BRANDI
RECHTSANWÄLTE

BRANDI-DATA PROTECTION LAW DAY ON THE TOPIC OF

"SECURITY BEGINS WITH DATA PROTECTION"

On May 24, 2024, Dr. Thilo Weichert, former head of the data protection supervisory authority in Schleswig-Holstein (ULD), and Prof. Dr. Eckhard Koch, Vice President for Research, Development and Transfer at FHDW Paderborn, were guests at BRANDI. As part of this year's Data Protection Law Day on the topic of "Security begins with Data Protection", our guests gave exciting insights into various data protection and IT security law topics, current procedures and their daily work in discussions with experts from BRANDI, including Dr. Sebastian Meyer, Dr. Christoph Rempe, Johanna Schmale, Dr. Carina Thull and Dr. Daniel Wittig.

Data subject rights and consequences of data protection violations

The first part of the event focused on issues relating to the rights of data subjects and the consequences of data protection violations.

Dr. Weichert gave an overview of the data subject rights and sanction options provided for in the GDPR in his keynote speech in line with the title of the first part. In particular, he addressed the transparency requirements and options for action of the supervisory authorities. Among other things, he pointed out the importance of transparent information for the persons affected by data processing and noted that there is often still room for improvement in this respect in practice. When providing information under data protection law, there is a tension between the need for detailed information on the one hand and easy comprehensibility on the other. He went on to explain that the right of access is the central fundamental right of data subjects. He dealt more specifically with the right to negative information, the freedom of purpose and the scope of the right of access. He also made it clear that identity verification is particularly important in practice, but often difficult, as there is a lack of functioning verification procedures in Germany. Another point Dr. Weichert highlighted was the right to compensation under Article 82 GDPR. He also outlined the requirements developed by the ECJ. With regard to the possible sanctions, he made it clear that not only the supervisory authorities, but also competitors or the consumer advice center, for example, can take action against violations. He also pointed out that a sanction could also be imposed by the supervisory authority issuing a warning against a company or a specific service and that, in his view, this is sometimes preferable in practice, taking into account the various difficulties in imposing and enforcing fines.

The proper handling of requests for information was then taken up again in the ensuing discussion in view of its high practical relevance. It was first emphasized that the type of information to be provided is in principle at the discretion of the controller. Nevertheless, all information requested by the data subject must be disclosed, unless the rights of third parties preclude disclosure. In this respect, it makes sense to seek dialog with the data subject. In this way, it is also possible to better identify any abusive requests. The practical implementation of identity verification was then discussed. It was pointed out that there are indeed technical procedures for verification, but that these have not been widely used to date due to their complexity or are themselves often not data protection compliant. In practice, the presentation of an identity card or the comparison of the request with existing data of the person concerned is most useful. In the case of persons known to the person responsible, a reply should be sent to their contact information already stored. Difficulties would arise in particular if the request could not be assigned to a specific person. In this case, however, an abstract declaration on data processing with the indication that more detailed information on the identity of the data subject is required for further information could be helpful. With regard to the scope of the right of access, the practical handling of restrictions in this regard, for example due to business secrets or the rights of third parties, was then discussed once again. The problem primarily concerns the disclosure of communications such as e-mails. In principle, such documents must be handed over if the other requirements are met. If necessary, editorial processing in the form of redactions must be carried out. In principle, it is recommended that personal data be stored in a structured manner in order to minimize the effort required in the event of disclosure. Finally, it was also discussed whether and for how long communication relating to incoming requests for information or deletion may be stored. It was stated that storage on the basis of legitimate interest is fundamentally permissible. With regard to the storage period, the classic limitation period of three years could be used as a guideline. Finally, with regard to the right to erasure, the importance of an erasure concept was emphasized at the end of the discussion. Without such a system, it is hardly possible to decide which data records must continue to be stored, for example due to retention obligations, and which data records must be deleted and when. The differentiation between different retention periods and the subsequent implementation of the deletion could be carried out practically by using different systems or by marking the different data records accordingly. The problem is that many software solutions do not provide sufficient functionalities for simple systematic deletion, which is why those responsible have to find another practical procedure, such as the manual storage of deadlines, at an early stage.

Data protection and new technologies

The second part of the event focused on issues relating to data protection and new technologies. Topics covered included the correct design of a cookie banner, the permissibility of pure subscription models and the correct use of artificial intelligence.

Prof. Dr. Koch spoke about the connection between data protection and cyber security in his keynote speech. He began by outlining various threats in the area of cyber security, including the risk of ransomware attacks, in which the attackers encrypt company data using a malicious program and decrypt it again in return for payment of a ransom. He made it clear how important it is for companies to be well positioned in the area of cyber security in view of the significant increase in the number of attacks and the level of damage, as well as the rapid development of new malware. He then outlined the historical development and geographical spread of cyber security and data protection and argued that cyber security and encryption have existed for a very long time and are widespread worldwide, while data protection is a relatively new topic. He concluded his presentation by pointing out that data protection has been a key factor in the further development of cyber security in recent years and will continue to be in the future, and that both topics are important success factors for digitalization.

