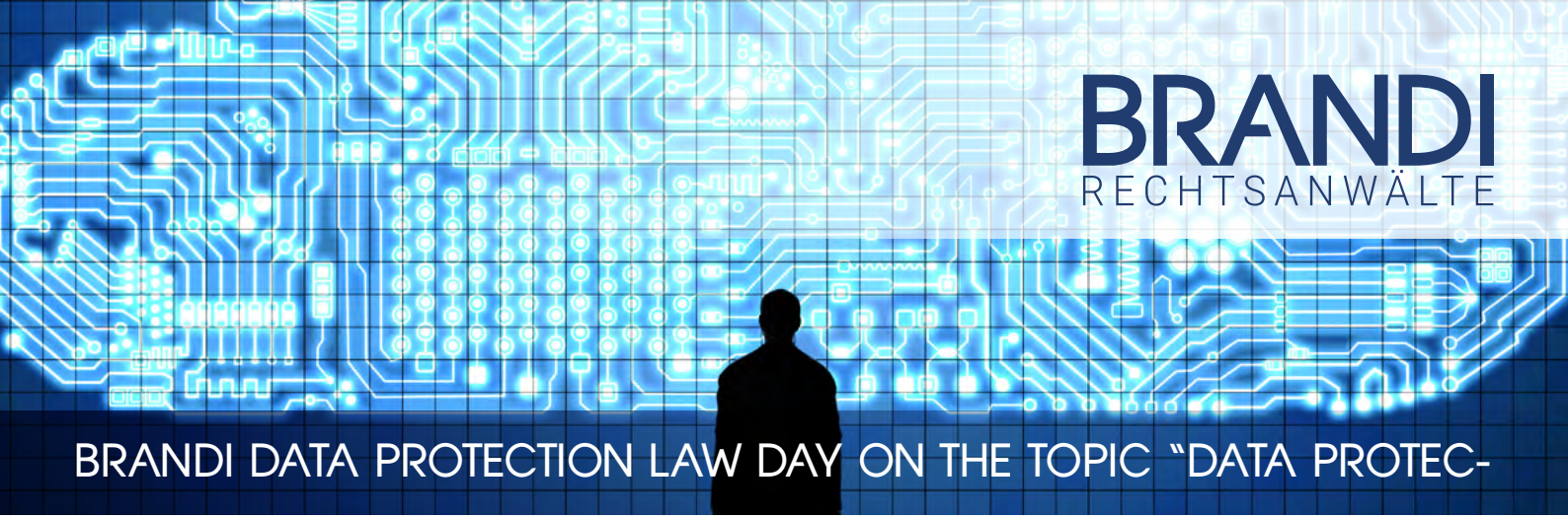

BRANDI DATA PROTECTION LAW DAY ON THE TOPIC "DATA PROTECTION IN THE CLOUD AND CYBERSECURITY"

Information on data protection I June 2023

Introduction

On May 12, 2023, Prof. Dr. Alexander Roßnagel was a guest at BRANDI in Bielefeld. Prof. Roßnagel is the Hessian Commissioner for Data Protection and Freedom of Information (HBDI). Previously, he was a senior professor of public law with a focus on the law of technology and environmental protection at the University of Kassel. As part of this year's Data Protection Law Day on the topic of "Data Protection in the Cloud and Cybersecurity", he gave fascinating insights into various data protection law topics, current procedures and the daily work of the Hessian Data Protection Authority and the Data Protection Conference (DSK) in conversation with lawyers from BRANDI including Dr. Sebastian Meyer, Dr. Christoph Rempe, Dr. Laura Schulte, Dr. Christoph Worms and Dr. Daniel Wittig.

During the event, issues relating to the use of cloud services and cybersecurity were examined. In the first part, the participants discussed, among other things, the legal advantages and disadvantages of on-premise solutions and cloud-based applications, the use of Microsoft 365, as well as aspects of contract negotiations with the providers of cloud solutions and the protection of third-country transfers, including the consequences of the Schrems II ruling and the current status of the new adequacy decision for the USA. Prof. Roßnagel began by speaking on the topic of "Data Protection in the Cloud". In the second part, following the keynote speech "Liability Risk Cyber Incidents" by Dr. Schulte, the discussion turned to the legal protection of cyber incidents, insurance law and criminal law aspects and various strategies for dealing with cyber incidents. In the third part of the event, prospective lawyers gave presentations on various current data protection law topics as part of the BRANDI Young Lawyers Award.

