Market Intelligence

PRIVACY & CYBERSECURITY 2020

Global interview panel led by WilmerHale

LEXOLOGY®
Getting The Deal Through

LEXOLOGY
Getting The Deal Through

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Business development manager
Dan Brennan
dan.brennan@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

Cover photo: shutterstock.com/g/handmadefont

ISBN: 978-1-83862-419-4

Printed and distributed by Encompass Print Solutions

Privacy & Cybersecurity 2020

Germany

Dr Martin Braun is a member of the WilmerHale European Union regulatory group and is co-chair of the WilmerHale big data practice group. He focuses his practice on data protection, cybersecurity and information technology law. Dr Braun has advised German and multinational companies on all aspects of privacy and data protection law including cross-border flows of personal data, data security, employee data protection, electronic discovery and document retention issues. He has significant experience litigating technology issues, which includes several cases before the Court of Justice of the European Union. WilmerHale has handled a significant number of major international data breaches and incidents.

Dr Braun is regularly recommended by the relevant legal handbooks as a leading lawyer in the fields of data protection and information technology. He is a regular speaker at data protection and cybersecurity conferences and among the authors of the WilmerHale Privacy and Cybersecurity Law Blog.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

Germany is currently in the final phase of updating its main cybersecurity law, the BSI Act (Act on the Federal Office for Information Security). The amendments will further strengthen the Federal Office for Information Security (BSI) and significantly expand its role in the general German cybersecurity architecture.

Among the changes will be a strengthened role of the BSI regarding consumer protection and consumer information, including with respect to products that have cybersecurity relevance; further competences regarding the information technology systems and networks of the German federal administration; and a lead role in the area of certifications. The BSI is expected to be given GDPR-style fining powers, with fines of up to the larger of €20 million and 4 per cent of global annual revenue.

It is also noteworthy that Germany will introduce specific rules regarding 'critical components', whose manufacturers may be required to submit formal trust-building statements to operators of critical infrastructures. The BSI may declare that a manufacturer of a critical component is not trustworthy if the manufacturer has made incorrect statements, if it does not sufficiently cooperate in security audits and evaluations, or if it does not remediate security weaknesses within an appropriate time frame. This can lead to formal prohibitions of the use of certain critical components. Further details will be specified in ordinances.

On a more general level, cybersecurity requirements in the General Data Protection Regulation (GDPR) have continued to play a major role in companies' implementation efforts. The importance of these efforts has been highlighted by the initial fining decisions of the German supervisory authorities, with several fines sanctioning inadequate IT security. This mirrors the development in several other countries in the European Union.

The IT Security Association Germany (www.teletrust.de), a business association, updated its document 'What is "state of the art" in IT security?', in January 2020. The document aims to provide interested parties with recommended actions and guidelines on the 'state of the art' required for technical and organisational measures.

The BSI, under its current president Arne Schönbohm, has continued its active outreach to all relevant actors in the field and successfully formed a substantial number of new alliances and cooperation partners. The BSI continues to publish sector-specific guidance documents in the area of cybersecurity. The BSI also had a particular focus on creating awareness for cybersecurity in the energy sector. The authority awarded certificates to several companies under the Cloud Computing


Martin Braun

Compliance Controls Catalogue (C5). In June 2020, the BSI announced a partnership with the Federation of German Consumer Organisations, which includes joint activities for informing consumer about cybersecurity, but may also involve mutual support in enforcement activities and litigation.

Other regulators have continued to thoroughly review and act on cybersecurity topics. Regulators for financial services on a European and German level have continued their updates of several guidance documents regarding IT in general, cybersecurity, cloud computing or outsourcing and breach reporting.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

Since 25 May 2018, the key general data breach notice obligations are the respective obligations under the GDPR. Since that date, the number of breaches reported to the data protection authorities has increased significantly, with many actors taking a very cautious approach and a decision to rather err on the side of over-reporting.

In a statement preparing the evaluation of the GDPR, the German data protection authorities suggested modifications of the current provisions, as the GDPR appears to require the reporting of breaches that to not lead to material risks for the affected individuals.

The German Federal Data Protection Act does not contain any comparable obligation, but the German Telemedia Act and the German Telecommunications Act (TKG) continue to require providers of information society services and providers of electronic communications services to notify certain breaches. The obligations in the TKG are still based on the European framework in Directive 2002/58, but Germany is expected to implement Directive 2018/1972, the European Electronic Communications Code, later this year. In addition, there are sector-specific obligations (eg, in social security, energy, financial services and electronic signatures, among others).

The implementation of the NIS Directive on cybersecurity has created additional notification obligations, which are not tied to personal data, but to security incidents in general. This has further increased complexity, as one breach may require the notification of several regulators in parallel.

