

## General Data Protection Regulation: Call for action regarding employee data

**As of May 25, 2018 the General Data Protection Regulation (GDPR) will apply. Simultaneously, a new data protection law comes into force in Austria. Thereby, the GDPR is supplemented and implemented in Austria. From this date onwards, new rules apply with respect to the processing of personal employee data. In this context, not only works council agreements play an outstanding role.**

Due to the new data protection rules, protection of employee data must be made a priority within a compliance organization of an company. This is particularly relevant as extraordinarily high penalties may be imposed in case of violations. The GDPR does not provide for further transitional periods which is why May 25, 2018 is to be considered as "deadline" for achieving legal compliance.

### High standards for the lawfulness of data processing

First, companies must observe certain principles when processing employee data, namely the principles of transparency (data processing must be comprehensible for the employees), adherence to a certain purpose (data may only be processed for a certain purpose), data minimization (only such data may be collected which are absolutely necessary) and correctness (data must be maintained in an updated status).

Further, the processing of personal employee data is only legally permissible if certain requirements are met, e.g. in case the data processing is necessary to fulfill legal obligations (e.g. to fulfill the employment contract or tax or social security obligations) or in case vital interests of the employees are protected. Also overweighing interests on part of the company may justify a data processing.

For the processing of sensitive data (e.g. data regarding ethnic affiliation, political opinion, religious belief, world view or trade union membership) even stricter requirements apply under the GDPR.

### Conducting of a processing registry

As of the date the GDPR comes into force, companies must maintain a record of processing activities. Companies with less than 250 employees are excluded from such obligation, but only

- if the processing is not related to special risks (e.g. processing of big data volumes or data of underage employees),
- if the processing only occurs occasionally,
- if no sensitive data is processed.



Such record replaces the currently required notification with the data processing registry.

### **Obligation to report**

In case of a violation of data protection rules, the employer must inform the data protection authority within 72 hours (e.g. in case of a hacker attack or a data leak), if it leads to a risk for the rights and freedoms of employees (e.g. risk of financial loss, loss of data). Further, the employer must inform the employee without delay about the data breach if there is a higher risk.

### **High standards for information obligations**

In future, employers must give employees particularly thorough information about the processing of the data. For example, employees must be informed about the person in charge of controlling the data processing (e.g. the employer), the purpose of the data processing, the legitimate interests for the data processing, the duration of data storage and the employees' right to insist on deleting, rectifying or restrict the data processing. Thereby, fair and transparent processing of data shall be secured. Existing data protection statements and information letters shall therefore be reviewed.

### **Works council agreements**

In many instances, the electronic processing of personal employee data requires a works council agreement. Under the GDPR, such works council agreement must meet certain minimum requirements. This includes reasonable and special measures to protect human dignity as well as justified interests and constitutional rights of employees. In this respect, transparency of data protection plays an important role. A check-up should be based on two questions:

- Do the required works council agreements for the processing of employee data exist at all within the company?
- Do existing works council agreements meet the requirements of the GDPR?

### **Further sensitive areas**

Beside the topics mentioned above, due to the GDPR special attention should be paid to the following areas:

- How long are data of candidates and employees stored?
- Are employees subject to video surveillance?
- How are social media data of employees treated?
- Do employees use smart devices or a home office?
- How are private emails and internet researches of employees treated?

---

For further information, please contact:



Dr. Philipp Maier  
[philipp.maier@bakermckenzie.com](mailto:philipp.maier@bakermckenzie.com)



Dr. Lukas Feiler  
[lukas.feiler@bakermckenzie.com](mailto:lukas.feiler@bakermckenzie.com)



Lisa Jobst  
[lisa.jobst@bakermckenzie.com](mailto:lisa.jobst@bakermckenzie.com)

---

Diwok Hermann Petsche Rechtsanwälte LLP & Co KG ist ein Mitglied von Baker & McKenzie International

**Vienna**  
Schottenring 25  
1010 Vienna  
Tel.: + 43 1 24 250  
Fax: + 43 1 24 250 600

[www.bakermckenzie.com](http://www.bakermckenzie.com)

Get Connected:



This client newsletter is prepared for information purposes only. The information contained therein should not be relied on as legal advice and should, therefore, not be regarded as a substitute for detailed legal advice in the individual case. The advice of a qualified lawyer should always be sought in such cases. In the publishing of this Newsletter, we do not accept any liability in individual cases.

Diwok Hermann Petsche Rechtsanwälte LLP & Co KG is a Member of Baker & McKenzie International, a Verein organized under the laws of Switzerland with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.