Cyber Incident Response and Data Breach Notification (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 addressing legal requirements and considerations when handling data breaches, cyberattacks, 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 (BDSG) and critical infrastructure provider obligations under the IT Security Act and IT Security Act 2.0. It also 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. 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.

Data breaches, cyberattacks, and other information security incidents are increasingly common across sectors and affect a wide range of large and small organizations. In response, data breach notification laws, regulations, and best practices raise significant challenges for global companies. This Practice Note explains the German laws and regulations an organization must consider and the local resources available when handling data breaches of personal data originating from Germany.

Cyber incidents occur when events compromise the security, confidentiality, integrity, or availability of an information technology (IT) system, network, or data. Reporting and notification obligations vary according to a cyber incident's characteristics. For example:

- Data breach notification obligations may apply if the event exposes personal information to potential unauthorized access or use.
- Other cyber incident notification requirements may apply if the event affects critical infrastructure or regulated entities.

Some cyber incidents result from criminal activities. Victimized organizations should consider reporting cybercrime to applicable authorities. 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.

Data Breach Notification

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) replaced the EU Data Protection Directive (Directive 95/46/EC) and 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 its Federal Data Protection Act (BDSG), align it with the GDPR, and make conforming changes to other laws.

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

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 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 provisions that regulate data protection outside the GDPR's scope of application, for example, relating to data breach notification by public bodies responsible for addressing criminal or administrative offenses (Sections 45, 56(2), and 66(5), BDSG; Recital 19, GDPR).

When analyzing and responding to a data breach affecting personal data in Germany, 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); or
    - affected individuals (see Notification to Affected Individuals Under the GDPR).
- They are subject to additional sector-specific requirements (see Sector-Specific Notification Requirements).

Organizations must also document any personal data breaches to enable their supervisory authority to verify compliance with the GDPR's specific requirements and accountability principle, including details, such as:

- The facts relating to each data breach.
- Its effects.
- The organization's remedial actions.

(Articles 5(2) and 33(5), GDPR.)

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.)

Controllers must notify:

- The applicable data protection authority (DPA) in 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), 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 the GDPR (WP250) (Feb. 6, 2018) (EDPB Breach Guidelines).
- Data breach notification examples in its Guidelines on Examples regarding Data Breach Notification (Jan. 14, 2021) (pending public consultation).

Notification to Authorities Under the GDPR

The GDPR requires controllers to notify their supervisory data protection authority:

- Without undue delay.
- Where feasible, in 72 hours of becoming aware of a personal data breach.

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 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).

The BDSG calls for data breach notification to the responsible supervisory authority from the German state DPAs (for a list of state DPAs, see Data Protection Authorities). 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 appropriate German DPA if they have identified them as their lead supervisory authority, for example, because their EU main establishment is in that area of Germany. The EDPB Breach Guidelines provide additional guidance on notifying authorities of cross-border data breaches.

Notification to Affected Individuals Under the GDPR

The GDPR requires 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.)

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 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 EDPB Breach Guidelines provide further guidance on the risk analysis for controllers and notifying affected individuals.

The GDPR does not apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties (Recital 19, GDPR). The BDSG contains an applicable notification obligation for data breaches that are likely to result in a substantial risk to the interests of affected individuals (Section 66(1), BDSG).

Substitute Notification Under the GDPR

Controllers may use substitute notification, under the GDPR, if individual notifications would require a disproportionate effort. 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

The 2nd DSAnpUG-EU made GDPR-conforming changes to various laws, generally deferring to the BDSG for data breach notification requirements. However, some companies must also abide by the notification requirements found in sector-specific laws.

For example:

- Under the revised Telecommunications Act (in German) (TKG), which comes into force on December 1, 2021:
    - telecommunications providers must also notify the Federal Network Agency when a data breach involves either customer usage data, such as user identification data or traffic data, or customer contract data, such as subscriber registration data; and
    - the Federal Network Agency has authority to require notifications to affected individuals and investigate, like the state DPAs' BDSG authority.

    (Section 169, TKG.)
- The Energy Industry Act (in German) (EnWG) imposes specific notification requirements on operators of essential services in the energy sector. These operators must notify the Federal Office for Information Security (BSI) of any cyber incidents, including data breaches, that could actually or potentially lead to the disruption or the substantial impairment of the energy supply network or of the relevant energy facility. (Section 11(1c), EnWG).
- Specific notification requirements also apply under the German Nuclear Act (AtG) that:
    - covers most nuclear power providers; and
    - requires prompt notification to the BSI of any data incident which may cause or has already caused a disruption that risks the nuclear safety of the operator's facility.

