A Practice Note addressing legal requirements and considerations when handling data breaches, cyber attacks, or other information security incidents in Germany or drafting data breach response notifications regarding personal data originating from Germany. It discusses the Federal Data Protection Act (Bundesdatenschutzgesetz) (BDSG) and critical infrastructure provider obligations under the IT Security Act (IT-Sicherheitsgesetz) (IT-SiG). It also addresses recent changes in EU law, such as the General Data Protection Regulation (GDPR), the Directive on the Security of Network and Information Systems (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). The Germany-specific guidance in this Note may be used with the generally applicable resources in the Global Cyber Incident Response and Data Breach Notification Toolkit (W-010-2382).

DATA BREACH NOTIFICATION

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) replaces the EU Data Protection Directive (Directive 95/46/EC) and applies in all member states beginning on May 25, 2018. Germany enacted the Data Protection Adaptation and Implementation Act (Datenschutz-Anpassungs- und Umsetzungsgesetz EU) (DSAnpUG-EU) in mid-2017 to update its Federal Data Protection Act (Bundesdatenschutzgesetz) (BDSG) and align it with the GDPR. The updated BDSG provisions apply on the GDPR’s effective date.

For more details on the BDSC’s general data protection requirements, see Country Q&A, Data protection in Germany: overview (3-502-4080).

DATA BREACH NOTIFICATION UNDER THE GDPR

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 special rules that apply to processing sensitive personal data, which includes:
- 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(f), GDPR.)

The updated BDSG provisions under the DSAnpUG-EU contain some GDPR-permitted derogations, for example, relating to data breach notification by public bodies (Sections 45, 56(2), and 66(5), BDSG and Article 23, GDPR).

When analyzing and responding to a data breach affecting personal data in Germany on or after the GDPR’s effective date, organizations should consider whether:
- The event triggers GDPR notification requirements (see Triggering Events Under the GDPR).
- The GDPR requires notice to:
  - regulatory authorities (see Notification to Authorities Under the GDPR); and
  - affected individuals (see Notification to Affected Individuals Under the GDPR).
- They are subject to additional sector-specific requirements (see Sector-Specific Notification Requirements).

**Triggering Events Under the GDPR**

The GDPR defines a data breach as a compromise of personal data transmitted, stored, or otherwise processed, through:
- Accidental or unlawful destruction, loss, or alteration.
- Unauthorized disclosure or access.

(Article 4(12), GDPR.)

Data controllers must notify:
- The applicable data protection authority within 72 hours, including specific details, unless the breach is unlikely to result in risk to individuals’ rights (Article 33, GDPR; see Notification to Authorities Under the GDPR).
- Affected individuals without undue delay, if the breach is likely to result in high risk to individuals’ rights, with some exceptions (Article 34, GDPR; see Notification to Affected Individuals Under the GDPR).

Data processors must notify affected controllers without undue delay when they become aware of a data breach (Article 33(2), GDPR.)

The European Data Protection Board (EDPB, formerly the Article 29 Working Party), composed of EU member states’ data protection authorities and the European Data Protection Supervisor, provides further guidance on triggering events and notification obligations in its Guidelines on Personal data breach notification under Regulation 2016/679 (WP29 Breach Guidelines).

**Notification to Authorities Under the GDPR**

The GDPR requires data controllers to notify their supervisory data protection authority:
- Without undue delay.
- Where feasible, within 72 hours of becoming aware of a personal data breach.

Data controllers need not notify authorities if the data breach is unlikely to result in risk to affected individuals’ rights and freedoms. Organizations that do not meet the 72-hour deadline must explain their delay when providing notification. (Article 33 (1), GDPR.)

Notifications to authorities should:
- Describe the personal data breach, including, if possible:
  - the categories and approximate number of affected individuals; and
  - the types and quantity of affected personal data.
- Include the name and contact information for the organization’s data protection officer or other contact point.
- Describe the data breach’s likely consequences.
- Explain any measures the data controller has taken or proposes to take to address the data breach and mitigate its possible adverse effects.

(Article 33(3), GDPR.)

Organizations:
- Can provide the required notification information to authorities in phases, as necessary (Article 33(4), GDPR).
- Must document personal data breaches to enable their supervisory authority to verify compliance with the GDPR’s requirements, including details for each breach, such as:
  - the facts relating to each data breach;
  - its effects; and
  - the organization’s remedial actions.

(Article 33(5), GDPR.)

The updated BDSG provisions under the DSAnpUG-EU call for data breach notification to the responsible State Commissioner for Data Protection and Freedom of Information (Landesbeauftragter für den Datenschutz und die Informationsfreiheit). However:
- If the organization has more than one establishment in Germany, the GDPR’s definition regarding main establishment applies to determine which supervisory authority is competent (Article 4(16), GDPR and Section 40(2), BDSG).
- Organizations that engage in cross-border processing, which includes processing personal data for individuals in multiple EU member states, should provide data breach notice to their lead supervisory authority under the GDPR (Articles 4(23) and 56(6), GDPR).