Use of cloud solutions

The first part of the event was devoted primarily to the use of cloud services and the relevant data protection issues and requirements in this context.

Keynote speech: Data Protection in the Cloud

In his keynote speech, Prof. Roßnagel started by pointing out that most cloud providers were not from Germany or the EU and explained what it meant to understand cloud computing as commissioned processing. In doing so, he addressed the basic concept of commissioned processing as well as the requirements resulting from Article 28 GDPR. At the same time he made it clear that, in practice, the power relationship between the client and the contractor is usually reversed in the case of cloud computing, which is why it is sometimes difficult to comply with and implement the requirements provided for by the GDPR. In this respect, he cited Microsoft 365 as an example and discussed the weaknesses in terms of data protection law in the contract processing agreement provided by Microsoft and Microsoft's lack of willingness to negotiate. In this context, he also pointed out that cloud computing is usually associated with international data transfer and that appropriate safeguards must therefore be put in place. In this context, he addressed the requirements developed by the ECJ in its Schrems decisions and reported on the current status of the European Commission's new adequacy decision for data transfers to the USA ("Trans-Atlantic Data Privacy Framework"). In particular, he cited various critiques, such as the continuing possibilities of access by the U.S. authorities and the inadequate complaint mechanisms, which have already been formulated by the EDPB and the LIBE Committee of the European Parliament. Moreover, the adequacy decision is not expected to enter into force before the end of this year – provided that the further procedural steps are successfully completed – and it is likely that it will then be quickly challenged by legal action. In conclusion, Prof. Roßnagel pointed out that one should make oneself as independent as possible from the disputes described above and must therefore orient oneself in the long term towards the goal of achieving as high a degree of digital sovereignty as possible. He also reported on the recently developed position paper of the DSK, which sets out criteria that can be used in the future to assess the extent to which a sovereign cloud offering exists.

Cloud-based applications and on-premise solutions

The panel discussion that followed the keynote speech began with a conversation about the legal advantages and disadvantages of cloud-based applications on the one hand and on-premise solutions on the other. Dr. Meyer began by explaining that on-premise solutions are software applications that can be controlled and operated on a company's own systems and are sovereign. However, this also means that the respective company must guarantee the security of its systems. In contrast, a distinction must be made between different variants of cloud services, also with regard to the legal assessment. While a private cloud, for example, is only operated for a specific user, other systems (public cloud) are provided for a large number of users. Cloud services are also frequently offered as SaaS services. This has the advantage that the respective provider takes care of the system support and accordingly also of security-relevant aspects and the up-to-dateness of the systems. Prof. Roßnagel also referred to this and the benefits of professional safety management in his presentation. However, it is problematic

that many providers – even those who advertise a domestic service – sometimes use third-country subcontractors, which results in complex processing chains and greater dependence on the respective service provider. At the same time, however, Dr. Meyer also pointed to the expertise of a specialized service provider, which in turn could be seen as quite advantageous.

The question of the extent to which sovereign cloud models are also tailored to the needs of companies was then addressed. It was explained that corresponding models could also be usefully applied in the private sector. In the area of videoconferencing services, for example, open source solutions (e.g. Big Blue Button) could be implemented, or models could be used in which a service provider is interposed to operate a service such as Zoom on its own (inner-European) servers and control the service's access to the data. In addition, there are current efforts by major providers such as Microsoft and Google to work together with European providers to provide alternative applications that meet the data protection requirements for a sovereign cloud. In the future, the selection of data protection-compliant and sovereign cloud solutions could also be facilitated by corresponding certifications; options in this direction are currently being developed.

Relevant aspects when using cloud solutions
In the further course of the discussion, Dr. Rempe explained which aspects are particularly relevant with regard to the data protection-compliant use of cloud solutions and in the context of negotiations with the respective provider. He emphasized that it is definitely advisable to interpose a service provider from the point of view of data protection law as well as from the point of view of liability law. In addition, companies should always check and critically scrutinize the respective contract and terms of use as well as the data protection agreements and make sure that (additional) security measures are included. In this context, particular attention should also be paid to which subcontractors are used by the respective provider, as many European service providers also make use of subcontractors from third countries. In addition, companies should make use of their agreed rights, such as monitoring options, and also carry out checks if necessary.

