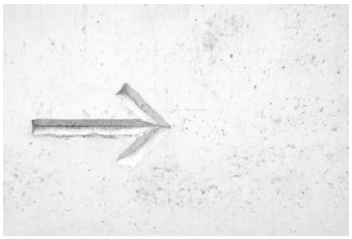
**GDPR Related National Laws & Modifications**

The European Union's General Data Protection Regulation (GDPR) sets a common standard for protecting personal data across the EU. It also allows member nations some flexibility to create additional provisions and limitations.

Some examples, which may impact HR teams, include the ability for EU member states to:

- provide "specific rules to ensure the protection of…employees' personal data in the employment context" (Art. 88);
- limit the transfer of "specific categories of personal data to a third country or international organization" if the country (or international organization) is deemed not to have adequate protections in place (Art. 49, (5)); and,
- "determine the specific conditions for the processing of a national identification number or any other identifier of general application" (Art. 87).



**Derogations in Germany**

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. The Law also outlines when a Data Protection Officer must be appointed.

**Processing Data in the Employment Context**

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). When processing sensitive personal data without the employee's consent, employers should document the data that is being processed along with the reason why the employer's interests outweigh the interests of the employees.

Employee monitoring is only permitted when the employer can document how the employee is believed to have engaged in criminal conduct or committed a serious breach of their employment duties. In addition, the Federal Labour Court holds that the permanent monitoring of employees and monitoring without sufficient grounds is impermissible and evidence gathered during illegal monitoring must not be used in court.

**Consent in the Employment Context**

Employers may use consent in certain cases, but the dependence of the employee will be considered when assessing whether the consent was freely given. One potentially beneficial area for employers is that "[c]onsent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests."

When consent is used, employees must be informed as to why their personal information is being processed and notified that they have the

right to withdraw consent at a later time. These details must be provided in text form (in most cases) to employees and the consent must be given in writing.

**Data Subject Access Rights**

A few data subject rights were restricted in Germany's Federal Data Protection Act, including:

Right of access: If an employee's personal data is only stored to comply with statutory retention provisions, or for the purposes of data backup or monitoring, the access right doesn't apply. The right also doesn't apply in cases where giving access to the employee or individual would reveal confidential data (including private information on third parties or trade secrets). When access requests are refused, the reasons behind the refusal should be documented. Some higher labour courts have a broad understanding of "request for a copy of personal data" under Art. 15 (3) GDPR and have granted copies of records generously (including internal investigation reports).

Right to erasure: The controller (i.e., the employer) is exempted from its obligation to erase personal data where erasure is, in case of non-automatic data processing, impossible, or only possible with disproportionately high effort and the data subject has a minor interest for erasure.

**Employee Personal Data Breach Notification**

The Federal Data Protection Law includes certain exception to providing breach notifications to individuals, including when confidential information would be put at risk by the notification.

**Compensation**

If a data controller causes harm to a data subject by collecting, processing or using the individual's personal data in violation of data protection regulations, the controller must compensate the data subject for the harm caused. There are no punitive damages under German law. The right to claim compensation also applies if the personal data is stored by non-automated procedures or filing systems. This obligation will not apply if the data controller has exercised due care in accordance with the circumstances of the specific case.

**Data Protection Officer (DPO) Requirements**

Germany has additional requirements as to when businesses must appoint DPOs. Under German law, Data Protection Officers must always be appointed when a company processes information subject to a data impact assessment or, when personal data is commercially processed for the purpose of transfer, anonymized transfer or market research. In addition, Germany requires businesses to designate a Data Protection Officer when there are consistently 20 or more employees who routinely process data through automated means. Note that DPOs have protected employment under the BDSG (i.e. DPOs can only be fired when there is evidence that would allow immediate termination for cause).

Last updated April 2021.