Information Security Considerations (Germany)

by Dr. Paul Voigt, Taylor Wessing PartG mbB, with Practical Law Data Privacy Advisor

Practice notes | Law stated as of 10-Aug-2021 | Germany

A Practice Note describing the laws, regulations, enforcement practices, and local resources to consider when developing, implementing, and maintaining an information security program in Germany or as applied to data originating from Germany. It discusses the Federal Data Protection Act (BDSG) and critical infrastructure provider obligations under the IT Security Act and IT Security Act 2.0. It addresses related EU law, such as the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), the EU Directive on the Security of Network and Information Systems (Directive 2016/1148/EC) (NIS Directive), and Germany's implementing laws. It also discusses Federal Office for Information Security (BSI) regulations, standards, and resources. The Germany-specific guidance in this Note may be used with the generally applicable resources listed in the Global Information Security Toolkit.

Information security programs protect the confidentiality, integrity, and availability of data and information technology (IT) assets. However, differences in local data security laws, practices, and standards create challenges for global companies, and failure to comply with them can result in enforcement action and litigation. This Practice Note explains the German laws, regulations, enforcement practices, and local resources to consider when developing, implementing, and maintaining an information security program in Germany or as applied to personal data

originating from Germany. The Germany-specific guidance in this Note may be used with the generally applicable resources listed in the Global Information Security Toolkit.

Information Security Laws and Regulations

Several German laws regulate information security and set related standards, including:

- The Federal Data Protection Act (BDSG), which protects personal data. Germany updated the Act to align with the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) (see GDPR and the BDSG).
- The Federal Office for Information Security (BSI) Act of 2009 (BSIG), as amended by the IT Security Act and IT Security Act 2.0 (both in German), which affects various critical infrastructure sectors. Germany updated the BSIG when it transposed the EU Directive on the Security of Network and Information Systems (Directive 2016/1148/EC) (NIS Directive) into German law, under the NIS Directive Implementation Act (see NIS Directive Implementation and the BSIG).
- The Telecommunications and Telemedia Data Protection Act (TTDSG), which comes into force on December 1, 2021 (see Sector-Specific Requirements).
- Other legal regimes that protect at-risk data and interests (see Other Laws).

Data security requirements and expectations may also derive from general compliance obligations. For example, the managing director of a German limited liability company (GmbH) has a general duty of care towards the company that may include implementing adequate data security measures (Section 43(1), Limited Liability Company Act (in German)).

GDPR and the BDSG

The GDPR applies in all member states as of May 25, 2018. Germany enacted the Data Protection Adaptation and Implementation Act (DSAnpUG-EU) and the Second Data Protection Adaptation and Implementation Act (2nd DSAnpUG-EU) to update the BDSG, align it with the GDPR, and make conforming changes to other laws.

For more information on Germany's general data protection requirements, see Country Q&A, Data Protection in Germany: Overview.

The GDPR broadly defines personal data to include any information relating to an identified or identifiable natural person (Article 4(1), GDPR). Personal data generally includes information that alone or in combination with other information that an organization has or is likely to have access to directly or indirectly identifies an individual data subject.

The GDPR has additional rules that apply to processing special categories of personal data, which include:

- Racial or ethnic origin.
- Political opinions.
- Religious and philosophical beliefs.

- Trade union membership.
- Health, sex life, or sexual orientation.
- Genetic and biometric data.

(Article 9(1), GDPR.)

The BDSG contains some GDPR-permitted derogations, for example, relating to exceptions from:

- The information notice obligations (Section 33, BDSG and Article 23, GDPR).
- The designation of a data protection officer (Section 38(1), BDSG and Article 37(4), GDPR).

(For more, see Country Q&A, GDPR Derogations: Germany.)

The BDSG also contains provisions that regulate data protection outside the GDPR's scope of application, for example, relating to the processing of personal data by public bodies responsible for addressing criminal or administrative offenses (Sections 45 to 84, BDSG; Recital 19, GDPR).

Protecting Personal Information Under the GDPR and the BDSG

The GDPR:

- Requires controllers and their data processors to:
  - take a risk-based approach to securing personal data; and
  - implement appropriate technical and organizational measures commensurate with risks.

