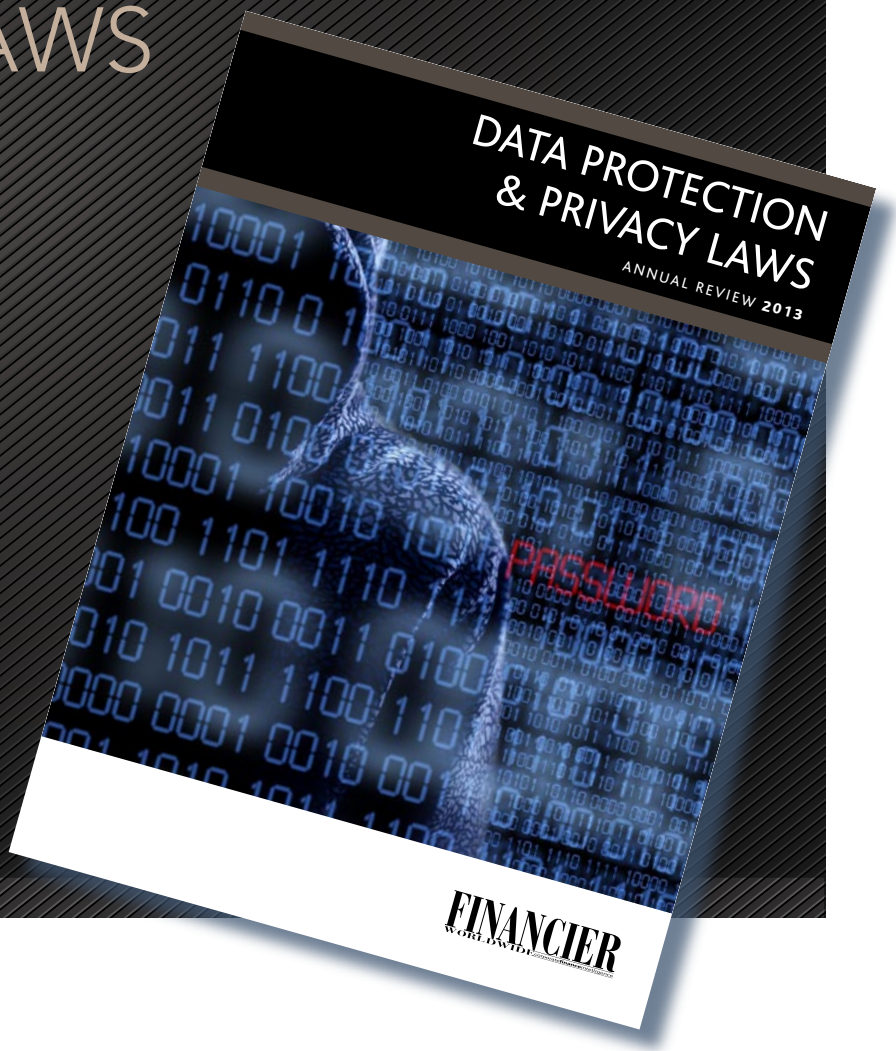
ANNUAL REVIEW

DATA PROTECTION & PRIVACY LAWS



REPRINTED FROM
ONLINE CONTENT
SEPTEMBER 2013

PREPARED ON BEHALF OF

BUSE HEBERER FROMM
RECHTSANWÄLTE · STEUERBERATER PARTG

FINANCIER WORLDWIDE corporatefinanceintelligence

Germany

STEFAN SIMON
BUSE HEBERER FROMM

Q AS COMPANIES INCREASE THEIR DATA PROCESSING ACTIVITIES, INCLUDING TRANSFER AND STORAGE, WHAT REGULATORY RISKS DO THEY FACE IN GERMANY?

SIMON: Companies face a situation whereby the data protection provisions currently in effect, particularly those governing the use and transfer of data, do not meet the requirements of modern forms of economic collaboration. In particular, as a practical matter, there are no suitable legal standards with respect to cloud solutions for data storage and management under which companies can manage data with legal certainty. This applies especially to the question of access rights, deletion rights, and proof of data security for cloud solutions. Moreover, it is very difficult to organise the international transfer of data in complex structures with legal certainty. To be sure, the EU Commission has drafted standard contracts; however, they cannot be adapted to national requirements abroad. There is also a difficult regulatory environment with respect to the implementation of whistleblower systems. No special statutory provisions exist in this area. In practice, it is difficult to implement the general requirements of data protection law with respect to whistleblower systems. The result is that whistleblowers are not protected by statute, and companies are operating in a grey area when implementing whistleblower systems.

Q COULD YOU OUTLINE THE LATEST LEGAL AND REGULATORY DEVELOPMENTS, IF ANY, AFFECTING CORPORATE HANDLING OF DATA IN GERMANY?

