audit[5]) then forms the basis for the legal and technical inspection.

Building on the data protection/privacy audit, the technical requirements regarding data protection which the operator must have implemented by means of his IT installation, including his network connection, are made concrete and included in the follow-on security-related inspection. Weaknesses of the IT installation are identified and evaluated within the framework of penetration tests and configuration analyses. These must be free of contradictions and fulfil "applicable entitlements to privacy".

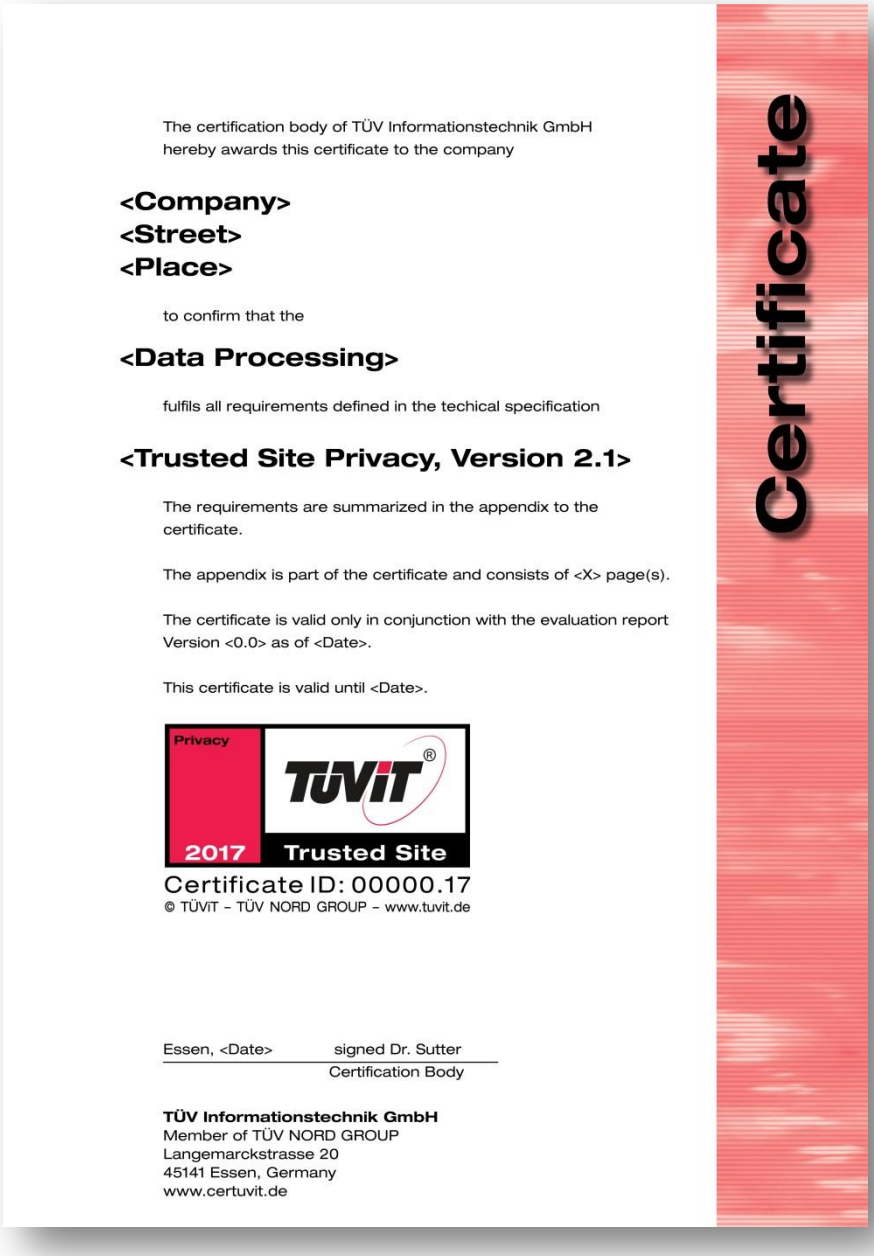
Trust in the security of the subsystems and the components (or security products) used in them is a necessary prerequisite for the security of the entire installation. Hence, an assessment is made of components or subsystems which implement security functions, in order to establish how far they can be considered as trustworthy.

It can only be guaranteed that IT installations are secure in normal operation and also in exceptional situations if suitable technical means and organizational measures are available for the purpose. Suitable configuration tools for security-specific components must be present, and it must be possible to monitor these components. All administration tools must naturally be secured to the same level as the security-specific subsystems themselves.