Use of Microsoft 365
In the further course of the discussion, it was explained with regard to the use of Microsoft 365 that the DSK had identified and pointed out various problematic points in terms of data protection in the past. These had then been discussed in numerous meetings with Microsoft. However, the adjustments that Microsoft subsequently made in its agreement on commissioned processing did not result in any significant improvement in terms of data protection. Even using the latest supplementary paper, it is not possible to comply with the requirements of the GDPR, so that it is not possible to use the data in a manner that complies with data protection. Particularly critical in this respect was the fact that Microsoft was allowed to use the users' data for its own purposes, without it being clear what these purposes were and what specifically happened to the data.

Prof. Roßnagel also reported that there are currently no plans for systematic audits with regard to the use of cloud services, but that the aim is to support companies in using cloud services in a way that complies with data protection requirements. However, this does not mean that responsible companies cannot be confronted with an audit in individual cases. This would have to be done, for example, if citizens filed complaints with one of the data protection supervisory authorities. If necessary, sanctions could also be imposed in such cases, should companies not respond to the authorities' arguments.

New adequacy decision for the USA
According to Dr. Meyer's assessment, the new adequacy decision will not lead to more legal certainty, at least from a technical perspective, because data transfers will not immediately become more secure. From a risk-based perspective, the question arises as to the extent to which the new decision can be relied upon, or if it will once again be declared invalid by the courts. Dr. Meyer assumes in this respect that the ECJ will again refer to the lack of adequacy of the level of data protection in the U.S. and refer to its previous decisions. Moreover, the extent to which such an adequacy decision can be relied upon at all will still need to be clarified, since it has already been declared invalid several times and fundamental problems still persist. There is also the question of what relevance a new adequacy decision has at all. It would make data transfers to the USA easier; but at the same time, the use of American service providers would not be dispensed with in many cases at present – without an adequacy decision. Instead, attempts are being made to safeguard such data transfers by including standard contractual clauses and additional measures. In the future, a dual approach is conceivable in order to provide a safeguard in the event that this new adequacy decision too is not upheld.

With regard to the use of Microsoft 365, and taking into account the fact that the new adequacy decision will probably not mean a real breakthrough, Dr. Meyer also recommended making use of the options and configuration possibilities that are currently offered by Microsoft and, as far as currently possible, to safeguard oneself in this way. It would be advisable to carry out a comprehensive risk assessment for the specific case, taking into account the possible alternatives, and to document this before using the relevant products.

Cyber incidents

The second part of the event focused on issues surrounding cyber incidents - accountability and liability, legal coverage, insurance and criminal law aspects, and strategies for dealing with cyber incidents.

Keynote speech: Liability Risk Cyber Incidents
Dr. Schulte first presented the relevant threats in the area of cybersecurity in her talk, focusing in particular on the threat posed by ransomware. This involves attacks in which the company's data is encrypted by the attackers using a malware program and decrypted again upon payment of a ransom. She pointed out that both the number of attacks and the amount of the ransom demanded were steadily increasing. In addition, the attacks could also lead to business interruptions, loss of trade secrets, loss of reputation, and fines. She then outlined the various regulations relevant in this context that are intended to oblige companies to ensure IT security and prevent cyber incidents. These arise primarily from data protection law and directly from IT security law, but also from general civil law or contractual agreements. She made it clear that the legal obligations must be complied with not only by the management of a company or the IT security officer, but also by the individual employees. The same applies to service providers used by companies. Looking forward, Dr. Schulte referred to the regulations of the NIS II Directive, which will have to be taken into account in the future by companies from certain sectors - such as the healthcare sector and public services - in the area of IT security. The directive takes a cross-hazard and risk-based approach and, above all, will require intensified reporting obligations in the event of cyber incidents comparable to data protection law. In addition, the NIS Directive, like the GDPR, sets the groundwork for a significantly increased fine structure compared to the respective predecessor regulations.