  (Article 32, GDPR.)
- Highlights several appropriate security measures, including:
  - pseudonymization and encryption;
  - abilities to ensure the ongoing confidentiality, integrity, availability, and resilience of data processing systems and services;
  - abilities to restore availability and access to personal data in a timely manner if a physical or technical incident occurs; and
  - a process for regularly testing, assessing, and evaluating the effectiveness of the organization's technical and organizational security measures.

  (Article 32(1), GDPR.)

For general information on the GDPR, see Practice Note, Overview of EU General Data Protection Regulation. For more details on anonymization and pseudonymization as information security controls, see Practice Note, Anonymization and Pseudonymization Under the GDPR. The Federal Commissioner for Data Protection and

Freedom of Information (BfDI) has also provided guidance (in German) on anonymization practices and related issues.

Data Destruction Under the GDPR and the BDSG

The GDPR requires that controllers retain personal data only for as long as necessary for the processing purposes (Article 5(1)(e) GDPR). The BDSG does not otherwise generally address personal data destruction.

Certain data processing activities may be subject to additional data retention restrictions (for more, see Country Q&A, Records Retention: Germany).

NIS Directive Implementation and the BSIG

The Federal Office for Information Security (BSI) in the Federal Ministry of the Interior acts as Germany's national cybersecurity authority, under the BSIG.

The NIS Directive and BSIG:

- Apply minimum information security standards to critical infrastructure (see Critical Infrastructure).
- Update information security-related obligations under several German sector-specific laws (see Sector-Specific Requirements).
- Require various sectors and service providers to notify the BSI and other agencies if a cyber incident occurs (see Cyber Incident Response and Data Breach Notification).

Critical Infrastructure

Critical infrastructure includes facilities that are important to Germany because a loss of their operation may lead to significant supply shortages or endanger national security. The NIS Directive and BSIG, lay out security and cyber incident notification requirements for:

- Digital service providers that offer certain information society services, including:
    - online marketplaces;
    - online search engines; and
    - cloud computing services.

  (Article 4(6), NIS Directive; Section 2(11), BSIG.)
- Operators of essential services across various critical infrastructure sectors, including:
    - Energy.
    - Transportation.
    - Banking and financial market infrastructures.
    - Health care.

- Water.
- Digital infrastructure.

(Article 4(4), NIS Directive; Section 2(10), BSIG.)

The IT Security Act and IT Security Act 2.0 updated the BSIG to:

- Expand the critical infrastructure sectors to include:
  - information technology and telecommunications, including digital infrastructure;
  - insurance, in addition to banking and financial services;
  - municipal waste disposal; and
  - nutrition.

  (Section 2(10), BSIG.)
- Add obligations for certain companies that are not necessarily operators of essential services but are important to the public interest due to:
  - their role in the critical infrastructure supply chain as manufacturers of certain critical components;
  - other economic impact factors; or
  - hazardous material handling.

  (Sections 2(13) and 2(14), BSIG.)

Under the NIS Directive and BSIG, covered companies must take technical and organizational security measures that:

- Are appropriate and proportionate to the risks posed.
- Consider the state of the art.

(Articles 14(1) and 16(1), NIS Directive; Sections 8a, 8c, and 8f, BSIG).

German law further requires critical infrastructure providers, including operators of essential services, to:

- Adopt appropriate organizational and technological measures to protect the availability, integrity, authenticity, and confidentiality of their IT systems and facilities that:
  - align with state-of-the-art technology; and
  - may leverage industry-defined sector-specific security standards (for more information on IT baseline protection profiles for particular groups, see Industry Standards).

- Demonstrate to the BSI every two years that their facilities meet BSIG requirements (see Program Review and Certification).
- As of May 1, 2023, use attack detection systems that continuously and automatically record, evaluate, and take appropriate remedial measures for threats to the organization's systems (Section 8a(1a), BSIG).
- Notify the Federal Ministry of the Interior of any planned, first-time uses of certain critical components in their systems (Section 9b(1), BSIG).
- Obtain a declaration from the manufacturer about the trustworthiness of certain critical components they use (Section 9b(3), BSIG).

BSI-Kritis regulations further implement the BSIG's information security and notification requirements in some sectors. For more information, see the critical information protection website which supports a joint initiative from the BSI and the Federal Office of Civil Protection and Disaster Assistance.

The NIS Directive and the European Commission's implementing regulations impose more detailed security requirements on digital service providers. However, the Directive also prohibits member states from imposing additional security and notification obligations on digital service providers because of the cross-border nature of their services (Article 16(10), NIS Directive).