1.5 Certification

Certification is based on the results of the data protection audit and the security-related examination. The certification demonstrates fulfilment of the organizational and technical data security requirements. It gives the customer and in particular third parties certainty regarding the privacy of personal data in the sense of a "Third Party Inspection" by the independent certification body of TUViT.

[5] ToA = Target of Audit



The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

<Company>
<Street>
<Place>

to confirm that the

<Data Processing>

fulfils all requirements defined in the techical specification

<Trusted Site Privacy, Version 2.1>

The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate and consists of <X> page(s).

The certificate is valid only in conjunction with the evaluation report Version <0.0> as of <Date>.

This certificate is valid until <Date>.

Privacy 2017 Trusted Site

Certificate ID: 00000.17

Essen, <Date> signed Dr. Sutter
Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD GROUP
Langemarckstrasse 20
45141 Essen, Germany
www.certuvit.de

Certificate

Figure 1: Example of certificate

2 Aspects of evaluation

The quality level of the data protection that has been achieved is established based on fulfilment of requirements. In this process, a series of quality characteristics is included into the investigation, as listed below:

The data protection audit includes the following aspects for evaluation:

- Legal requirements
- Permissibility of processing
- Customer friendliness
- Employee friendliness
- User friendliness
- Transparency
- Data protection quality management
- Data security

An investigation of the system from the technical point of view is also performed.

2.1 Data protection audit

2.1.1 Legal requirements

First the legal norms that apply to the target as regards processing of personal data are identified (e.g.: Federal Data Protection Act, labour law, medical law, telecommunications law). These result directly from the context in which the target is used. In a further step, an assessment is made as to whether the legal requirements which have been established as relevant are fulfilled.

2.1.2 Permissibility of processing

Data protection law states that personal data may not be processed without legal permission or the valid agreement of the affected person. Following identification of the data types which are relevant to the examination, each data type is investigated in order to establish if processing is permissible with regard to the aim of the data processing. Requirements regarding data economy, i.e. to ensure that only essential data is collected, are taken into consideration in association with the state of technology.

2.1.3 Customer friendliness

The customers of a company have a right to know what happens to their personal data, how processing continues afterwards, and whether there is a possibility for self-data protection, i.e. for influencing the processing of the data.

2.1.4 Employee friendliness

The employees of a company must also be informed as to which of their data are processed using what processes. It must be made transparent to them what rights they have, and what possibilities to find out about the handling of their data, and also how their personal data is saved. Data protection must already play an important part in drawing up the contract and describing the workplace.

2.1.5 User friendliness

When an IT product is used, the user must be informed of the function of the product, in order to be able to process personal data securely and in compliance with data protection law. The information should include, for example, suitable product descriptions and installation guides and also corresponding instructions and/or the possibility to receive information from a company which installs and uses an information processing product.

2.1.6 Transparency

The data protection policy, the data protection concepts and also the organizational and technical measures used to implement the data protection within the company or process must be made transparent and understandable to all those affected. The focus of the examination is that the measures which have been taken to ensure permanent data protection and privacy are designed so as to be logical and transparent.

2.1.7 Data protection quality management

Changes in the area of information technologies and the legal bases of data protection generally have an influence on the concept used in order to fulfil data protection requirements. They must be regularly and promptly examined and implemented with regard to the effects on data protection. Analyses and action models must also be adapted as necessary. The examination is also concerned with the quality management measures which are developed from this.

2.1.8 Data security

The information systems which are used can only fulfil the requirements of data security if suitable organizational and technical measures are taken in relation to data security. Corresponding concepts must be present and trustworthy components should be used in the design and construction of the systems.

Access control

Equipment for processing or use of personal data must be protected from unauthorized PHYSICAL access by third parties.

Access control

Use of the data processing systems by unauthorised persons must be effectively prevented through use of suitable measures against unauthorized logical SYSTEM access.

Access control

This section comprises the measures against unauthorized DATA access: Persons who are authorised to make use of a data processing system should only be able to access the data for which they have corresponding authorisation. Unauthorised reading, copying, changing or removal of personal data must not be possible during processing, use and subsequent saving.

Transmission control

Unauthorised reading, copying, changing or removal of personal data must not be possible during electronic transfer or during transportation or storage on data carriers. It must be possible to check and establish at what points transfer of personal data through data transfer equipment is intended.

Input control

It must be possible to check and establish afterwards if and by whom personal data have been input into the system, changed or removed/deleted from the system.

