schönherr legal insights *new technologies*

BYOD - Do your employees know what they are getting into?

Contact
Wolfgang Tichy
T: +43 1 534 37 50194
E: w.tichy@schoenherr.eu

Employees increasingly want to use their own smartphones or tablets for work purposes, which also involves integrating these devices into a firm's IT network. This development raises significant legal issues that both sides, employees and employers, are often too willing to ignore.

The trend of Bring[ing] Your Own Device (BYOD) to the office is currently the biggest technological development impacting our work environment. A recently published study established that nearly 50 percent of all Britons already use their personal digital devices for work-related purposes. However, only a small fraction of the survey participants said that their employer had the appropriate technical and legal framework for doing so.

The BYOD trend clearly emanated from the employees and not from the employers or their IT departments. Instead of using what they view as the plain and boring digital devices that their employers provide them, employees prefer their own "stylish" smartphones and use these in order to avoid carrying two devices. In doing so, employees often take their cue (with somewhat of a time lag) from the top management, which wanted to use their privately-owned tablets (above all, iPad's) instead of clunky laptops. The end result is that IT departments are increasingly under pressure to integrate personal digital devices in their firm's IT systems. This trend raises a whole host of issues for the IT specialists, as they're tasked with ensuring the systems' security and functionality.

However, BYOD involves so many technical and legal risks that also the top management level and individual employees should seriously consider whether they aren't paying too heavy a price for the technical comforts that BYOD provides. Employees in particular are often unaware of the degree to which BYOD leads them to assume risks that would otherwise be borne by their employers.

Advantages vs. legal risks

The advantages of BYOD are well-known: primarily, more comfort, greater flexibility, improved employee motivation, and increased availability. However, new [legal] danger zones emerge from the fact that BYOD leads to company-related information being stored and processed on devices that are not under the employer's immediate control. Above all, this applies to protecting confidential and sensitive data and to limiting the costs incurred through BYOD.

The following areas are relevant for BYOD from a legal perspective:

employment law: particularly with regard to consent requirements on the part of employees or a works council, employers' duty of care obligations, and working hours regulations

general civil law: particularly with regard to the issue of the property rights associated with digital devices, and potential damage compensation obligations
data protection law: particularly with regard to data protection, confidentiality obligations, and data security

copyright law: the work-related use of apps can potentially lead to license infringements

In implementing a BYOD policy that has a solid technological and legal basis, it is

important to pay particular attention to employment law, as the control measures that an employer implements often require the conclusion of a works agreement (one-sided BYOD policies are not sufficient in that event). For that reason, the firm can't simply assume that they are free to analyze GPS data to establish where employees are or have been, or to monitor what websites they've visited or their email usage. In general, one must differentiate between permanent measures that apply to all employees and event-related individual measures, particularly those related to suspicions of wrongdoing. Naturally, the latter are far more likely to be permissible than the former. One also cannot overlook the fact that the rising usage of the devices outside of regular work hours also raises the likelihood that work will be done outside of those hours, which also has implications with regard to maximum working hours (overtime!).

Ensuring clarity: setting a strategy

Firms that want to allow BYOD and to implement it sensibly should address the following issues in advance:

1. What personal digital devices will be allowed and what forms of access will be provided? Will that access only be possible via specialized software on the digital device, or will it also be possible to use standard software and applications that make it possible to exchange data and to store files on the device? In other words, will the employee's personal and professional data be separated?

2. Does access occur solely via an encrypted connection? What steps must be taken to ensure that unauthorized individuals are not able to access the device and its contents?

3. What password regulations exist? What security software will be installed? Who is responsible for which updates?

4. What work-related information and data can be accessed via personal digital devices? How must these be administered on the device and how must they subsequently be erased?

5. How must these devices be kept safe and secure? Can third persons (family members, for example) access the devices? Who is responsible for backups and how/when should these be performed?

6. Can the device be synced with the employee's home computer?

7. What happens in the event that the device is lost? How can the employer remotely erase company-related data (mobile data management) and what happens to the employee's personal data, which is also stored on the device?

8. Is the employer entitled to supervise the device's usage – and thus also the employee's usage of it for personal purposes – and to implement measures if necessary?

9. What employees will be permitted to BYOD?

10. How will the employer access the data stored on the device in the event that the employment relationship should come to an end?

11. Who will bear the costs, particularly those associated with data roaming or if the device is lost or stolen? It is worth pointing out that employees usually choose

their personal telephone contracts on their own and aren't able to get rates as attractive as those for firms.

A BYOD policy is absolutely necessary

The answers to these questions must not only be implemented correctly from a technological perspective, but must also be addressed within the framework of a corresponding BYOD policy. Before being allowed to use his/her personal digital device for work-related purposes, an employee must be aware of the firm's BYOD policy, must understand it and accept it. Every employee must be aware that failing to adhere to this policy involves consequences that can include being fired and facing claims for damages. Only those persons who are fully aware of this framework can truly judge for themselves whether the advantages associated with BYOD actually outweigh the disadvantages.