

Information Security Considerations (Germany)

PAUL VOIGT, TAYLOR WESSING PARTG MBB, WITH PRACTICAL LAW DATA PRIVACY ADVISOR

Search the [Resource ID numbers in blue](#) on Westlaw for more.

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 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, including the Data Protection Adaptation and Implementation Act (Datenschutz-Anpassungs- und Umsetzungsgesetz EU) (DSAnpUG-EU) and the NIS Directive Implementation Act (NIS-Richtlinien-Umsetzungsgesetz). It also discusses critical infrastructure issues and Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) (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 ([W-003-1855](#)).

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 ([W-003-1855](#)).

INFORMATION SECURITY LAWS AND REGULATIONS

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

- The Federal Data Protection Act (*Bundesdatenschutzgesetz*) (BDSG), which protects personal data. Germany updated the Act to align with the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), effective May 25, 2018 (see GDPR and the BDSG).
- The IT Security Act (*IT-Sicherheitsgesetz*) (in German) (IT-SiG), which affects telemedia services, including websites, social media, and other online services, telecommunications, and other critical infrastructure sectors. Germany updated this Act when it transposed the EU Directive on the Security of Network and Information Systems (Directive 2016/1148/EC) (NIS Directive) into German law (see IT-SiG and NIS Directive Implementation). A first draft bill for the IT Security Act 2.0 is under consideration.
- 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 (*Gesetz betreffend die Gesellschaften mit beschränkter Haftung*) (in German) (GmbHG)).

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 (*Datenschutz-Anpassungs- und Umsetzungsgesetz EU*) (DSAnpUG-EU) to update the BDSG and align it with the GDPR. The updated BDSG provisions applied on the GDPR's effective date.

For more information on the BDSG's general requirements, see Country Q&A, Data protection in Germany: overview ([3-502-4080](#)).

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 updated BDSG provisions under the DSAnpUG-EU contain some GDPR-permitted derogations, for example, relating to exceptions from:

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

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 45-84, BDSG and Recital 19, GDPR).

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 ([W-007-9580](#)). For more details on anonymization and pseudonymization as information security controls, see Practice Note, Anonymization and Pseudonymization Under the GDPR ([W-007-4624](#)).

IT-SiG AND NIS DIRECTIVE IMPLEMENTATION

The Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*) (BSI) in the Federal Ministry of the Interior acts as Germany's national cybersecurity authority, under the BSI Act of 2009 (*BSI-Gesetz*) (BSIG), as amended by the IT-SiG. Germany updated the BSIG in mid-2017 to transpose the NIS Directive into German law under the NIS Directive Implementation Act (*NIS-Richtlinien-Umsetzungsgesetz*).

These laws:

- Apply minimum information security standards to critical infrastructure (see Critical Infrastructure).
- Update information security-related obligations under several German sector-specific laws, including those that apply to public websites and social media (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 which are important to Germany because a loss of their operation may lead to significant supply shortages or endanger national security. The NIS Directive lays 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.)
- Essential services operators 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.)

Under the NIS Directive, operators of essential services and digital service providers 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; Section 8a(1), BSIg).

German law further requires critical infrastructure providers, including essential service operators, 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).
 - Every two years demonstrate to the BSI that their facilities meet IT-SiG requirements (see Program Review and Certification).

BSI-Kritis regulations (*BSI-Kritisverordnungen*) further implement the IT-SiG'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 (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe*) (BBK).

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).

For more details on the NIS Directive and its requirements, see Practice Note, EU NIS Directive Implementation Activities: Overview ([W-013-2158](#)).

Sector-Specific Requirements

The IT-SiG updates information security-related obligations under several German sector-specific laws, including those that apply to:

- **Telemedia services operators.** The Telemedia Act (*Telemediengesetz*) (in German) (TMG) includes public websites, social media, and other online services. Under the updated TMG, operators must implement technologically feasible and economically reasonable data security measures, such as encryption, regular software updates, and vendor management, to:
 - ensure that no unauthorized access to the services is possible; and
 - protect the services from attacks that could result in service interruptions.
 - (Section 13(7), TMG.)
- **Telecommunications providers.** The Telecommunications Act (*Telekommunikationsgesetz*) (in German) (TKG) regulates providers of telecommunications facilities and services. Under the TKG, providers must:

- implement appropriate technological measures to protect against service interruptions and manage security risks (Section 109(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 ([W-003-4711](#))).

- **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. The Federal Network Agency (*Bundesnetzagentur*) and BSI together support standards for documenting and implementing these and related information security requirements.