Job control

Personal data which are processed by order or on behalf of the client may only be processed in accordance with the customer's instructions. A supplier may only collect, process or use the data in order to fulfil the instructions issued by the customer.

Availability control

Personal data must be protected from accidental destruction or loss by means of suitable measures.

Need for separation

It must be ensured by means of appropriate measures that data collected for different purposes is processed separately and not combined to create new information.

2.2 Security-related investigation

2.2.1 Security of the components used

Formal evaluations already performed and/or other reliable publicly available information on security audits of partial components which implement security functionalities can be considered. It can be taken as a fact, that those components have been assessed as trustworthy.

2.2.2 Means for system management

It is checked whether suitable configuration possibilities exist, along with suitable monitoring and logging to ensure a secure and reliable operating state. Tools used for this are subject to the same security requirements as the IT product / IT system itself.

2.2.3 Tests and inspections

Comprehensive penetration tests and analyses of technical weaknesses are performed during the assessment. The weaknesses which are identified during the tests and analyses are rated according to the environmental risk profile of the IT product / IT system.

3 Assessment criteria for Trusted Site Privacy, Version 2.1

There are a series of test items for each assessment aspect. These are summarised below.

Aspects of assessment	Test items
Legal requirements	• Legal category of test object • Formal requirements • Requirements for the different processing phases • Cross-border operation • Responsibilities • Description of the requirements for the test object

Permissibility of processing	• Purpose
	• Authorisations and justification for the data processing, e.g.:
	  • Contract and relationships of trust similar to contract
	  • Justified interest of the data controller
	  • Justified interest of a third party
	  • Justified public interest
	  • Generally/publicly accessible sources
	  • Transmission in the form of a list
	  • Agreement of the data subject
	  • Other legal regulations or legislation
	• Fulfilment of the basic principles of data protection and privacy
	• Observance of the rights of data subjects
	• Technical and organisational measures
	• Structural conditions
	• Proportionality
	• Declaration of obligation

Aspects of assessment	Test items
Data subject friendliness	• Notes drawing attention to data protection • Participation • Possibility for individuals to protect their own personal data by technical or organisational means • Acceptance of the technical and organisational means • Appropriate product description • Installation instructions • Possibility of training or information b
Transparency	• Transparency of the data protection policy • Transparency of the technical and organisational means used
Data protection quality management	• Data protection policy • Risk analysis • Responsibility for data protection • Data protection qualification • Notes drawing attention to data protection • Documentation • Continual improvement process • System administration • Documentation
Data security	• Entry control • Physical access control • Data access control • Transmission control • Data entry control • Order control • Availability control • Data separation
Security inspection	• Security of the components used, also network and data transport security • Means and methods used for system management • Tests and inspections