Photo: shutterstock.com/g/euregiocontent

Regulators have updated their expectations for the reporting of breaches, including for situations where third-party service providers are involved, such as in cloud computing. In addition to the general risk management motivation, the implementation of the PSD2 (payment services) directive has led to additional awareness in this area. Most regulators now make available online tools for actual reporting.

In terms of enforcement, fines for failing to report breaches have not been common yet, but warnings are increasing. In May 2020, the Irish Data Protection Commission announced that it is close to issuing a formal decision in a case involving a possible breach by Twitter. It is widely expected that the European Data Protection Board will weigh in, so further clarifications with pan-European impact regarding the interpretation of certain key terms in the GDPR can be expected.

Contrary to many observers' expectations, litigation of affected individuals as a reaction to breaches has been limited so far. Most of the time (at least currently) the notification obligations to regulators and affected individuals take centre stage when evaluating breach response strategies.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

Meeting legal obligations to notify breaches is extremely difficult without proper preparation: timelines for the required notifications are ambitious and investigating factual and legal topics in parallel and taking into consideration the interdependencies can be extremely challenging.

We have seen more and more breaches with a significant international dimension, adding further complexity because of the need to coordinate the response across different jurisdictions and time zones.

Companies must generally try to quickly determine what has actually happened, stop the underlying issue (ideally without compromising evidence) and then decide whether there are legal obligations to notify the breach to regulators and affected individuals. Depending on the extent of the breach, there may be obligations to inform shareholder and there is very often also a need to check the actual insurance status. Finally, the public relations fallout can be very significant and needs to be actively managed.

Following a breach notification, data protection and other regulators might also be interested in the company's activities in general, so companies should be prepared that such notifications may lead to additional audits in related and unrelated fields.

If a breach or a suspected breach has occurred and needs to be investigated, such investigation itself is subject to German data protection and employment laws. These are highly relevant in a number of aspects. Generally, German data protection

"The *Schrems II* case on 16 July 2020 has brought these restrictions of international data flows back to centre stage."

authorities have been taking a rather strict view regarding the retention of data such as log files in preparation for possible investigations, which can make it difficult to trace back attackers. In addition, the scope of possible investigations may be limited, because the authorities have taken the position that employers who permit private use of the internet or email are subject to secrecy of telecommunications, putting them at risk of criminal investigations if the review of a breach or security incident goes beyond the limits of secrecy of telecommunications. Finally, many companies have an organised workers' representation, the works council, which needs to be involved in most IT-related topics.

Third parties involved in investigating and responding to a breach must be contractually bound to maintain confidentiality and to implement appropriate IT security measures. In many instances, they will be acting as processors, which means that there needs to be a written agreement with certain mandatory content, as required by the GDPR. If, for example, forensics firms are located outside the European Union, there will be additional issues regarding international data transfers.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Preparation is crucial. We recommend preparing for possible security incidents by setting up an internal and external panel of experts, which would include forensics firms and outside lawyers, but also advisers for public relations topics, and to enter into the required contracts well before an incident occurs. This will save critical time if there is an actual incident.

A written, detailed breach response plan is another critical element of the preparations. There are still too many companies having a response plan that looks more like 'we will inform management, the legal department and IT, and they will work this out.' These plans need to be much more detailed to be actually useful and there needs to be list of individuals assigned to be the core incident response team.

We strongly recommend to also test the plan periodically by simulating an incident or a breach and going through the required steps, including possible additional knowledge that only develops after investigations have actually begun.

For organisations with an international footprint, there must be an alignment of local, regional and international plans. This needs to involve some thinking on, for example, how to respond to situations where decision makers are located in different time zones.

Finally, given the rapid development of applicable law and regulatory guidance, there is a need to continually monitor legal development and to update the plans accordingly.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

German public opinion is still quite sceptical regarding cloud computing, but German organisations are increasingly moving their data to cloud providers. Regulators have generally also been quite hesitant.

In the German tradition, cloud computing is usually considered to be a form of a controller-processor relationship. In the light of the recent judgment of the Court of Justice of the European Union, there are now some questions whether this perspective will continue to dominate under the GDPR or whether we will see 'joint control' with increasing frequency. Under article 26 of the GDPR, joint controllers also set up an arrangement to allocate rights and responsibilities.

Like German law in the past, the GDPR now has a quite extensive list of specific topics that must be addressed in the contract with processors (here: the

cloud provider). We are seeing initial market practice evolve regarding template documents in this regard, after several industry associations and regulators have published suggestions for language to address the legal requirements.

International data transfers to recipients outside the European Union are usually of particular interest. Very often, German customers demand that the cloud environment should be physically located in Germany or at least in the European Union, even though the legal framework for international data transfers to recipients outside the European Union would typically apply and allow transfers in other countries, such as the United States. Vendors who have opened data centres in Germany have been able to attract many German customers who had been sceptical about cloud computing beforehand.

Organisations need to remember that the international transfer restrictions still apply if the data is stored in Germany, but there is access to the data from outside the European Union.

