



GERMANY

DR STEFAN SIMON
SPITZWEG PARTNERSCHAFT



Q IN YOUR EXPERIENCE, DO COMPANIES PAY ENOUGH ATTENTION TO THE RISKS ASSOCIATED WITH DATA PROTECTION? ARE THEY BEGINNING TO FULLY UNDERSTAND THEIR DUTIES OF CONFIDENTIALITY AND PRIVACY IN THE DIGITAL AGE?

SIMON: Most companies in Germany have a 'feel' for data protection in general, and with respect to the kinds of individual issues raised due to public scandals. There is still essentially no understanding and no knowledge of the specifics of data protection for employee or customer data, or the permissibility of transferring data to an outside service provider or internationally within a corporate group. The fact is that data protection, so far, is not considered an issue for the CEO. But a process for change has been initiated in the last months of 2014. Some key factors, such as the Snowden-affair, political based discussions in the US and EU on global data protection, and national movements including public-private initiatives on national IT-security conferences, have caught companies' attention. Further, due to the development of an IT-integrated industry, 'industry 4.0', which is strongly supported by the German Mittelstand, data as a business secret and customer data have become the focus for companies. Germany has a quite severe data protection framework, and it is now up to companies and the IT security industry to use this framework in the proper way.

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

SIMON: The EU data protection regulation project is still in progress. Adoption of the regulation was not expected until the end of 2014, but since negotiations between Parliament, the Commission and Member States continue, the adoption date will not be before autumn 2015. One of the regulations' primary aims is to avoid 'framework shopping', which involves companies choosing the most favourable privacy laws for their activities within the European Union. In Germany, the Data Protection and Privacy Act will not be amended or supplemented before the EU regulation has been adopted. Recently, however, a draft of a German IT Security Act has been launched. The legislators' aim is to



protect companies against cyber attack, but the provisions also foresee that online service providers are entitled to store personal data relating to website visits in general. Therefore, the Act is in a constitutional conflict, so more time is required to assess whether and in what form the Act will be adopted. By the end of October 2014, Germany, along with over 50 other countries, signed an international agreement to prevent tax fraud. On the basis of this agreement, from September 2017, participating countries will exchange personal data on revenues, income and further tax-related data.

Q IN WHAT WAYS HAVE
GLOBAL AUTHORITIES
INCREASED THEIR
MONITORING AND
ENFORCEMENT ACTIVITIES
WITH RESPECT TO DATA
PROTECTION AND PRIVACY
IN RECENT YEARS?

SIMON: The EU-Commission was going to be more sensitive in recent years with respect to the security of data stored by global companies operating within the EU, as well as for data transfers from the EU to the US. As it turned out, the EU data protection regulation has actually increased the conditions for storing and transferring data. M. Andrus Ansip, designated EU-Commissioner, declared during a Parliament hearing that he would be suspending the Safe Harbor Framework for the inter-continental exchange of personal data between the EU and the US. He anticipated that the framework would be in conflict with European data security standards. In this context, a judgment of the European Court of Justice may clarify the situation, as the Irish High Court has presented a case at the European level, involving the question of the lawfulness of the Safe Harbor Framework.



Q WHAT INSIGHTS CAN WE DRAW FROM RECENT HIGH-PROFILE DATA BREACHES? WHAT IMPACT HAVE THESE SITUATIONS HAD ON THE DATA PROTECTION LANDSCAPE?

SIMON: We draw the conclusion that, in the long term, only high-profile data breaches, such as the 'PRISM' spyware, will promote greater awareness of data security and the handling of personal data. These data breaches have the potency to drive legal developments, even on a transnational level. But they may also encourage market players in the IT sector to implement improved standards for data handling, transfer and storage, as we have seen in Germany.

Q THE USE OF THIRD PARTIES, SUCH AS CONSULTANTS, AGENTS AND DISTRIBUTERS, EXPOSES FIRMS TO UNIQUE DATA PROTECTION RISKS. WHAT ARE SOME OF THESE RISKS AND WHAT STEPS CAN BE TAKEN TO MITIGATE THEM?

SIMON: In practice, many companies, especially of the German Mittelstand, fail to pay attention to the data security of their business partners. In fact, the German Data Protection Act provides that a company cooperating with a third party has to guarantee the same level of data protection as itself and, furthermore, must regularly audit the business partner. So, companies have to turn their attention to the security architecture of their business partners and verify the conditions of data storage. Further, they need to implement an audit and certification process of any business partners that processes their data.

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

SIMON: One thing to be aware of: nobody can ensure absolutely that there will be no data breach. However, a company can take steps to heighten the awareness of risks, and also put in place strategies to minimise those risks. To manage risks, it is necessary to have data management guidelines and policies that are binding on all employees and govern the handling of personal data, the use of hardware and confidentiality. It is advisable to promote proper awareness of data protection risks. Further, detailed training of employees and management, as well as regular audits, should form part of the risk management program. Appropriate control measures to determine whether all employees are conforming to the rules should be implemented. Finally, the company has to invest in technical measures to improve data security, especially when outsourcing data processes.



“Companies have to turn their attention to the security architecture of their business partners and verify the conditions of data storage.”

Q WHAT ADVICE CAN YOU OFFER TO COMPANIES ON MANAGING DATA RISK, INSTALLING INTERNAL COMPLIANCE PROCESSES AND MAINTAINING COMPLIANCE ON DATA PRIVACY GOING FORWARD?

SIMON: Companies should use instruments to monitor data security risks. On the other hand, they have to return, at all levels of employment – especially management – to a more ‘conservative’ attitude when it comes to processing electronic data. Firstly, companies should identify their critical data flows and address the potential risks from a technical perspective. That means they have to act according to a ‘need to know’ principle when using external service providers, emphasise access rights management, and monitor the execution of access rights. Companies need to be aware that data is an important asset, and should therefore be treated as such.



Dr Stefan Simon

Partner
SPITZWEG Partnerschaft
+49 89 678006 146
stefan.simon@spitzweg.com

SPITZWEG

RECHTSANWÄLTE
STEUERBERATER
WIRTSCHAFTSPRÜFER

Dr Stefan Simon is a partner in the IT-service line of SPITZWEG (spin-off from Buse Heberer Fromm) and works in the field of data protection and privacy laws as well as European economic law. He specialises 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.