4 Certification

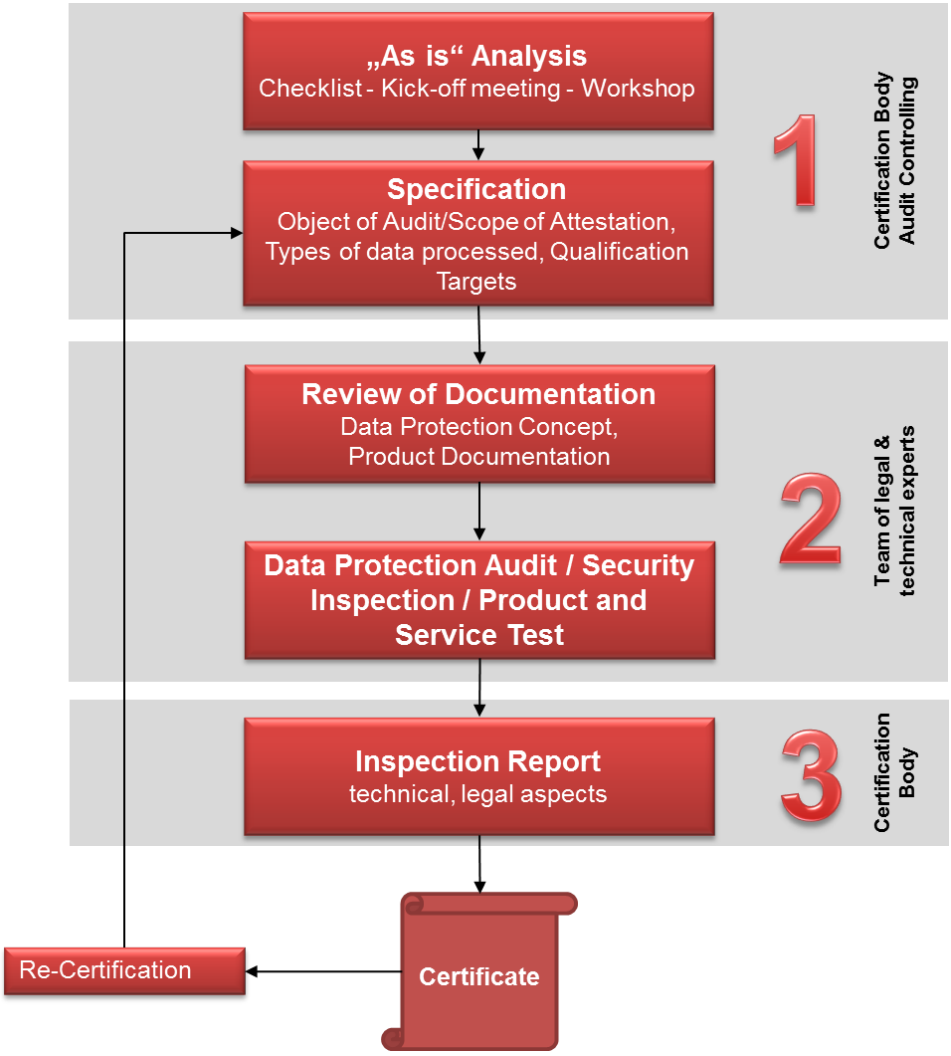


Figure 2: Certification scheme

The quality of the data protection is evaluated by auditors who are accredited by the certification body. In the preparation phase, the audit team will review relevant documents referring to the target (data protection policy, data protection guidelines, data protection guidelines and declarations, manuals, risk analyses etc.) and prepare the on-site audit. On site at the customer's premises, data is collected by the auditors in interviews and in random samples regarding the technical and organizational environment of the target.

In the following security-related investigation, implementation of the technical data protection requirements is checked. After this an audit report is drawn up which documents the fulfilment of the requirements and if appropriate also describes potentials for improvement in relation to data protection.

Following presentation of the audit report, which confirms that the assessment aspects are fulfilled, the certification body issues a certificate which authorises the holder to make use of the Trusted-Site Privacy mark in its dealings with the public and in advertising and marketing. The certificate is valid for two years.

5 Trusted Site certification family (abstract)

Under the "Trusted Site" logo, TÜV Informationstechnik GmbH awards test marks that confirm the fulfilment of security and quality features for IT systems.

Trusted Site — *Infrastructure*

examines the infrastructure (building, energy supply, security systems, fire alarm and extinguishing technology et.) and confirms the suitability for security areas for which high availability is demanded.

Trusted Site — *Security*

examines the IT security of (typically networked) IT installations and confirms the fulfilment of suitable security targets within the framework of a security-related validation procedure.

Trusted Site — *ITSM*

examines the IT Service Management Processes of the ITIL Reference model concerning quality, integrity and level of implementation in reference to the requirements of ISO 20000 for the organisation.

Trusted Site — *PK-DML*

examines the audit-proof archiving of document management solutions.

The above TUViT test marks can also be issued in the form of combined test marks if they have the same term of validity and cover the same area within a company.

6 About TÜViT

TÜV Informationstechnik GmbH – TÜViT in short – is a member of the **TÜV NORD GROUP**, based in Hannover, Germany. TÜV NORD has a workforce of more than 10.000 staff worldwide and is active in 70 countries in Europe, Asia and America besides Germany. Over a TÜV tradition reaching back 140 years, TÜV NORD has performed and developed technical tests and inspections in very many different areas. The principles upon which the company operates stipulate that the TÜV NORD GROUP must offer and implement its services independently and on a neutral and impartial basis.

As an intermediary with the role of creating trust in IT security and IT quality, TÜViT has specialised in the inspection, evaluation and certification of IT products, IT systems and IT processes of all kinds, and also on assessment in relation to special requirements, laws, guidelines and directives (eCompliance). TÜVIT develops evaluations and assessments for manufacturers, operators and users based on general requirements and national/international standards. In this process, TÜViT makes use of recognised processes and also offers advice and professional services in the area of information technology.

TÜViT is accredited by national and international organisations, and official authorities and bodies, for the scope of IT security and IT quality. Accreditations are the official recognition by a higher-level organisation of the expert competency of an inspection body. The accreditations are confirmed by means of regular audits and therefore demonstrate the expert competency of TÜViT in these areas.