SIMON: At the present time, a proposed EU data protection regulation is awaiting adoption. The current version of the draft regulation would reduce the level of data protection as compared to the present state. In addition, lawmakers are discussing a federal law to protect employee data, which would codify the current state of legislation, legal precedent, and administrative practice into law. Finally, a law to protect whistleblowers is still under discussion. Draft laws were discussed in the spring of 2013. It is expected that such a law will be adopted during the next legislative session. With respect to management of the Safe Harbour Agreement, several data protection oversight authorities have decided

continued...

that data transfer based on this agreement with the United States can no longer be regarded as a legally compliant solution. They are calling for an amendment or even cancellation of the agreement.

Q DO YOU BELIEVE COMPANIES FULLY UNDERSTAND THEIR DUTIES OF CONFIDENTIALITY AND DATA PROTECTION IN AN AGE OF EVOLVING PRIVACY LAWS?

SIMON: In practice, many companies have a 'feel' for data protection in general and with respect to individual questions, particularly the questions raised in public scandals. However, it appears that there is essentially no understanding and no knowledge of the specifics of data protection for employee or customer data, or the permissibility of data transfer to an outside service provider or international data transfer within a corporate group. In particular, there is no familiarity with the legal framework for supervising employees and transferring data outside the company. In these areas, companies often work on the basis of an 'established practice'.

Q WHAT PENALTIES MIGHT ARISE FOR A COMPANY THAT BREACHES OR VIOLATES DATA OR PRIVACY LAWS IN GERMANY?

SIMON: If the provisions of data protection law are violated, companies – as well as the managers of those companies – can face fines of up to 300,000 per individual incident. In individual cases, particularly in the areas of supervision of employee data and invasions of privacy, persons may, in principle, be threatened with imprisonment up to two years. In practice, the crucial factor for a company is the risk that the company's reputation and thus its 'brand' may be permanently damaged through reports that become public. This is of particular relevance to companies that sell consumer-oriented goods and services, that operate in sensitive economic areas – such as the arms industry – or that are otherwise in the public eye, for example, because they are owned by government institutions or large foreign investors.

continued...

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD A COMPANY TAKE TO PREPARE FOR A POTENTIAL DATA SECURITY BREACH, INCLUDING UP-TO-DATE KNOWLEDGE OF ANY NOTIFICATION REQUIREMENTS?

SIMON: The key to preparing for a serious data protection violation is for the company to be organisationally prepared for the situation. Ideally this means that a data security team, consisting of a small number of persons, should exist in the company. This data security team will be in charge in any crisis situation involving a data protection violation so that the necessary decisions from a technical and organisational perspective – such as reports to the data protection oversight authorities and the affected parties, if necessary – and from a PR perspective, can be made quickly and correctly. This team should consist of competent employees from the IP Department, the company's data protection officer, and an employee of a staff department, such as the Compliance Department. In crisis situations, such as a serious data protection violation, a coordinated team must assess and repair the damage, call in the necessary authorities, and provide selected information to third parties. The crucial factor is that the crisis process must be actively controlled – not reactively.

Q WHAT CAN COMPANIES DO TO MANAGE INTERNAL RISKS AND THREATS, SUCH AS LIABILITIES ARISING FROM THE ACTIONS OF ROGUE EMPLOYEES?

SIMON: To control internal risks within the company, it is necessary to have data management guidelines that are binding on all employees and govern the handling of personal data, the use of hardware, and confidentiality. Only in this way is it permissible under labour law to implement appropriate control measures to determine whether all employees are acting in conformity with the rules. Another compliance instrument can be the use of a whistleblower system, which must be adapted to the situation at the specific company. A further option is to fragment sensitive records through a technical process or personalise access authorisations to sensitive records to ensure that the number of employees with access to sensitive records is as small as possible or is limited to trusted, long-term employees.

continued...

Q WOULD YOU SAY THERE IS A STRONG CULTURE OF DATA PROTECTION DEVELOPING IN GERMANY? ARE COMPANIES PROACTIVELY IMPLEMENTING APPROPRIATE CONTROLS AND RISK MANAGEMENT PROCESSES?

SIMON: From a legal perspective and in the public view, there has been a rigorous awareness of data protection and personal privacy since the end of the 1990s. However, this awareness and the conscious implementation of strict data protection rules by companies has only become a focus in recent years. The primary reason for this is the data scandals experienced by large companies, which have resulted in company management being held personally liable and the serious damage that has been inflicted on the company's reputation as a result. Generally, large companies which do not already process data in a professional manner due to their lines of business – telecommunications, banks, insurance companies, and so on – and SMEs still have a lot of catching up to do. However, it should be noted that in recent years more of these companies have been addressing the topic of data protection proactively, taking inventory within the company, and implementing the first structures to protect sensitive company data in a professional manner.

DR STEFAN SIMON

Partner
Buse Heberer Fromm
+49 89 678006 146
simon@buse.de

BUSE HEBERER FROMM
RECHTSANWÄLTE · STEUERBERATER PARTG

Dr Stefan Simon is a partner in the IT/TC Practice Group of Buse Heberer Fromm and works in the field of data protection and privacy laws, as well as IT-related commercial contract solutions and litigation matters. He is specialised in the establishment of compliance systems, particularly in regard to data protection and international data transfer issues. In addition, Dr Simon advises on the implementation of whistleblowing systems and handling crisis situations in data protection and privacy matters.