The judgment of the Court of Justice of the European Union in the *Schrems II* case on 16 July 2020 has brought these restrictions of international data flows back to centre stage. The court invalidated the Privacy Shield arrangement, and

also clarified that the use of standard data protection clauses alone is very often not sufficient to allow transfers of personal data to countries that the European Commission has not expressly declared as providing an adequate level of data protection.

Organisations must review their international data transfers and find an alternative legal basis for transfers that have been conducted under the Privacy Shield. They must also re-read the standard data protection clauses and comply with the obligations in these clauses. In addition, an understanding of the laws in any country outside the European Union will be required, which will be the basis for possible additional measures to protect such data, especially from government surveillance.

In the absence of such additional measures, the data protection authorities may suspend such data flows.

In general, more developments are already announced: the European Commission is expected to update the existing standard data protection clauses shortly, and it will also finalise its review of the current adequacy decisions.

As a general recommendation, we usually recommend reviewing the technical and organisational measures of the respective cloud provider in detail and to document such review. There is also a legal requirement to periodically update such review, as IT security standards and measures can change over time. Encryption of data, both at rest and in transit, tends to be a topic that attracts significant interest in this context.

When thinking about using cloud services, organisations should also check for legal requirements arising out of other areas of the law. Typical examples are German tax law, which requires that certain tax-relevant documents are kept in Germany (or at least the European Union).

Germany has recently updated its laws and relaxed criminal law restrictions on the use of third parties by medical professionals, certified accountants, lawyers, certain forms of insurance and the public sector. While not all details are fully clear yet, the new framework has significantly reduced legal uncertainties for these sectors when using third-party providers, including in a cloud and outsourcing context.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

Germany had implemented national laws very similar to the NIS Directive already before the NIS Directive was finalised. Germany was also very quick in implementing the NIS Directive after it was finalised. In the light of recent ransomware attacks, sophisticated attacks against the German parliament and widespread fears of foreign countries trying to interfere with the national election in September 2017,

many stakeholders have already argued that additional measures need to be taken to deal with cyberthreats on a national and European level.

The German BSI and the domestic intelligence services are very actively involved in raising awareness of cybersecurity threats and in making specific recommendation for actions (eg, in response to ransomware, CEO fraud and general IT security challenges).

Law enforcement, while generally understaffed to deal with the complexities of cybersecurity threats, has set up central units in most of the German states with special cybersecurity expertise. These units have had some notable successes in the past months in tacking large-scale online crimes. Companies are strongly encouraged to contact law enforcement if they are the target of online criminals.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

Unfortunately, privacy and data security issues are still very often not treated with the required care in the context of M&A deals. A company's data and IT systems are very often a crucial factor for the entire operation and special care should be used to determine if data, especially customer data, has been collected lawfully and whether it can be used as intended post-closing.

German data protection authorities have started issuing fines where the parties to an M&A transaction wrongly assumed that they could just sell customer data and failed to comply with legal requirements regarding the information of the data subjects and providing an opportunity to opt out or even seek consent.

With the background of increased attacks against a company's information technology systems, due diligence should pay particular attention to whether business secrets, critical know-how and personal data have been properly protected against theft. Valuations of companies are now critically dependent on IT security, and intruders are becoming more sophisticated by the day.

These topics should be addressed through appropriate language in the representations and warranties in the underlying deal documentation.

Martin Braun
martin.braun@wilmerhale.com

WilmerHale
Frankfurt
www.wilmerhale.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

The lawyer needs to be able to explain legal concepts and requirements to a non-legal, especially technical audience, but he or she also needs to be able to truly understand what has happened from talking to technical experts.

The regulatory framework is evolving quite dynamically, so it is important to be up to date regarding the latest developments.

Project management skills and experience with internal investigations and crisis situations. For larger clients, the ability to work in an international setup and across time zones will be important.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

Cybersecurity and privacy work occurs at the intersection of a large number of legal and non-legal areas. The field is also currently moving at high speed. Incidents and breaches can be a threat to the survival of an organisation and successfully helping clients navigate challenges in this kind of crisis is usually very rewarding.

How is the privacy landscape changing in your jurisdiction?

The interpretation of many of the GDPR's provisions is not settled yet, so everybody needs to continue monitoring the legal developments and to update processes and documentation. Unfortunately for organisations, international data transfers and their legal bases have been subject to significant changes and uncertainties for years and these are going to continue.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

Recent developments have made clear that ransomware can have a crippling effect on companies. Threats arising out of non-technical attacks, such as CEO fraud, persist and have even increased. This makes clear that effective defensive measures against cybercrime are not limited to technology, but need to also involve organisational measures and especially increased training of employees.

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by WilmerHale, this *Privacy & Cybersecurity* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Covid-19 response
M&A risks
Latest regulatory trends
Cloud hosting

an LBR business

ISBN 978-1-83862-419-4