Employee Data Privacy – Germany

Data Privacy Laws and Regulations

What laws apply to the collection and use of individuals' personal information?

Data privacy laws have become more prominent in recent years. As the amount of personal information available online has grown substantially, there has been an enhanced focus on the processing of personal data, as well as the enforcement of such laws.

The EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) went into effect on May 25, 2018 and has become new cornerstone of data protection laws throughout the EU. Organizations in the European Economic Area (EEA) must comply with EU data protection laws when retaining documents containing personal data. The EEA includes the EU countries as well as Norway, Lichtenstein, and Iceland.

National Laws Under the GDPR

Germany was one of the earliest adopters of a national law implementing the GDPR. The Federal Data Protection Act (BDSG) includes guidance on processing personal and sensitive personal information in the employment context, further clarifying the rights of employers and employees.

Under the Law, employers are allowed to process personal data "for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations of employees' representation laid down by law or by collective agreements or other agreements between the employer and staff council (Sub-chapter 2, Section 26-1)." Sensitive personal data may also be processed without consent for employment purposes to comply with legal obligations relating to labor law, social security and social protection law (except in cases where the employee has an overriding legitimate interest).

There are also state data protection laws providing legal requirements for data processing carried out by state-level public authorities or public bodies.

EU Legislative Framework

It is important to understand who is the "data controller" under the EU legislative framework. An organization is a data controller when it determines the purposes and manner in which personal data is processed. "Personal data" refers to "any information relating to an identified or identifiable natural person." That person is considered a "data subject" under the GDPR and may be "identified, directly or indirectly…by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Clearly, a lot of employee-related information collected by employers qualifies as personal data, thereby subjecting European employers to EU data privacy regulations. The employer collecting the employee-related data is the data controller, and every HR solution adopted might be qualified as a sub-processing activity.

Regardless of whether an employer utilizes subcontractors to process information, data management processing principles will still need to be followed. This is because the "processing of personal data" is construed broadly and includes physical and automated procedures, such as:

collecting, recording, organizing, structuring, storing, adapting/altering, retrieving, consulting, using, disclosing by transmission, disseminating, making available, aligning/combining, restricting and erasing/destructing.

Therefore, as controllers of employee personal data collected in the employment context, employers must comply with the following personal data processing principles:

- process personal data fairly and lawfully;
- collect personal data only for specified, explicit, and legitimate purposes;
- collect personal data only to the extent that it is adequate, relevant, and not excessive in relation to the purposes for which it is collected;
- ensure that personal data is accurate and, where necessary, kept up to date; and,
- do not keep personal data in a form that permits identification of individuals for longer than is necessary.

Employers should be able to provide a documented rationale for processing each piece of personal data. Processing can be legally justified if the:

- data subject has unambiguously consented to the processing (under the GDPR, regulators are cognizant that employee consent may not be freely given due to the nature of the employee/employer relationship);
- processing is necessary for the performance of a contract to which the data subject is party;
- processing is necessary for compliance with a legal obligation;
- processing is necessary in order to protect the vital interests of the data subject;
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to which the personal data is disclosed, except where such interests are overridden by the data subject's fundamental rights and freedoms.

If the employee data qualifies as sensitive personal data, then a narrower set of conditions applies. For example, one such condition is that a data subject has given explicit consent to the processing of his/her sensitive personal data. "Sensitive personal data" is the personal data consisting of information about the data subject's racial or ethnic origin; political opinions; religious beliefs or beliefs of a similar nature; trade union membership; physical or mental health or condition; or sexual life.

In addition to the federal regulator, each state has a separate regulator which oversees data protection compliance by private companies (except telecommunications and postal services).

The authority responsible for enforcement of data privacy law and regulations in Germany is the:
Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)
www.bfdi.bund.de

In addition to the federal regulator, each state has a separate regulator which oversees data protection compliance by private companies (except telecommunications and postal services).

Last updated May 2023.