Affecting business worldwide

The General Data Protection Regulation – key principles and changes

By Dr. Svenja Fries, LLM

On May 25, 2018, the EU General Data Protection Regulation (GDPR) came into effect. It is intended to harmonize data protection law across the EU, modernize existing laws in light of technological progress, regulate the free movement of personal data within the EU and protect the fundamental rights and freedoms of EU data subjects. In contrast to previous national or EU data protection laws, the GDPR has a renewed focus on accountability, documented compliance processes and enforcement. Although a European regulation, it has extraterritorial effect and will impact businesses worldwide.

Data protection authorities can impose much higher sanctions than before.

Scope of application

The GDPR applies internationally. It covers not only the processing of personal data by establishing a controller or processor in the EU, regardless of whether the processing takes place in the EU, but also organizations outside of the EU insofar as their data processing activities are related either to offering goods or services to EU individuals, or to monitoring their behavior within the EU.

Materially, the GDPR applies to the processing of personal data, which is defined as any information relating to an identified or identifiable natural person. This covers any information from which a specific living individual (the data subject) can be identified, including information that only identifies a person if aggregated with other data held by the respective data controller.

Some special categories of personal data (sensitive data) are more closely protected. This is information that relates to someone's race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health, sex life and sexual orientation, and genetics and biometrics.

Data protection principles under the GDPR

The GDPR provides for seven key principles relating to the processing of personal data:

- Lawfulness, fairness and transparency: Personal data may only be processed where this is permitted and proportionate. To make the processing transparent, the data subject must be informed in clear and plain language that data is being collected, and by whom and how the data will be used.

→

- Purpose limitation: Personal data may only be processed for a specified, explicit and legitimate purpose, and data collected for one purpose shall not be used for a new, incompatible purpose.

- Data minimization: Organizations must not collect any data that is not necessary for their respective processing purposes. This principle limits not only the amount of personal data that can be collected, but also the extent of processing, the period of storage and accessibility.

- Accuracy: Personal data must be accurate and kept up-to-date. Inaccurate data must be amended or deleted, taking into account the purpose for which it has been collected.

- Storage limitation: The period for which the personal data are stored must be limited to a strict minimum. In practice, this requires a regular review process.

- Integrity and confidentiality: Organizations are required to use appropriate technical and organizational measures to ensure protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

The controller (i.e., the person, agency or other body determining the purposes and means of data processing – in an employment law context, this will typically be the employer) is not only responsible for compliance with the abovementioned principles but also for demonstrating said compliance. This new accountability obligation is the most important factor of the increased compliance burden and leads to extensive documentation requirements.

Requirements for lawful data processing

Under the GDPR, the processing of personal data is unlawful unless there is a lawful basis. Such legal base can derive from the GDPR itself, laws and regulations based on the GDPR or the data subject's consent.

The GDPR itself provides for various legal grounds for lawful processing, including but not limited to necessity for the performance of a contract with the data subject, the controller's legal obligations and the pursuit of legitimate interests insofar as they are not outweighed by the data subject's fundamental rights.

In addition, EU Member States may provide for more specific rules for the protection of employee data. These rules can be based both on law and collective agreements. Germany has made use of this option: Under the new Section 26 of the Federal Data Protection Act (*Bundesdatenschutzgesetz, BDSG*), personal data, including sensitive data, can be processed on the basis of collective agreements. Most importantly, this allows for data processing on the basis of collective bargaining agreements and works council agreements. This new Section 26 of the *BDSG* covers all phases of employment, from the application and hiring process to the execution and termination of the employment relationship.

Finally, data processing can be based on the data subject's consent. The GDPR enhances the requirements for valid consent. It needs to be freely given, specific, informed and unambiguous, and it must take the form of an affirmative action or statement. In addition, data subjects have the right to refuse and withdraw their consent at any time.

In principle, consent can also be the legal basis for data processing in an employment situation. However, due to the imbalance of power between employer and employee, it can be questionable whether consent was voluntary: Oftentimes, employees will feel that they have no option but to consent. German lawmakers have recognized this issue and emphasized in the new Section 26 *BDSG* that the validity of an employee's consent needs to be assessed based on the facts of the individual case, taking into account the employee's dependency on his employer. Against this background, organizations should only request and rely on an employee's consent where no other legal basis applies.

Cross-border data transfers

The GDPR's restrictions on cross-border data transfers are similar to the previous legal situation: They may only take place if made to an adequate jurisdiction or if the data exporter has provided appropriate safeguards. Third countries (i.e., non-EEA countries) can be determined as adequate if the European Commission finds that they ensure an adequate level of data protection. Such a decision has been adopted in particular with regard to the EU-US Privacy Shield framework, allowing data transfer to US companies that have self-certified under the Privacy Shield. A transfer to countries lacking this status requires a lawful data transfer mechanism, e.g., the standard contractual clauses adopted by the European →

Commission and binding corporate rules that have been approved by the competent EU data protection authorities.

Rights of data subjects

Under the GDPR, data subjects have the following rights:

- Right of access: Data subjects can receive a copy of the personal data the controller holds about them, and information about, inter alia, the purposes of processing, the categories of personal data concerned and the recipients of the data.
- Right of rectification: Data subjects can request the correction of any incomplete or inaccurate information.
- Right to erasure (right to be forgotten): Data subjects have the right to request the deletion or removal of their personal data if they have been processed unlawfully, are no longer needed for their original or other lawful purpose, or have to be erased for compliance with a legal obligation, or if the data subject has withdrawn his or her consent or exercised his or her right to object to processing.
- Right to object to processing: If the controller relies on public or legitimate interests for processing, the data subject can object to this processing on grounds relating to his or her particular situation.
- Right to restrict processing: Processing needs to be restricted if the data subject contests the accuracy of the data, if the processing is unlawful or if the controller no longer requires the data for their original purpose, but the data subject needs them for the establishment, exercise or defense of legal claims.
- Right of data portability: Data subjects can request a copy of their personal data in a machine-readable format in order to transfer them to another recipient. Where technically feasible, the transfer can also be carried out by the controller directly.

Sanctions

Finally, data protection authorities can impose much higher sanctions than before. Administrative fines for violations of the GDPR can be up to €20 million or 4% of the respective company's worldwide turnover for the preceding financial year, whichever is higher. <–

Dr. Svenja Fries, LLM,
Rechtsanwältin, Associate,
Mayer Brown,
Frankfurt am Main

sfries@mayerbrown.com

www.mayerbrown.com