Criminal law relevance
Mr. Weber-Blank, a specialist attorney for tax and criminal law at BRANDI in Hanover, provided impulses for the criminal law perspective during the ensuing discussion. Mr. Weber-Blank began with a report on the increasing relevance of IT-related matters to criminal law and the problem that, in his view, this area is not sufficiently mastered by the law enforcement authorities. He referred to the example of fake stores and spoke from experience that criminal prosecution is very lengthy and often not very successful. Among other things, the responsibility and lack of expertise of the authorities, the complexity of the issues and the difficulty of tracing their sources are problematic. Against this background, he pointed out how important it is to secure the IT systems of one's own company against cyber-attacks in advance.

In the further course of the discussion, the extent to which payment of the ransom in the event of a ransomware attack can also have consequences under criminal law was also addressed. Mr. Weber-Blank explained that a payment - comparable to the area of money laundering - could sometimes also be relevant under criminal law and recommended that, if necessary, the issue be examined in advance from a legal point of view and in particular from the aspect of money laundering.

Legal hedging options
Dr. Meyer then reported on the options and conditions for taking out legal, e.g. contractual, cover in the area of cyber incidents. At the outset, he made it clear that one should not expect too much from such legal protection, as it is generally not a real protection against such incidents, but can only ensure that the damage does not occur at one's own company, but at someone else's – such as the service provider. This would require a well-drafted contract that, on the one hand, specifically specifies the responsibilities of the respective service provider with regard to IT security and, on the other hand, regulates issues relating to the liability framework and insurance in the interests of the company. Taking this problem into account, it was also pointed out that the focus should be placed more on preventive measures.

Prof. Roßnagel reiterated the importance of taking preventive hedging measures. He also pointed out the general problem that in the event of a cyber-incident – specifically a ransomware attack – the IT systems are regularly infected by malware and that this problem persists regardless of legal protection or the payment of a ransom. The only solution in this respect is to reboot the systems.

In addition to addressing the question of the extent to which liability issues can be shifted to a service provider, the discussion also touched on the issue of managing director liability. This could have consequences under both criminal and civil law. In this respect, it is not sufficient for the management to appoint an IT security officer on a one-off basis. Instead, the management must continuously deal with the issue and keep an eye on the processes. Parallels could also be drawn at this point to the VW emissions scandal, in the context of which the management was also increasingly brought into focus with regard to liability issues.

Cyber insurance
In the further course of the discussion, the question also arose as to the advantages of cyber insurance and the aspects to be considered when taking out such insurance. Regardless of the specific insurance conditions, it is not always easy to obtain such insurance under attractive and affordable terms. The requirements of insurance companies are very high in this respect, and companies often have to prove that they are well-positioned from an IT law perspective. It therefore makes sense to be prepared and to list one's own security measures in advance, as well as to draw up an emergency plan. What is ultimately an attractive product depends on the needs of the company in each individual case. Dr. Meyer also pointed out that two aspects are particularly relevant when taking out cyber insurance - on the one hand, the subsequent insurance cover itself, and on the other hand, in particular, the prior examination of the company's own IT infrastructure and the hedging measures already taken or still required.

Cyber Competence Centers
Prof. Roßnagel also pointed out that there was a cyber-competence center in Hesse that companies could contact in the event of a cyber-attacks. This center would then provide advice and could also establish contacts with IT specialists. Dr. Meyer noted that such centers also existed in other federal states, but at the same time pointed out that such facilities could of course only provide assistance during their opening hours. If, for example, an incident occurs on a Friday afternoon or at the weekend, it is generally not possible to fall back on such assistance. In this context, Dr. Meyer also made it clear how important the time factor is in cyber-attacks and why it is important to be prepared for such incidents. To this end, it is helpful to practice emergency plans and procedures in advance.

Reporting obligations and fines
In the course of the discussion, it was further pointed out that in the event of cyber incidents, the data protection notification obligations under Articles 33 and 34 GDPR may also have to be considered. In addition to the obligations provided for in the GDPR, there are also other notification obligations in the area of IT security law that also need to be taken into account. Furthermore, the question of the extent to which customer information can also be useful independently of legal reporting obligations – also in order to prevent further damage – must be addressed in a timely manner.