On December 16, 2020, the European Commission (EC) and the High Representative of the Union for Foreign Affairs and Security Policy issued an updated cybersecurity strategy that anticipates a reformed NIS Directive (Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade) and included the EC's proposed Network and Information Systems 2.0 Directive (NIS 2.0 Directive).

For more details on the NIS Directive and its requirements, see Practice Note, EU NIS Directive Implementation Activities: Overview.

Sector-Specific Requirements

The updated BSIG addresses information security-related obligations under several German sector-specific laws, including those that apply to:

- **Telemedia service operators.** The Telemedia and Telecommunications Data Protection Act (TTDSG) comes into force on December 1, 2021 and replaces various privacy and IT security related provisions of the Telemedia Act. The TTDSG regulates public websites, social media, and other online services as well as telecommunication services. Operators of telemedia services must implement technologically feasible and economically reasonable measures to ensure that:
  - users are at all times able to terminate the services;
  - no unauthorized third-party access to the services is possible (Section 19(1), TTDSG); and
  - feasible protections against internally and externally caused service interruptions are in place (Section 19(4), TTDSG).
- **Telecommunications providers.** The Telecommunications Act (in German) (TKG) regulates providers of telecommunications facilities and services. While these providers are also covered by the new TTDSG, some of the sector-specific requirements in the TKG continue to apply in parallel. The Federal Network

Agency has published a catalog (in German) of security requirements for telecommunications and related data processing systems. Under the TKG, providers must:

- implement appropriate technological measures to protect against service interruptions and manage security risks (Section 165(2), TKG); and
- warn customers if they detect that their network connections are being used in cyberattacks, for example, as part of a botnet (for more information on botnets and other forms of malicious software, see Practice Note, Cybersecurity Tech Basics: Malware and End User Attacks: Overview).

- **Electricity supply network providers.** The Energy Economy Act requires electricity supply network providers to protect the telecommunications and IT systems necessary for safe and reliable electricity operations (Section 11(1a) EnWG). The Federal Network Agency and BSI together support standards for documenting and implementing these and related information security requirements.

Health Data

The Social Code Book Five (in German) (SGB V), as amended by the Patient Data Protection Act (in German) in 2020, requires all hospitals to adhere to specific information security standards and regulations beginning January 1, 2022 (Section 75c, SGB V). The BSI has also published technical guidance (in German) on security measures for digital health apps, which requires developers to:

- Address core information security principles of confidentiality, integrity, and availability.
- Build data security into their apps throughout the development process.

Other Laws

German law protects other types of at-risk data and interests, including:

- **Information and IT systems for public companies.** The Stock Corporation Act (in German) (AktG) requires German Stock Corporation managing boards to comply with all applicable laws, manage the corporation's business diligently, and monitor corporation management (Section 93, AktG). These obligations may require the managing board to ensure the organization implements adequate information security measures, according to data sensitivity and risks. Managing board members may be liable for damages arising from a violation of these duties.
- **Trade secrets.** The Trade Secrets Protection Act (in German) (GeschGehG) requires that information not be easily accessible to receive trade secret protection (Section 2 number 1, GeschGehG). To ensure trade secret protection, organizations must:
  - take sufficient organizational and technological measures to protect their information; and
  - prevent unauthorized third party access to their trade secrets.

- **Business contracts.** Requirements to implement data security measures may also arise under contractual duties. Conversely, organizations that fail to support sufficient data security measures may be liable for damages claims based on German contract and tort law. Common obligation sources include:
    - data processing agreements;
    - non-disclosure agreements; and
    - general contractual commitments to follow industry standards and practices, including implicit or unwritten expectations.

Industry Standards

The BSI developed and has long offered organizations the IT-Grundschutz, a set of information security standards, recommendations, and best practices. The IT-Grundschutz:

- Takes a step-by-step methodology approach.
- Explains how to design, implement, and maintain an information security management system and program.
- Includes companion resources on risk analysis and business continuity management.

Organizations that implement the IT baseline protection of the IT-Grundschutz can apply for internationally-recognized ISO/IEC 27001 certification.