Accordingly, organizations that engage in cross-border processing should provide notice to the German authorities if they have identified Germany as their lead supervisory authority, for example,
because their EU main establishment is in Germany. The WP29 Breach Guidelines provide additional guidance on notifying authorities of cross-border data breaches.

**Notification to Affected Individuals Under the GDPR**
The GDPR requires data controllers to notify affected individuals without undue delay, if the data breach is likely to result in high risk to individuals’ rights and freedoms. The notification to individuals should:
- Describe the personal data breach in clear and plain language.
- Include at least the information the organization provided in its notification to authorities.
(Article 34, GDPR.)

Data controllers need not notify affected individuals if:
- They applied appropriate security measures, such as encryption, to the affected personal data and those measures rendered it unintelligible to unauthorized parties.
- They subsequently took measures to avoid the high risk to individuals’ rights and freedoms.
- Individual notification would involve disproportionate effort (see Substitute Notification Under the GDPR).
(Article 34(3), GDPR.)

The data controller’s supervisory authority can compel notification to affected individuals, after considering the likelihood of high risk to individuals’ rights and freedoms (Article 34(4), GDPR). The WP29 Breach Guidelines provide further guidance on the risk analysis for data controllers and notifying affected individuals.

The GDPR permits member states to limit data breach notification for affected individuals to safeguard certain public interests such as law enforcement and national security and defense (Article 23, GDPR). However, the updated BDSG provisions under the DSAnpUG-EU only allow certain public bodies to delay or skip their notifications to affected individuals:
- If necessary to protect certain law enforcement and public security interests or a third parties’ legal interests.
- Unless the affected individuals’ interests outweigh those of the controller.
(Sections 45, 56(2), and 66(5), BDSG (as amended by the DSAnpUG-EU).)

**Substitute Notification Under the GDPR**
Data controllers may use substitute notification, under the GDPR, if individual notifications would require a disproportionate effort. Data controllers in these circumstances should use a public communication or similar measure to inform affected individuals in an equally effective manner. (Article 34(3)(c), GDPR.)

**Penalties Under the GDPR**
The GDPR imposes potential administrative fines for failure to provide appropriate security measures or required data breach notification of up to EUR10 million or 2% of the organization’s annual global turnover (Article 83(4), GDPR).

**SECTOR-SPECIFIC NOTIFICATION REQUIREMENTS**
Some companies must also abide by the notification requirements found within sector-specific laws. These include:
- **Telecommunications Providers.** Under the Telecommunications Act (Telekommunikationsgesetz) (TKG), notification obligations are triggered when a data breach involves:
  - customer usage data, such as user identification data or traffic data; or
  - customer contract data, such as subscriber registration data.
  (Section 109a, TKG.)
- **Website and Telemedia Providers.** Under the Telemedia Act (Telemediengesetz) (TMG), website and telemedia providers must notify affected individuals of a data breach when there is a high likelihood of unauthorized access to:
  - contractual user data, including personal data necessary for the formation, organization, or amendment of the contractual relationship, such as name and email address; or
  - usage data, including all personal data required to provide services to the user, such as IP addresses.
  (Section 15, TMG.)
These forms of data likely fall under the GDPR’s broad definition of personal data (see Data Breach Notification Under the GDPR), creating potentially overlapping obligations.

**OTHER CYBER INCIDENT NOTIFICATION REQUIREMENTS**
The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) (BSI) within 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 Security Act (IT-Sicherheitsgesetz) (IT-SiG).

**CYBER INCIDENT NOTIFICATION UNDER THE NIS Directive**
- Digital service providers that offer certain information society services, including:
  - online marketplaces;
  - online search engines; and
  - cloud computing services.
  (Article 4(6), NIS Directive.)
- Essential services operators across various critical infrastructure sectors, including:
  - Energy.
  - Transportation.
  - Banking and financial market infrastructures.
  - Health care.
Cyber Incident Response and Data Breach Notification: Germany

- Water.
- Digital infrastructure.
  - (Article 4(4), NIS Directive.)

For more details on the NIS Directive and its requirements, see Practice Note, EU NIS Directive Implementation Activities: Overview (W-013-2158). For more information on security requirements in Germany, see Practice Note, Information Security Considerations: Germany (W-006-6878).

TRIGGERING EVENTS FOR CYBER INCIDENT NOTIFICATION

Critical infrastructure providers must immediately report to the BSI events that both:
- Are significant disturbances in the availability, integrity, authenticity, or confidentiality of their IT systems.
- Have led or could lead to a failure or compromise in critical infrastructure operations.
  (Section 8b(4), BSIG.)

As of May 10, 2018, digital service providers also must immediately report to the BSI significant cybersecurity incidents, considering:
- The number of affected users.
- The incident’s duration.
- The affected geographical area.
- The extent of the service interruption and its impact on economic and societal activities.
  (Sections 8c(3) and 15, BSIG.)

NOTICE TO AUTHORITIES OF CYBER INCIDENT

Critical infrastructure and digital service providers must provide the BSI with the following information for triggering cyber incidents:
- The affected critical infrastructure sector.
- The type of disruption.
- The presumed or known cause of the disruption.
- The surrounding technological conditions and affected information technology.
- The type of affected facility or site.
  (Section 8b(4), BSIG.)