With regard to the imposition of fines in the context of cyber incidents, Prof. Roßnagel made it clear that it is important to report relevant incidents in a timely manner pursuant to Articles 33 and 34 GDPR and to inform affected parties, as otherwise fines may be imposed for failure to report or inform. However, companies would not be fined for the notification itself, taking into account the nemo-tenetur principle. However, it cannot be ruled out that the report may draw attention to the company, and that an obligation for safety measures to be reviewed in the follow-up may arise. Dr. Meyer also pointed out in this context that it would be useful to use an incident of this kind as an opportunity to subject the hedging measures taken by the company to a general review.

BRANDI Young Lawyers Award

At the end of the event, current topics in data protection law were presented in short lectures by prospective lawyers as part of the BRANDI Young Lawyers Award.

User Tracking, Cookie Banner and Consent Management
The first presentation by Ms. Christina Prowald reported on the use of user tracking tools and the data protection requirements of the various legal sources as well as the case law that must be complied with when using them. As for any other data processing, the existence of a sound legal basis is especially required. In addition, users must be provided with comprehensive information on data protection law so that they can make informed decisions about the processing of their personal data and exercise their rights accordingly. For the use of cookies, it was clarified that, in principle, active user consent must be obtained. If other technologies are used, it must be determined to what extent the user's consent to the respective data processing is also required, or if the process can be justified

on another legal basis. In addition to designing the cookie banner in accordance with the legal requirements, care must also be taken to ensure that the user decision is also implemented correctly from a technical point of view. Ms. Prowald also discussed the new provision of Section 26 TTDSG, which contains regulations for consent management services and is intended to counter the cookie banner fatigue of many users, as well as the planned Consent Management Ordinance. She presented the advantages as well as problematic aspects of the new regulations and raised various data protection issues regarding the implementation of corresponding services.

Dealing with requests for information under data protection law

In the second presentation, Ms. Johanna Schmale went into more detail about the right of access according to Article 15 GDPR. This is an important aspect in the exercise of the right to informational self-determination. In this respect, it is necessary that data subjects are informed about the cases in which personal data is processed and what information is available about their own person at a controller. The right of access serves this circumstance as well as facilitating the assertion of other data subject rights. Ms. Schmale reported that the scope of the duty to provide information depends on the specific request of the data subject. She went on to explain that responsible bodies can be threatened with serious consequences if they do not respond to requests for information or do not respond in a timely manner, at the latest within one month. A coordinated and internally agreed procedure is therefore recommended to ensure a legally compliant response. The required information must be provided to the data subjects free of charge and in a precise, transparent, comprehensible and easily accessible form. In order to prevent the personal data of the data subject from being disclosed to an unauthorized third party, the identity of the inquirer must also be verified before the information is provided. In cases of doubt in particular, it also makes sense for the data protection officer to support the company in processing the request for information.

ECJ on damages under the GDPR

Mr. Lukas Ingold concluded by reporting on the current ruling of the European Court of Justice (ECJ) on the requirements for damages under the GDPR. In the original proceedings, the plaintiff had asserted a claim for damages against Österreichische Post AG because the latter had collected information about political preferences, defined "target group addresses" and attributed a certain party affinity to the plaintiff. This had caused the plaintiff to be annoyed and ashamed. The Supreme Court had then referred to the ECJ in a preliminary ruling procedure, among other things, the questions of whether a mere breach of the GDPR is sufficient to give rise to a claim for damages and whether it is a prerequisite for the claim that the infringement brings with it a consequence of at least some weight. Mr. Ingold reported that, in the opinion of the ECJ, concrete damage was required. In particular, the wording of Article 82 GDPR as well as various grounds for consideration and the systematic comparison with the right of appeal as well as the sanctioning by fines were cited as reasons. Furthermore, the ECJ denied a materiality threshold and in this respect also referred to the wording of Article 82 GDPR and EEC 146 as well as the uniform interpretation of the concept of damage. Furthermore, the criteria for determining the extent of damages were to be determined by the Member States themselves.

Conclusion

As part of our Data Protection Law Day, event participants commented on various data protection law issues surrounding the topic of "Data Protection in the Cloud and Cybersecurity". It became clear that the use of cloud solutions on the one hand brings advantages for the day-to-day activities of companies, but on the other hand also raises various data protection issues that require closer examination. With regard to the topic of cyber incidents, it became clear that, in addition to legal protection through appropriate contracts with the service providers and insurance companies involved, the focus should also be on preventive measures to ward off corresponding attacks.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 890
F +49 521 96535 - 113
M christina.prowald@brandi.net