Avoiding data-protection pitfalls

E-mail and Internet in the workplace: crystal-clear rules are needed to handle an area strewn with stumbling blocks

By Guido Zeppenfeld, LL.M.

From a legal perspective, employee usage of an employer's IT systems at the workplace is a tricky area. While employers certainly do have a vital interest – plus a statutory obligation – to ensure compliance when its employees use company-owned electronic communication systems, including the Internet, monitoring and controlling rights are heavily restricted by data-protection laws and the individual employee's privacy rights. In practice, there are many pitfalls employers need to be aware of. On January 27, 2016, the Conference of Independent Federal and State Data Protection Authorities in Germany issued written guidance on the limits of control of e-mail and other Internet services in the workplace. Such guidance may help to avoid some of the major risk faced by employers. It contains detailed recommendations for employers, both public and private.

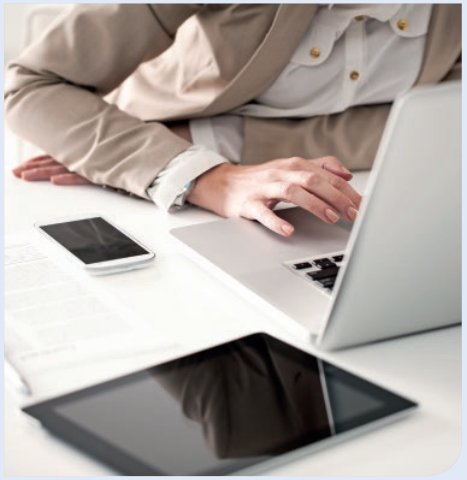
In a nutshell, the data protection authorities ("DPAs") clearly emphasize their restrictive position regarding the employer's control rights. While the guidance is not legally binding, it provides a useful indication of the DPAs common views and likely approach to specific issues regarding data protection in connection with e-mail and Internet usage in the workplace.

When it comes to the legitimacy of an employer's monitoring and control measures, the principal question is whether the employer allows – or merely tolerates – private use of the Internet or of the company's e-mail system. If it does, the employer is, according to the DPAs, to be considered a provider of telecommunication or telemedia services. As a result, the employer has to comply not only with the Federal Data Protection Act *(Bundesdatenschutzgesetz – "BDSG")*, but also with the regulations of the German Telecommunication Act *(Telekommunikationsgesetz – "TKG")* and the Telemedia Act *(Telemediengesetz – "TMG")*. In this case, the employer is subject to the legal principle of the secrecy of telecommunications, the violation of which may even constitute a criminal offence

Private use prohibited – broader options

If the employer prohibits the use of the Internet and company e-mail for private purposes, the employer may, in principle, conduct random checks to ensure compliance. According to the DPAs, these random checks are to be conducted anonymously – specifically, that is, without the employer knowing the IP addresses of the respective users. A personalized, full check will, in the eyes of the authorities, only be permissible in the case of a concrete suspicion of a violation connected to a criminal offence committed by the employee. Even in this case, checks need to be commensurate. In addition, the most privacy-friendly methods to limit Internet use are to be chosen. Blacklists – that is, lists that block certain websites – or white lists – that is, lists that allow access only to particular websites – are recommended.

If use of the company e-mail account is limited to business purposes, the employer may, in principle, only take notice



Handle with care. Data-protection-rules should always be considered.

of the content of incoming and outgoing business e-mails if they are forwarded by the respective employee. Automatic forwarding settings, however, are only permissible if the employee is absent. To comply with the principle of commensurability, it is recommended that this be restricted to situations where an out-of-

→

office note is insufficient to protect the employer's business interests.

The DPAs take the view that the employer will only be allowed to access sent and received e-mails insofar as it is necessary for business purposes. Even if private use of the e-mail account is forbidden, the employer may not take notice of the content of an e-mail as soon as its private nature is recognized. Exceptions can apply when this is necessary to ensure the effective prevention of misuse.

Private use permitted – little leeway without employee consent

If use of the Internet and/or e-mail for private purposes is permitted or tolerated by the employer, the DPAs consider the employer to be subject to the principle of secrecy of telecommunications. This means the employer may only access personal data with employees' explicit consent. Employees may refuse to give their consent without incurring disadvantages related to their employment relationship.

If the employer, for instance, wants to access log data in order to determine compliance with restrictions on private use, it may not do so without obtaining the employee's consent to both his or her Internet usage being logged and to the employer accessing this data. Even where consent has been given, every step taken by the employer needs to be commensurate. Thus a specific check, despite the employee's consent, will only be permitted in cases of concrete suspicion of a crime, a violation of duties under the employment contract, or a violation of an agreement covering private e-mail and Internet use.

Regarding e-mail use, it is recommended to put in place – obviously under due observance of the works council's co-determination rights – specific regulations on the settings of the company e-mail account in case of an employee's absence. If these regulations are not complied with, the employer may access the e-mail account if it is necessary to protect the business interests and if the employee has given his or her prior consent.

If private use is permitted or tolerated, the employer is allowed to access the e-mail account or data files on the Internet without the employee's consent only in very limited circumstances. For instance, access is possible where it is necessary to detect, isolate or eliminate errors or malfunctions.

Special restrictions concerning secrecy agents

"Secrecy agents" are people entrusted with employees' confidential information as part of their work or tasks (for example, members of the works council, company data-protection officers, company physicians or equal-opportunity officers). These individuals enjoy a special relationship of trust with the respective employees. The employer may not access the e-mails of these secret carriers or control their Internet use under any circumstances. This prohibition also applies to communication from other employees with these secret carriers.

Cybersecurity

The Data Protection Conference also points out that the requirements stipulated by data-protection law also need to be adhered to when implementing measures to protect employers' IT systems against computer viruses or to filter unsolicited e-mail.

According to the guidelines, employees need to be informed about a central spam filter in advance. Codetermination rights of the works council also need to be taken into account. Furthermore, the most privacy-friendly defense of should be used. As such, marking suspicious messages is considered preferable to deleting them. In the eyes of the DPAs, employees should be able to decide, as autonomously as possible, how to treat messages addressed to them.

Lastly, filtering and examining private e-mails containing viruses in such a way that enables the employer to see their content should only be allowed insofar as it is necessary to detect, isolate or eliminate malfunctions or errors within the telecommunications system.

Employer's to-dos

The DPAs recommend establishing written policies on business and/or private use of the company e-mail account and the Internet. These policies should contain crystal-clear rules for accessing, logging, processing and controlling e-mail and Internet usage by employees. They also recommend allowing, if at all, only private use of the Internet, including private webmail services, while prohibiting private use of the company e-mail systems and accounts.

This will reduce the risks connected with private use of the company e-mail account. Finally, nonpersonalized, role-related e-mail accounts should be –>

set up for secrecy agents (for example, workscouncil@company.com). This makes it easier to exclude these e-mails from control, assessment and processing.

Despite the nonbinding nature of the guidelines, employers are well advised to consider the Data Protection Conference's recommendations and, where possible, adjust their policies and rules related to employee use of company-owned communications systems accordingly. In doing so, compliance with employment law regulations needs to be ensured. In addition, works council's codetermination rights need to be adhered to. It can be expected that the DPAs – both national and regional – will use the conference's guidelines as a common basis for future decision making. <–

Guido Zeppenfeld, LL.M.,
Rechtsanwalt, Licensed Specialist in Labor Law,
Certified Information Privacy Professional (CIPP/E), Partner,
Mayer Brown LLP, Frankfurt am Main

gzeppenfeld@mayerbrown.com

www.mayerbrown.com