The ensuing discussion began with an exchange on the development of requirements in the area of cookies and the data protection-compliant design of cookie banners. Among other things, the requirement for consent under the ePrivacy Directive, the development of tracking options, the failed introduction of Personal Information Management Systems (PIMS) for centralized consent queries and the permissibility of pure subscription models were discussed. In this context, a recent decision by the EDPB was also discussed, according to which the "pay or okay" procedure was only deemed permissible to a limited extent. In this respect, further developments by the supervisory authorities and in case law are to be expected in the near future. According to the current status, the data protection-compliant design of a cookie banner requires in particular the transparent presentation of the "Agree" and "Reject" options on the first page of the cookie banner. It is also important to provide the user with the information required for their decision. Further information could also be outsourced to the privacy policy, as long as the points essential for the decision are provided centrally in the cookie banner itself. The cookie banner must also be adapted to the respective end device on which it is to be displayed. In the future, the requirements could become even stricter if particularly sensitive data categories within the meaning of Article 9 GDPR are to be processed using cookies.

The topic of cybersecurity was then addressed once again with regard to the mandatory technical and organizational measures to be taken in accordance with Article 32 GDPR. In this respect, it is particularly important for companies to have an access authorization concept in place in order to be able to control who accesses the data and to what extent. In addition, it should also be logged and checked who has actually accessed the data. It also makes sense to store data in encrypted form on the (external) systems used by the company, such as servers or clouds. It is also important to sensitize employees to the legally compliant handling of data, for example through training measures or IT security guidelines.

BRANDI-Young Talents Round

At the end of the event, current data protection topics were presented in short talks by prospective lawyers as part of the Young Talents Round.

Christina Prowald and Gesche Kracht began by reporting on the topic of "Employer access to employees' email accounts". They first discussed the requirements under data protection law and explained in particular which legal bases can be used to justify such access depending on the case. This was followed by an examination of the question of whether, in addition to the provisions of data protection law, telecommunications secrecy must also be observed if employees are permitted or at least tolerated to use their email accounts privately. Until final clarification, it is advisable to expressly regulate the issue internally within the company, at best to prevent private use or alternatively to be exempted from the restrictions of telecommunications secrecy. Finally, the speakers discussed how to proceed in the event of access due to temporary or permanent absence of an employee and due to abusive behavior and gave recommendations for the practical handling of access requests. In this respect, it is advisable to regulate the topic in advance and to specify measures such as setting up an out-of-office note or forwarding or saving relevant information in a central storage location. If access is nevertheless necessary, care should be taken to ensure that the inspection is only carried out to the extent necessary by sensitized employees in accordance with the "multiple-eye principle" and that this is also logged. A prior assessment by the data protection officer is generally recommended.

In the second presentation, Carolina Vortkamp reported on the decision of the Federal Court of Justice on the right to a copy of data in accordance with Article 15 (3) GDPR. After a brief introduction to the facts of the case and the course of the proceedings, she focused on the reasons for the BGH's decision. The latter is of the opinion that personal data exists if information of any kind is given about a person. This can be assumed if the information is linked to a specific person due to the content, purpose or effect of the information. In this respect, letters from the data subject to the controller are to be classified as personal data in terms of their entire content, as their own statements or writings are generally linked to the person making the statement. As a result, there is a right to receive a copy of the entire document. However, in the case of documents that do not originate from the data subject himself, only the personal data actually contained therein is covered by the right of access, so that there is only a right to receive a copy of the data contained therein, not the entire document. Something else only applies if the contextualization is necessary in order to understand the data processing and to be able to make use of his rights.

Hendrik Verst concluded by reporting on the use of Microsoft 365 in the company. He explained that from a data protection perspective, an agreement on data processing must be concluded in addition to the license agreement. The problem is that Microsoft's market power means that there is no room for negotiation and, as a result, the standard contract of Microsoft must be concluded. In this respect, the supervisory authorities criticized the lack of transparency in the presentation of the data processing taking place, the data processed and the data subjects, the inadequate delimitation of responsibilities and the lack of instruction and control options. In practice, it is advisable to conclude the latest version of the agreement, use the technical configuration options and thus limit the outflow of data to Microsoft, prepare comprehensive documentation and, if necessary, take additional measures, for example to encrypt the data.

Further information on the 5th BRANDI-Data Protection Law Day and the individual contents can also be found on our website.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net