Federal Office for Information Security

- Accreditation according to DIN EN ISO/IEC 17025:2005 for evaluations according to ITSEC/ITSEM/CC/CEM as well as BSI-TR 03105 Part 3 and 5, BSI-TR 03121, BSI-TR 03132 and BSI-TR 01201
- Licensed auditors for IT-Grundschutz, ISO/IEC 27001 on the basis of IT-Grundschutz and for De-Mail
- IT-Security Service Provider in the field of IS-Revision and IS-Consulting and Penetrationtesting

German Accreditation Body

- Testing Laboratory for IT Quality: Competence for evaluations in the field of IT Ergonomics and IT Security, accredited according to DIN EN ISO/IEC 17025
  - Evaluation Body for IT Security: Accreditation for evaluations according to CC/CEM/ITSEC/ITSEM
  - Evaluation Body for IT Usability: Accreditation for evaluations according to DIN EN ISO 9241-110, DIN EN ISO 9241-11, ISO/IEC 25051, DIN EN ISO 13407 and ISO 9241-210
- Certification Body: Competence for certifications of products in the field of IT Security (ITSEC, Common Criteria, ETSI EN 319 401 / 319 411-1 / 319 411-2 / 319 421, ETSI TS 101 456 / 102 042 / 102 023, DIN EN 50518-1:2014 / -2:2014 / -3:2014), accredited according to DIN EN ISO/IEC 17065:2013
- Certification Body: Competence for certifications of products, processes and services in accordance with EN ISO/IEC 17065:2013 and ETSI EN 319 403 V2.2.2 in the scope qualified trust service providers and the qualified trust services provided by them in the scope of application REGULATION (EU) No 910/2014 (eIDAS)

Federal Network Agency

- Confirmation Body according to Signatures Act/Signatures Ordinance for the confirmation of products for qualified electronic signatures
- Confirmation Body according to Signatures Act/Signatures Ordinance for the confirmation of the implementation of security concepts for certification service providers

German Banking Industry Committee

- Listed Testing Body for Electronic Payment Transactions

Independent Centre for Privacy Protection Schleswig-Holstein

- Test Centre for Privacy (legal/technical)
- EuroPriSe Experts (legal/technical)

Information-technology Promotion Agency, Japan

- IT Security Evaluation Facility: Competence for evaluations according to CC/CEM

National Institute of Technology and Evaluation, Japan

- Evaluation Body for IT Security: Accreditation according to DIN EN ISO/IEC 17025 in the field of IT / Common Criteria evaluations (Lab Code: ASNITE0019T)

National Institute of Standards and Technology, USA
National Voluntary Laboratory Accreditation Program, USA

- Evaluation Body for IT Security (NVLAP Lab Code: 200636-0) for Cryptographic Module Testing (scopes 17BCS, 17CAV/01, 17CMH1/01, 17CMH1/02, 17CMH2/01, 17CMH2/02, 17CMS1/01, 17CMS1/02, 17CMS2/01, 17CMS2/02) and Biometrics Testing

Europay, MasterCard and Visa, USA/United Kingdom/Japan

- Full Service Laboratory for evaluations of ICs and IC cards according to EMVCo Security Guidelines
- Modular Label Auditor

Visa, USA

- Test House for performing Visa Chip Product security evaluations

MasterCard, United Kingdom

- Accredited to perform CAST (Compliance Assessment and Security Testing) evaluations

Betaalvereniging Nederland, The Netherlands

- Evaluation Laboratory

In the field of testing/evaluation services, TÜViT, as an independent authority, strengthens the adequate trust in quality, security and efficiency. Thus, TÜViT enhances the acceptance of products and systems as well as their operation in the financial sector, industry and public administration. In national and international research projects and bodies, TÜViT participates actively in developing the state of the technology.

Related to this is, for instance, TÜViT is involved in the shaping of auditing and certification practices according to IT-Grundschutz method of the Federal Office for Information Security and ISO/IEC 27001. TÜViT deploys auditors for IT-Grundschutz and ISO/IEC 27001.

TÜViT meets its customers' high expectations with an active and responsive quality management system certified according to ISO 9001:2008.

Furthermore, TÜViT performs comprehensive training courses and consultancy for all eCompliance topics.

7 Contact

Jörg Schließke, LL.B.

Product Manager Data Privacy Qualification

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstrasse 20
45141 Essen, Germany

Tel.: +49 201 8999-533
Fax: +49 201 8999-666
j.schlisske@tuvit.de
www.tuvit.de