    (Section 44b, AtG.)
- The Patient Data Protection Act (in German) (PDSG), enacted in 2020, updated the Social Code Book Five (in German) (SGB V) to require certain health care providers that use specified IT services, such as the digital health card, to:
    - report data breaches related to Germany's centralized health care information technology infrastructure to the Association of Telematics; and
    - if applicable, notify the Federal Office for Information Security (BSI) and the Ministry of Health.

(Section 329, SGB V and Article 1(31), PDSG.)

For more on the BSI and operators of essential services' data breach and cyber incident notification obligations, see Other Cyber Incident Notification Requirements.

Other Cyber Incident Notification Requirements

The Federal Office for Information Security (BSI) acts as Germany's national cybersecurity authority, under the BSI Act of 2009 (BSIG), as amended by the IT Security Act and IT Security Act 2.0 (both in German).

Cyber Incident Notification Under the NIS Directive and the BSIG

Germany updated the BSIG in mid-2017 to transpose 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. 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.)
- 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.)

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. For more information on security requirements in Germany, see Practice Note, Information Security Considerations (Germany).

The IT Security Act and IT Security Act 2.0 expanded the critical infrastructure sectors to include:

- Information technology and telecommunications, including digital infrastructure.
- Insurance, in addition to banking and financial services.
- Municipal waste disposal.
- Nutrition

(Section 2(10), BSIG.)

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.)

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.

(Section 8c(3), BSIG.)

The BSIG contains an exception for digital service providers that do not have sufficient access to the information required to assess the impact of a security incident (Section 8c(3), BSIG).

Certain companies that are not necessarily critical infrastructure providers but are important to the public interest due to their critical infrastructure supply chain role, other economic impact factors, or hazardous material handling must similarly report any disruptions to their IT systems, components, or processes that significantly impair their services. The report must contain information on the suspected or actual cause of the disruption, the affected information technology, and type of facility involved. (Sections 2(13), 2(14), and 8f(7), 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 type of disruption.
- Possible cross-border effects.
- The surrounding technological conditions and affected information technology.
- The presumed or known cause of the disruption.
- The type of affected facility or site.
- The affected critical infrastructure sector and the effects of the disruption on those services.

(Sections 8b(4) and 8c(3), BSIG.)

Penalties

The BSI can impose fines on critical infrastructure providers of up to EUR500,000 for failing to notify it about disruptions or breakdowns of their services or facilities, including cyber incidents (Section 14(5), BSIG).

Enforcement and Litigation

German regulatory agencies may potentially have the right to 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 controller or victimized organization to regulatory actions. Regulatory agencies authorized to take action include:

- The Federal Commissioner for Data Protection and Freedom of Information (BfDI), which enforces the compliant collection, processing, and use of personal data by:
  - federal authorities;
  - telecommunication providers;
  - postal service providers; and
  - private organizations subject to the Security Screening Act (in German).
- The 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 violate data protection laws and require them to respond in a time period determined by the BfDI.
- Notify other 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 supervisory 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 state DPAs can enforce their orders. However, controllers can bring court actions against the DPAs if they consider their enforcement actions unlawful.

Private Actions

Data subjects who suffer material or non-material damage resulting from a GDPR infringement have the right to receive compensation from the controller or processor for the damage suffered (Article 82(1), GDPR).

Data subjects who suffer damage resulting from violations of the BDSG or other applicable law by public bodies responsible for addressing criminal or administrative offenses 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 cyberattacks.

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 cyberattack 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).

Reporting Cyberattacks and Cybercrime

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, cyberattacks, and cybercrimes.
- Initiate proceedings if there is a suspicion of a data protection violation.

All state DPAs provide websites for reporting data breaches, including:

- Baden-Württemberg.
- Bavaria.

- Berlin.
- Brandenburg.
- Bremen.
- Hamburg.
- Hesse.
- Lower Saxony.
- Mecklenburg-Western Pomerania.
- North Rhine-Westphalia.
- Rhineland-Palatinate.
- Saarland.
- Saxony.
- Saxony-Anhalt.
- Schleswig-Holstein.
- Thuringia.

(All links in German.)

Public Prosecutors

Cyberattacks are often crimes. Victimized organizations should consider reporting and assisting law enforcement in investigating cyberattacks. Organizations that experience cybercrime may file a complaint with the Public Prosecutor.

Typical cybercrimes include:

- Data espionage (Section 202a, German Criminal Code (in German) (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).

END OF DOCUMENT