The BSI modernized the IT-Grundschutz to make it more flexible and responsive to current cybersecurity needs. This approach:

- Offers organizations three risk-based approaches, including:
    - basic protection, which focuses on basic information security functions and is targeted at small and medium-sized enterprises that are only beginning to implement such functions;
    - core protection, which expands basic protection but emphasizes securing fundamental business processes; and
    - standard protection, which reflects the current IT baseline protection approach and addresses a broader set of issues for implementing a comprehensive cybersecurity system.
- Provides guidance on the implementation of a data security emergency system.
- Supports greater community engagement, including opportunities to help develop state-of-the-art technology modules.
- Includes IT baseline protection profiles which:
    - allow similar organizations to share information security know-how and best practices; and

- may provide the basis for developing and maintain sector-specific security standards, as the IT-SiG encourages for critical infrastructure sectors.

The IT-Grundschutz methodology, other selected BSI standards, and related information security guidance and self-assessment publications are available in English and German on the BSI's website.

Developing, Implementing, and Maintaining an Information Security Program

German laws obligate most organizations to support an information security program for one or more purposes, such as:

- To protect the personal data they collect and use, including employee data (see GDPR and the BDSG).
- To secure their public websites, social media, or other online or telemedia services (see Sector-Specific Requirements).
- To protect facilities or services considered critical infrastructure (see Critical Infrastructure).

These laws require some organizations to support specific safeguards or other program elements. However, other organizations must develop, implement, and maintain a comprehensive, standards-based information security program. Some standards, including the IT-Grundschutz and ISO 27001, refer to an organization's overarching program or approach to information security as an information security management system (ISMS).

Documenting an organization's ISMS may provide significant risk management benefits, even if not explicitly required by law, for example, by:

- Demonstrating the organization's alignment with applicable industry standards (see Industry Standards).
- Prompting the organization to proactively assess risk and implement safeguards.
- Communicating information security expectations and practices to leadership, employees, customers, and other interested parties, including regulators.
- Establishing that the organization takes appropriate steps, especially if a data breach or other cyber incident occurs where litigation or enforcement action could follow.

For more details on building comprehensive information security programs, see the resources and guidance in Global Information Security Toolkit.

German laws, including sector-specific requirements, and industry standards may affect an organization's considerations when implementing several key information security program elements, including:

- Assigning accountability (see Information Security Coordinator or Officer).
- Identifying and assessing risks (see Risk Assessments).
- Developing information security policies (see Policies).

- Selecting safeguards (see Safeguards).
- Evaluating program effectiveness and compliance (see Program Review and Certification).

Information Security Coordinator or Officer

The GDPR requires some organizations to appoint a data protection officer (DPO) who oversees an organization's activities to protect personal data, including its information security measures. Specifically, organizations must designate a DPO if:

- They are a public authority or body that processes personal data, except for courts acting in their judicial role.
- They regularly and systematically monitor individuals on a large scale.
- Their core activities include processing special categories of personal data or personal data related to criminal offenses and convictions on a large scale.

(For more information on the GDPR, see GDPR and the BDSG.)

Organizations also must designate a DPO if they constantly employ at least 20 individuals who deal with the automated processing of personal data (Section 38(1), BDSG).

The BSI standards urge organizations to assign accountability for information security to upper management and designate an information security officer or coordinator. Some sector-specific laws also include related requirements. For example, the TKG requires telecommunications providers to appoint a telecommunication security officer to assess risks and implement appropriate security measures, which may include cybersecurity controls (Section 109(4), TKG).

Organizations should consider applicable industry standards, any sector-specific obligations, and their overall risks and business needs when choosing how to assign accountability for information security.

Risk Assessments

The BSI standards take a risk-based approach to information security and provide guidance on performing risk assessments (see Industry Standards). German law does not include a general obligation to perform overall data security risk assessments. However, risk assessments play a crucial role in maintaining information security and many organizations are increasingly subject to related obligations. For example, organizations must assess and manage information security risks to:

- **Protect personal data.** The GDPR and BDSG require organizations to adopt appropriate security measures commensurate with risks (see GDPR and the BDSG). Organizations must perform risk assessments to reliably identify appropriate security measures.
- **Meet enhanced IT security obligations.** The BSIG and other sector-specific laws require various organizations to adopt appropriate safeguards to protect their systems and facilities, which implies assessing and managing risks. For example, these obligations apply to organizations such as:

- operators of essential services;
- telemedia services operators, including public websites, social media, and other online services; and
- certain companies that are not necessarily operators of essential services but are deemed important to the public interest.

(For more, see NIS Directive Implementation and the BSIG.)

- **Evaluate external service providers.** Organizations that outsource processing personal data and other IT functions must include information security risk assessments in their due diligence and service provider oversight processes to avoid surprises and meet their own obligations.