Energy supply providers and nuclear power providers, including organizations that provide, store, process, or otherwise use nuclear power, must also provide the BSI with the type of information technology affected by the disruption (Section 44b, German Nuclear Act).

PENALTIES

The BSI can impose fines on critical infrastructure providers of up to EUR50,000 for failing to notify it about disruptions or breakdowns of their services or facilities, including cyber incidents (Section 14(2), BSIG).

ENFORCEMENT AND LITIGATION

German regulatory agencies may take action against organizations that fail to properly or timely notify affected individuals or applicable authorities.

REGULATORY ENFORCEMENT

Failing to comply with notification or incident response requirements may subject a data controller or victimized organization to regulatory actions. Regulatory agencies authorized to take action include:
- The Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit) (BfDI), which enforces the compliant collection, processing, and use of personal data by:
  - federal agencies;
  - telecommunication providers;
  - postal service providers; and
  - private organizations subject to the Security Screening Act (Sicherheitsüberprüfungsgesetz).
- The state-level data protection authorities (Landesdatenschutzbehörden) (state DPAs), which enforce the compliant collection, processing, and use of personal data by private and public organizations at the German state level (Section 40, BDSG) (see Notification to Authorities Under the GDPR).

The BfDI has authority to:
- Receive complaints about data protection violations.
- Issue complaints to public federal authorities that are violate data protection laws and require them to respond within a time period determined by the BfDI.
- Notify supervisory authorities for complaints directed to public corporations, public agencies, and public foundations.
- Obtain information from and inspect federal public authorities.

The BfDI also accepts data breach notifications from data subjects who believe that the processing of personal data by public bodies infringes their rights (Section 60(1), BDSG) (see Notification to Authorities Under the GDPR).

The state DPAs have authority to:
- Monitor private organizations’ compliance with the GDPR and BDSG.
- Receive complaints about data protection violations, as the generally responsible data protection authority.
- Order suspension of business operations.
- Order closure or cancellation of the file, register, or database that processes personal data.
- Seize equipment.
- Oversee private actions, civil actions, class actions, or criminal prosecution.
- Impose administrative fines, penalties, or sanctions.
- Audit or investigate the organization.

The data protection authorities can enforce their orders. However, data controllers can bring court actions against the data protection authorities if they consider their enforcement actions unlawful.
PRIVATE ACTIONS

Data subjects who suffer damage caused by processing personal data in violation of the BDSG or other applicable law can demand compensation from the controller (Section 83, BDSG).

Affected individuals can file with Public Prosecutors (see Public Prosecutors) a complaint against public or private organizations that fail to protect personal data or to provide notification if a data breach occurs (see Data Breach Notification).

Individuals can also file a complaint with the BfDI or state DPAs (Sections 40 and 60(1), BDSG).

GETTING HELP WITH CYBER INCIDENT RESPONSE

Germany supports public-private partnerships and various computer emergency response team (CERT) resources to coordinate cyber incident response and help organizations recognize, respond, and recover from cyber attacks.

Some notable resources include:

- The National Cyber Response Centre, which reports to the BSI and supports cross-agency cooperation and response to cyber incidents across law enforcement, military, and intelligence agencies.
- The federal CERT-Bund (in German), which also reports to the BSI and provides services primarily available to federal agencies, such as:
  - a 24-hour available emergency hotline;
  - incident report analysis and recommendations; and
  - cybersecurity information sharing services, including vulnerability and threat alerts.
- The public Bürger-CERT (in German), which provides the public, including consumers and small businesses or others with less sophisticated cybersecurity programs, cost-free information and guidance on:
  - current cyber attack and malicious software (malware) trends; and
  - known cyber vulnerabilities and threats.
- The CERT-Verbund (in German), which is an association of private CERTs and other interested parties, including security researchers.

The BSI also supports industry standards for information security and cybersecurity information sharing initiatives. For more details on information security and resources for preventing data breaches and other cyber incidents in Germany, see Practice Note, Information Security Considerations: Germany (W-006-6878).

REPORTING CYBER ATTACKS AND CYBER CRIME

DATA PROTECTION AUTHORITIES

State DPAs monitor the compliant collection, processing, and use of personal data by private and public organizations at the German state level (see Regulatory Enforcement). State DPAs also:

- Accept reports about possible data protection violations, including missing or incomplete data breach notification, cyber attacks, and cyber crimes.
- Initiate proceedings if there is a suspicion of a data protection violation.

PUBLIC PROSECUTORS

Cyber attacks are often crimes. Victimized organizations should consider reporting and assisting law enforcement in investigating cyber attacks. Organizations that experience cyber crime may file a complaint with the Public Prosecutor (Staatsanwaltschaft).

Typical cyber crimes include:

- Data espionage (Section 202a, German Criminal Code (Strafgesetzbuch) (StGB)).
- Phishing (Section 202b, StGB).
- Acts preparatory to data espionage and phishing (Section 202c, StGB).
- Violation of the postal and telecommunications secret (Section 206, StGB).
- Computer fraud (Section 263a, StGB).
- Data tampering (Section 303a, StGB).
- Computer sabotage (Section 303b, StGB).