# Employee Data Privacy – Germany

## Security Requirements

### What security obligations are imposed on data controllers and data processors?

Security requirements may not always be included in the data protection law, but are key to guaranteeing lawful processing of personal data. The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, prevent alteration, corruption or access by unauthorized third parties.

Appropriate technical and organizational measures should be implemented to ensure a level of security appropriate to the risk.

Employers in Germany should follow the general security standards listed in Article 32 of the General Data Protection Regulation. When protecting employee and applicant data, consider the sensitivity of the information, the technology available, the expense of protecting the data and the risk to individuals if the data is compromised. Then take organizational and technological measures, including:

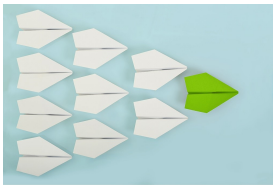
- pseudonymization/encryption;
- measures to ensure the confidentiality, integrity, availability and resilience of information processing systems
- measures to restore the system and access in case of an incident (such as a power outage)
- processes to regularly test and assess the system to ensure continued security.

In addition, Germany's Federal Data Protection Act allows health and medical data to be processed (where allowed) without the consent of the data subject, provided that the employer implements security protections, including:

- internal policies regulating secondary uses;
- appointing a Data Protection Officer;
- employee training;
- access controls;
- logging and monitoring;
- encryption/pseudonymization;
- backups and rapid-restore processes; and,
- regular security self-audits.

Germany has issued best practices for employers through the "Recommendation for Action on Data Protection in Technically Supported Procedures of Personnel and Budgeting by the German Government." This document includes several recommended security practices including:

- creating an authorization standard that limits access to personal data based on the tasks assigned to the authorized individuals;
- implementing/enforcing appropriate technical and organizational measures to protect confidentiality, integrity, authenticity and auditability of personal data archives;
- documenting archiving procedures including content and technology; and,
- ensuring records that are stored exclusively for the purpose of data protection control, backup or proper operations are not processed for other purposes (especially not for behavioral or performance monitoring).



## HR Best Practices:

Ensure contracts with service providers detail the security and confidentiality measures that will be implemented. In addition, regularly train employees who may have access to personal information, to ensure that they are following all technical and organizational security measures that have been put in place.

Last updated May 2023.