Policies

German law does not include a general requirement for organizations to develop, implement, and maintain information security policies. However, the GDPR and BDSG requirements for appropriate security measures imply the need for policies in most organizations.

Enhanced information security standards also require some organizations to implement policies (see NIS Directive Implementation and the BSIG). Organizations may benefit from a policy by:

- Establishing information security as a core value.
- Helping employees and others understand information security risks and take appropriate actions to minimize them.
- Providing clear strategies and rules for using and protecting the organization's information and other IT resources.

Policy Considerations for Employers

Companies that have implemented a works council, typically German workplaces with more than five employees, must consider co-determination rights when developing information security policies and controls. Specifically, the Works Constitution Act (in German) provides workers with co-determination rights regarding employers' use of technologies that monitor employee behavior or performance. These obligations likely affect technical controls that scan communications or network traffic, including anti-malware software, firewalls, intrusion detection and prevention programs, and data loss prevention tools.

Other German laws may affect typical information security policy areas, including:

- **Employee monitoring and personal use.** Employers in Germany are free to choose whether they allow or prohibit personal use of an organization's email, telephone, internet access, or other communications facilities. However, employers who permit personal use may be subject to communications secrecy laws. In both cases, the GDPR likely limits any monitoring without consent, and DPAs generally question consent as a legal basis in the employment context. For more information on employee monitoring issues, see Practice Note, Employee Monitoring (Germany).

- **Bring your own device to work.** Organizations with a works council that support bring your own device to work (BYOD) must establish a works council agreement for related policies and procedures. Organizations should also consider BDSG obligations to protect personal data when:
    - establishing BYOD policies;
    - entering into BYOD agreements with individuals; and
    - selecting BYOD technical controls such as data segmentation, encryption, and remote wiping capabilities.

Safeguards

German law generally requires organizations to take organizational and technical measures appropriate to protect the data they collect and the risks they face. Some laws specify particular safeguards, for example:

- The GDPR and BDSG require organizations to implement appropriate controls to protect personal data (see GDPR and the BDSG).
- The BSIG, as updated by the IT Security Act 2.0:
    - requires operators of essential services to use state-of-the-art technology and, beginning May 1, 2023, to implement systems for detecting cyberattacks;
    - encourages industry groups to develop sector-specific security standards.

    (For more, see NIS Directive Implementation and the BSIG.)

The BSI's industry standards include detailed recommendations for selecting and implementing safeguards and training employees (see Industry Standards).

Program Review and Certification

Organizations should periodically review their information security program, especially when there is a material change in business practices, IT systems, or the risks they face.

For example, under the BSIG, operators of essential services:

- Must demonstrate every two years to the BSI that their facilities meet BSIG requirements through audits, examinations, or certifications (Section 8a(3), BSIG).
- Are subject to significant fines of up to EUR20 million for failures (Section 14, BSIG).

Cyber Incident Response and Data Breach Notification

Germany does not generally mandate cyber incident response planning. However:

- Information security program standards imposed on some organizations, such as operators of essential services, typically include incident response planning.
- The European Data Protection Board guidance under the GDPR emphasizes that organizations have a responsibility to implement incident response plans (Introduction, Guidelines on Personal data breach notification under Regulation the GDPR (WP250) (Feb. 6, 2018)).
- Industry standards typically include response planning requirements.

A robust, well-tested incident response plan can help any organization respond more effectively to cyber incidents and data breaches (for an example plan, see Standard Document, Global Cyber Incident Response Plan (IRP)).

The GDPR requires notification to affected individuals and authorities for applicable breaches of personal data. Some organizations, including certain operators of essential services and other service providers, must report cyber incidents, even if they do not involve a personal data breach.

For details on responding to cyber incidents and providing data breach notification, including interacting with Germany's computer emergency response team (CERT) resources, see Practice Note, Cyber Incident Response and Data Breach Notification (Germany).

Cybersecurity Information Sharing

Germany supports public-private partnerships for cybersecurity information sharing through the BSI, including:

- The Alliance for Cyber Security (in German), which provides:
  - a nationwide cooperative platform for sharing information regarding cyber threats and attack response;
  - general cybersecurity information and research; and
  - training and industry-focused activities.
- UP KRITIS (in German), which focuses on critical infrastructure protection and includes sector-specific working groups that assist in developing standards under the BSIG.

