



# Proposed changes to German employee data protection law

COMPLIANCE MEASURES WILL BE HEAVILY AFFECTED

Germany's federal government recently proposed amendments to the existing laws on employee data protection. Once enacted, the new regulations would apply to practically all data collected and used by employers over the course of an employment relationship. One aim of the proposed amendments is to provide for increased protection of employees against secret surveillance measures at the workplace. As a result, the new regulations would in particular affect internal investigations to uncover cases of white-collar crime. The draft law would also restrict background checks on applicants. Overall, companies in Germany will face tougher rules on the collection, processing and use of employees' personal data.

## Introduction

On 25 August 2010, Germany's federal government proposed a new draft law on employee data protection. The planned amendments would apply to essentially all data collected and used by employers over the course of an employment relationship. The scope will not be restricted to automated data processing, so that, for instance, handwritten remarks about employees and personnel files will also – as today – fall under the data protection guidelines. Already under current law violating the statutory rules on data protection may in certain events trigger a serious fine or even imprisonment.

The German parliament is expected to decide on the proposed new law by the end of the first quarter of 2011. This briefing covers what we consider to be the most important aspects of the proposed amendments to the German Federal Data Protection Act for companies.

## Impact on compliance measures and internal investigations

In investigating serious cases of misconduct or white-collar crime – expressly cited examples include embezzlement and acceptance of bribes – existing employee data may be used only in anonymous form. Only after a suspicion has been substantiated may the data be linked to a specific individual. The affected employee(s) must be informed of the investigation into their personal data as soon as is possible without compromising the investigation.

An employer may collect (and process and use) data without the employee's knowledge for investigation purposes only if the facts substantiate the suspicion that the relevant employee has committed a crime or – and this is less restrictive than the current law – other serious misconduct in his capacity as an employee, which would entitle the employer to terminate employment for cause, and if collecting the data is necessary to expose the offence. Also, preventative measures designed to rule out further criminal acts or instances of serious misconduct are permissible only under these narrow circumstances.

## Monitoring of emails

The new amendments have not clarified the long-standing legal question as to whether an employer that allows private use of its email system is to be classified as a 'telecommunications provider' and, as such, subject to telecommunications secrecy.

Under the new amendments, work-related mails that have completed transmission (ie the email has arrived on the employee's workstation) may be used in anonymous form to uncover serious misconduct and white-collar crime – even without a concrete suspicion. However, work-related emails that have not completed transmission (in other words, are merely stored on a server) may be analysed only when the employer has a concrete suspicion that the relevant employee has committed serious misconduct or a white-collar crime.

Evidently private emails may be viewed only to the extent that doing so is 'essential for the conducting of normal

work or business operations’ and if the employees have been informed in writing that such emails may be viewed – irrespective of whether private emailing is allowed. What is ‘essential’ in specific cases is likely to be difficult to determine.

## Video surveillance at work

In specific cases, it is still permissible for an employer to openly conduct video surveillance of employees using clearly distinguishable video equipment for certain reasons, such as protecting company property and averting danger. However, premises relating to employees’ privacy (for example, changing rooms) may not be videoed. Furthermore, secret video surveillance is prohibited under the proposed new regulations. Strict rules also apply to the use of tracking devices, biometric systems and wire-tapping.

## Collecting data from job applicants

The permissibility of questions to applicants continues to be based on the relevance of the information for assessing an applicant’s suitability for the position. A prospective employer may ask questions relating to particularly sensitive data – in this context, the proposed new regulations expressly list: disabilities, health, religious or political views etc, as well as criminal records and financial standing – only if they are significantly and decisively pertinent to the work applied for. There are also guidelines stipulating the conditions under which an employer may require applicants and employees to take part in aptitude tests, including assessment centres or physical examinations.

It is currently unclear to what extent employers in Germany may gather personal information about job applicants through the internet for conducting background checks. The new laws would substantially restrict employers’ ability to obtain such data about applicants from social networking websites – the sole exception to this rule is for networks designed to convey professional information, such as LinkedIn or Xing.

## Deviations from data protection standards with employee consent

Encouragingly, the new amendments provide for the possibility to obtain an employee’s consent for the

employer to use his personal data. At the same time, however, the scope within which such consent can be legally obtained will probably be very restricted, which will leave companies with little room to deviate from data protection standards.

## Collective agreements as additional legal basis for data transfers

In principle, it remains possible to use collective agreements as an additional legal basis for processing employee data, as a supplement to the Federal Data Protection Act. Under the current law, as well as under the proposed amendments, the transfer of employee data within a group of companies (for example, from a subsidiary to its group headquarters) is generally permissible only if it is necessary for the performance of an employment contract. Therefore, in practice, such data flows that serve group-wide human resources purposes are often justified by a works council agreement. However, the extent to which this will still be possible in the future remains to be seen, given that the draft law prohibits deviations from the statutory provisions that would disadvantage employees.

For further information please contact

INTELLECTUAL PROPERTY  
AND INFORMATION  
TECHNOLOGY  
Norbert Nolte  
T +49 221 20 50 72 23  
E [norbert.nolte@freshfields.com](mailto:norbert.nolte@freshfields.com)

Philipp Becker  
T +49 221 20 50 71 95  
E [philipp.becker@freshfields.com](mailto:philipp.becker@freshfields.com)

EMPLOYMENT, PENSIONS  
AND BENEFITS  
Boris Dzida  
T +49 40 36 90 63 30  
E [boris.dzida@freshfields.com](mailto:boris.dzida@freshfields.com)

Timon Grau  
T +49 221 20 50 71 55  
E [timon.grau@freshfields.com](mailto:timon.grau@freshfields.com)

Freshfields Bruckhaus Deringer LLP is a limited liability partnership registered in England and Wales with registered number OC334789. It is regulated by the Solicitors Regulation Authority. For regulatory information please refer to [www.freshfields.com/support/legalnotice](http://www.freshfields.com/support/legalnotice). Any reference to a partner means a member, or a consultant or employee with equivalent standing and qualifications, of Freshfields Bruckhaus Deringer LLP or any of its affiliated firms or entities.

This material is for general information only and is not intended to provide legal advice.

© Freshfields Bruckhaus Deringer LLP 2010  
[www.freshfields.com](http://www.freshfields.com)