SQUIRE PATTON BOGGS

BRING YOUR OWN DEVICE
Considerations for Your Policy

1. Status Quo

Around two thirds of companies worldwide currently allow their employees to use their personal devices for company purposes. Recent statistics estimate that in Germany at least half of the companies allow, or at least tolerate, the use of private devices for corporate use. Bring your own device (BYOD) could be a cost-saving and fast way to introduce innovative, attractive technology within the company. However, it comes along with a lot of security issues and legal problems that need to be considered before sensitive business data is stored on unsecured smartphones or tablets that may become lost in the public domain. HR departments will often support BYOD as a means of motivation and a way to increase productivity, whereas IT departments fear various types of hardware can be difficult to maintain and control. The legal approach to the topic is multifaceted.

2. What Your BYOD Policy Should Cover

2.1 Areas Your Policy Should Cover

In order to avoid data loss, data breaches and uncontrollable document archives, as well as corporate and personal liability, BYOD should be introduced on the basis of a binding policy or an individual agreement reflecting privacy issues, IT security, licensing requirements and employment law, which in some countries – for example, in Germany – can involve difficult co-determination negotiations with the works councils.

2.2 Who Has Access to the Private Device?

The employee should be the only person with access to the device. Preventing any other person with access to the device should avoid an "illegal transfer" within the meaning of sec. 3 par. 4 Federal German Data Protection Act. However, it is advisable to properly reflect the user's typical behavior with respect to their devices, for example, use within a family.

2.3 How to Store and Use Data on Private Devices?

If an employee needs to store company data on a private device, there needs to be written obligations to cover this situation. Furthermore, the specifics of storage should be defined in detail; such as whether the employee is required to store certain apps on their device that are necessary for remote access, security reasons or control. It is advisable to agree on a clear separation between company and private data, and these separation duties need to be duly executed, otherwise the company may find itself in a position where access to the device is contrary to German privacy and employment law. This situation may lead to data deletion obligations – either prescribed by law or contractual obligations – that are not correctly fulfilled. It is therefore advisable to store business data in certain folders or in specially designed areas.

BYOD may also have consequences in regard to software licensing. Private devices will usually have pre-installed software including office packages. Do the underlying licensing agreements allow for business usage? The employer needs be aware of or restrict the usage of certain software for its data.

2.4 Information Duties for the Employee

The employee needs to accept certain duties with regard to the usage of their device, such as neglecting to change the configuration of the device (e.g. refrain from using "jailbreaks") or, first and foremost, giving immediate notice to the employer if the device is lost or seems to be corrupted. Following sec. 42a of the Federal Data Protection Act, in its role as a controller, the employer, on their part, may be obliged to notify the competent data protection authority in case of data loss or data breaches.

2.5 Technical Aspects and Mobile Device Management

Security measures, under German law, should reflect the technical and organizational measures prescribed in Exhibit 9 to sec. 9 of the Federal German Data Protection Act. These measures cover rights to be restricted, the usage of cloud services to be blocked and the installation of apps for securing the availability of company data.

2.6 Costs

Who will pay for telecommunication costs? In principle, the employer is obliged to compensate the employee for work-related telecommunication costs. If this is not the case, those costs should be explicitly included in the employee's compensation. In any case, the respective agreement with the employee must be in line with the company's contracts with their telecommunication providers. Existing company rebates might have been granted under the conditions of exclusiveness, but can BYOD violate these stipulations?

2.7 Liability

In terms of liability, the BYOD should clearly define guidelines for the employee on how to treat a device in a "reasonable way." However, in lieu of this, the German principles of liability will apply. Where the private device is damaged through corporate usage (so called operational damage – "betriebsbedingter Eigenschaden"), under German employment law, the employee will receive compensation. On the other hand, the employer's liability will, in principle, not arise for damages that result from a general risk in life. German courts have not yet taken up the topic but, presumably, some basic principles concerning corporate use of private cars may apply accordingly.

In addition, the employer needs to consider their liability to third parties due to data loss, data corruption, or the costs of rectification of a security problem in absence of a security concept or reasonable behavior of its employees.

2.8 Co-determination Rights of the Works Councils

Implementing a BYOD policy or amending an existing IT policy is subject to German co-determination rights of the works council, if established, in the respective company. Following Article 87 par. 1 nos. 1 and 6 Works Constitution Act, the works council's co-determination rights include the involvement in deciding on matters relating to conduct of employees in the establishment, and the introduction and use of technical devices for monitoring employees' conduct and performance. The employer therefore cannot take any action with regard to BYOD policies without the agreement of the works council and, indeed, either side can take the initiative in such matters. In consequence, the works council can even require the company to accept rules on these matters by referring to the conciliation board. However, it remains the company's business decision to allow BYOD or prohibit the usage of private IT for corporate purposes. Moreover, the employee's consent for BYOD is essential in any case.

Contacts

Dr. Annette Demmel
Partner, Berlin
T +49 30 7261 68108
E annette.demmel@squirepb.com

Tanja Weber
Partner, Berlin
T +49 30 7261 68106
E tanja.weber@squirepb.com