The BSI shares information on identified cybersecurity vulnerabilities and cyberattack trends with interested organizations and the public on its website.

Enforcement and Litigation

Regulatory Enforcement

Competent regulators have authority to assess and audit organizations' facilities, including the organizational and technical measures they take to protect information and IT systems.

Data Protection Authorities

German state data protection authorities (state DPAs) monitor BDSG and GDPR compliance, including the collection, processing, and use of personal data by public and private organizations. The DPA for the jurisdiction in which relevant activities take place is generally responsible for investigation and enforcement. State DPAs can initiate investigations on their own or in response to an individual's complaint.

State DPAs have the authority to:

- Issue cease orders to resolve irregularities.
- Impose fines.
- Limit the use of particular data processing procedures.
- Prohibit personal data collection, processing, or use.

(Article 58(2), GDPR.)

For more on state DPAs, including data breach reporting information, see Practice Note, Cyber Incident Response and Data Breach Notification (Germany): Data Protection Authorities).

The Federal Commissioner for Data Protection and Freedom of Information (BfDI) monitors personal data processing by:

- Federal agencies.
- Private organizations subject to the Security Screening Act (in German), which establishes procedures for security clearances related to national security, defense, and other sensitive activities.
- Some other private organizations, including telecommunications and postal services providers.

Like the state DPAs, the BfDI's office can initiate investigations on its own or in response to an individual's complaint. The BfDI is also responsible for overseeing data processing in the telecommunications and telemedia sector, including imposing fines for failure to implement certain security measures (Sections 28(1)(10) and 29(1), TTDSG).

The GDPR imposes potential administrative fines for failure to provide appropriate security measures under Article 32 of up to EUR10 million or 2% of the organization’s annual global turnover (Article 83(4), GDPR).

BSI and Other Agencies

The BSI and the Federal Network Agency enforce the BSIG and the TKG and can impose fines on operators of essential services, including telecommunications providers, that fail to:

- Provide appropriate notifications (see Cyber Incident Response and Data Breach Notification).
- Meet periodic program review and certification standards (see Program Review and Certification).

Private Actions

Affected individuals can bring tort actions or claim injunctive relief against public and private organizations that fail to adopt adequate data security measures as required by the BDSG (Section 823, German Civil Code). For example, the Federal Court of Justice ruled that press organizations may be liable to private individuals for damages that result from insufficient data security measures (Federal Court of Justice Apr. 4, 2010, no. VI ZR 245/08, recital 24).

The GDPR and BDSG provide data subjects with a private right of action against organizations that violate data protection law (Article 79, GDPR; Section 44(1), BDSG).

Organizations that protect and enforce consumers' interests may also bring claims against those who violate the BDSG's data protection requirements, under limited circumstances supported by the Unfair Terms and Conditions Act (in German) (UKlaG) (Section 2(2)(11), UKlaG). These rights and actions typically affect obligations related to consumer notices, consent, and whether the organization has a legitimate basis for data processing. They do not generally extend to information security-related issues.

However, an organization's false claim about the adoption of data security measures in its terms of service may be a crime under Section 16(1) of the Act Against Unfair Competition (UWG). False claims can also violate Section 5 of the UWG, which forbids misleading commercial practices. Consumer protection agencies may bring claims against the organization for Section 5 violations.

Protecting Sensitive Information Security Records

Organizations should exercise caution and protect from unnecessary disclosure sensitive information security analyses, such as risk assessments and cyber incident investigations, where possible. The attorney confidentiality obligation and the secrecy of communications may protect sensitive information security records. However, there is no work-product doctrine in Germany.

German law generally protects communication between lawyers and their clients under the professional confidentiality obligations of the Federal Lawyers' Act (BRAO) (Section 43a(2), BRAO). This professional confidentiality obligation allows attorneys to withhold information from prosecutors and protects the attorney's files from government access. However, attorney confidentiality does not generally extend to documents held by a client, except in some criminal investigation circumstances.

Public authorities may access records under certain circumstances, where sensitive information security records do not fall under these legal protections. For example, the German Federal Criminal Office may access IT systems without knowledge of the system's owner if there are indications of a danger for very important legally protected rights such as the life of a person (Section 20k, Federal Criminal Office Act). The police may also confiscate security records if they are of evidentiary relevance in a criminal investigation (Section 94, Criminal Procedure Act).

END OF DOCUMENT