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 (*Aktiengesetz*) (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 (*Gesetz zum Schutz von Geschäftsgeheimnissen*) (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-Grundschrift can apply for internationally-recognized ISO/IEC 27001 certification.

The BSI modernized the IT-Grundschrift 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 to small and medium-sized enterprises;
 - core protection, which expands 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.
- 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-Grundschrift methodology, other selected BSI standards, and related publications are available in English 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-Grundschrift 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 ([W-003-1855](#)).

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 as a rule at least ten persons dealing 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 IT-SiG requires 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:
 - critical infrastructure operators; and
 - telemedia services operators, including public websites, social media, and other online services.
- (For more information on IT-SiG requirements, see IT-SiG and NIS Directive Implementation.)
- **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 IT-SiG and NIS Directive Implementation). 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 (*Betriebsverfassungsgesetz*) (in German) (BetrVG) 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-virus 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 data protection authorities generally question consent as a legal basis in the employment context. For more information on employee monitoring issues, see Practice Note, Employee Monitoring: Germany ([W-008-3362](#)).

- **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 IT-SiG:
 - requires critical infrastructure operators to use state-of-the-art technology;
 - calls on telemedia services operators to prevent unauthorized access and service interruptions; and
 - encourages industry groups to develop sector-specific security standards.
- (For more information on IT-SiG requirements, see IT-SiG and NIS Directive Implementation.)

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.

Under the BSIG, critical infrastructure operators:

- Must every two years demonstrate to the BSI that their facilities meet BSIG requirements through audits, examinations, or certifications (Section 8a(3), BSIG (as amended by the IT-SiG)).
- Are subject to fines of up to EUR50,000 for failures (Section 14, BSIG (as amended by the IT-SiG)).

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 critical infrastructure providers, typically include incident response planning.
- The Article 29 Working Party (now the European Data Protection Board (EDPB)) 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)) ([W-004-5781](#)).

The GDPR requires notification to affected individuals and authorities for applicable breaches of personal data. Some organizations, including certain critical infrastructure 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) ([W-006-9022](#)).

CYBERSECURITY INFORMATION SHARING

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

- The Alliance for Cyber Security, 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, which focuses on critical infrastructure protection and includes sector-specific working groups that assist in developing standards under the IT-SiG.

The BSI shares information on identified cybersecurity vulnerabilities and malicious software (malware) trends with interested organizations and the public on its website. The BSI also describes and analyzes the causes and methods of current cyberattacks in its annual State of IT Security in Germany report.

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

Data protection authorities (DPAs) in each German state (*Landesdatenschutzbehörden*) monitor BDSG and GDPR compliance, including the collection, processing, and use of personal data by

public and private organizations. The DPA for the state 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.)

The Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) (BfDI) monitors personal data processing by:

- Federal agencies.
- Private organizations subject to the Security Screening Act (*Sicherheitsüberprüfungsgesetz*) (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 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 IT-SiG and NIS Directive Implementation Act and can impose fines on critical infrastructure operators, 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).

Different state authorities in Germany may impose fines on telemedia services providers that fail to implement technologically feasible and economically reasonable data security measures (Section 16 (2)(3), TMG). The competent state authority varies from state to state and depends on the distribution of responsibilities undertaken by each state government. For example, the Bavarian State Agency for Data Protection is responsible for imposing fines on telemedia service providers.

If the state government has not otherwise distributed responsibilities, the highest state authority for fine proceedings of the district in which the offense was committed, discovered, or in which the offender resides can impose fines (Sections 36 (1)(2)(a) and 37(1), Administrative Offences Act (*Ordnungswidrigkeitengesetz*) (OWiG)). Regulators can fine operators of public websites, social media, and other online services up to EUR50,000 (Section 16(3), TMG).

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 (*Bürgerliches Gesetzbuch*) (BGB)). 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 (*Bundesgerichtshof* (BGH) Federal Court of Justice Apr. 4, 2010, no. VI ZR 245/08, recital 24).

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

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 (*Unterlassungsklagengesetz*) (in German) (UKlaG) (Section 2(1)(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 (*Gesetz gegen den unlauteren Wettbewerb*) (UWG). False claims can also violate UWG, Section 5 that 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 (*Bundesrechtsanwaltsordnung*) (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 (*Bundeskriminalamtgesetz*) (BKAG)). The police may also confiscate security records if they are of evidentiary relevance in a criminal investigation (Section 94, Criminal Procedure Act (*Strafprozessordnung*) (StPO)).

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at legalsolutions.com/practical-law. For more information or to schedule training, call **1-800-733-2889** or e-mail referenceattorneys@tr.com.