BRANDI
RECHTSANWÄLTE

BRANDI Data Protection Law Day on the topic of

„DATA PROTECTION AND DIGITALISATION"

Information on data protection I July 2025

Introduction

Prof. Ulrich Kelber, former Federal Data Protection Commissioner, was a guest at BRANDI for the sixth Data Protection Law Day on May 16, 2025. As part of the event on the topic of "Data protection and digitalisation", Prof. Kelber gave an interesting insight into current issues and developments in the field of AI and his work as Federal Data Protection Commissioner in a discussion with BRANDI lawyers, including Dr. Sebastian Meyer, Dr. Christoph Rempe, Dr. Daniel Wittig and Dr. Christoph Worms. As announced (see June newsletter), we would like to look back at the Data Protection Law Day in this main topic and provide an insight into the expert discussions and presentations in the form of a summary.

Data protection and AI

The first part of the event was dedicated entirely to the central topic of the compatibility of data protection and AI.

In his keynote speech, Prof. Kelber gave an overview of data protection issues, regulatory challenges and how to deal with current legal uncertainties. According to Prof. Kelber, the political discourse in the European Union has recently seen a change in attitude from strong data protection to increasing data use driven by economic considerations. Of the legal regulations at EU level, the AI Regulation is currently at the centre of the discussion. In turn, the AI Regulation and GDPR are not congruent – one focuses on the type of processing, the other on the type of data processed. Nevertheless, a certain parallelism can be recognised, e.g. in transparency and accountability obligations, which could result in synergy effects. Likewise, many documentations could be created in parallel due to overlaps.

Prof. Kelber then presented the main features of the AI Regulation, which follows a risk-based approach, and made it clear that most AI tools are not subject to any special requirements under the AI Regulation, as they are largely classified as systems with minimal risk. Only the so-called high-risk systems are subject to special regulation, for which there are various separate obligations, such as the introduction of a risk management system and a fundamental rights impact assessment.

The former Federal Data Protection Commissioner then reported on the requirements of data protection law in relation to AI systems and current issues. The use of AI is data processing and is therefore only permitted on a legal basis if personal data is involved. However, consent in accordance with Art. 6 (1) (a) GDPR is particularly problematic and complex when it comes to AI. For example, training data is often obtained from sources for which no consent is given.

When using an AI system, in addition to objective requirements for data processing, such as integrity and confidentiality, the rights of data subjects under the GDPR must also be observed. Uncertainties exist in particular with regard to the right to rectification pursuant to Art. 16 GDPR, the right to erasure pursuant to Art. 17 GDPR and the right to object pursuant to Art. 21 GDPR. The topic of "unlearning" of AI systems, which is necessary to implement erasure or an objection, has not been sufficiently researched and is not very practicable. Prof. Kelber sees the need for legal concretisation here. Art. 22 GDPR is also relevant, according to which every data subject has the right not to be subject to a decision based solely on automated processing. It is currently not completely clear when a decision is fully automated. The national allocation of supervisory responsibilities is also still outstanding, with Prof. Kelber pointing out the problem of the fragmentation of competences and the duplication of responsibilities. Future developments in this regard remain to be seen.

Prof. Kelber concluded by saying that he sees great potential for facilitating and accelerating work assignments through specialised AI and that a discussion of the requirements for the use of AI is therefore recommended.

Discussion: Data protection and digitalisation

The presentation addressed various questions from the field of digitalisation, in particular on the topic of AI, which were then further explored and discussed in the panel discussion. Firstly, it was discussed what actually qualifies as an AI system. The transition between a simple data processing system and so-called weak artificial intelligence is fluid. Key criteria would be the flexibility of the system in relation to changes and autonomy. There is also sometimes a discrepancy between what is labelled as AI by companies or perceived as such by customers and the systems that actually fall under the AI regulation. This can only be countered through transparency and education, whereby the problem is that many users of AI themselves are provided with little information about the system by the manufacturer. Employees also need to be sensitised to the use of AI. This is the only way to ensure legally compliant behaviour.

The issue of certifying AI tools was also emphasised with regard to the legally compliant use of AI. By certifying systems, users could

assume that they are acting in accordance with the law when using AI, which could counteract the uncertainty that currently exists in some cases. However, difficulties would arise in this respect due to the lack of standardised certification procedures under the GDPR.
The problem of overlapping supervisory competences and how controllers deal with this was also addressed during the discussion. There was a need for improvement on the part of the supervisory authorities with regard to the exchange of information, the right to transfer data and the recognition of audit results from another supervisory authority. It would be desirable to have standardised, all-encompassing documentation that could be used vis-à-vis the various supervisory authorities. However, without legislative action, the possibilities in this regard are currently limited.
The specific example of the collection, processing and presentation of information on websites, which also includes personal data such as sports competition results, was then discussed. The media privilege was cited here in favour of data processing. The question arises as to whether data subjects should expect to be found with this data on the internet anyway and whether the level of protection would be lowered as a result. On the other hand, there would probably be a justified expectation that information published for a small target group would not be found so easily. In the digital age, the delimitation of journalistic services that could invoke the media privilege is also made more difficult by the diversity of information offerings.
A comparable demarcation difficulty exists in the case of decision-making based exclusively on automated processing in accordance with Art. 22 GDPR. In the context of frequent hybrid collaboration with AI, the question arises in particular as to how much human decision-making leeway is required for decision-making not to fall under Art. 22 GDPR. The diagnosis of an expert system in the healthcare sector was cited as an example, based on the evaluation and recommended decision of which employees make a decision. Liability issues must also be taken into account if a decision is made that differs from the result of the system. Transparency of the decision-making process also plays a major role.
Finally, general aspects of liability and risks for companies in the event of a breach of the GDPR and the AI Regulation were discussed. In particular, the question was raised as to what rights data subjects have - apart from the rights of data subjects under Art. 12 f. GDPR - vis-à-vis the companies responsible. In any case, this is limited in relation to private controllers. Case law does not assume a direct claim to the implementation of certain data protection measures. The obligation to implement specific measures is also inconceivable, as the adequacy of the level of protection is determined by the sum of the measures. Therefore, only the diversions via a claim for damages remains open, which could indirectly force those responsible to implement certain measures through financial constraints. However, a corresponding claim against public authorities was assumed in a court decision due to the monopoly on the use of force. Equally, there are powerful private actors with a comparable monopoly position, so that ultimately the individual case is likely to be decisive. The implementation of a new AI liability directive under EU law also remains to be seen.

Case studies on data protection law

At the end of the event, lawyers and research assistants from BRANDI gave short presentations on various case studies.

Responsibility for multi-level processing systems

Dr. Jan Peter Möhle and Mr. Schwarzenberg began by reporting on the topic of "Responsibility in multi-level processing systems using the example of a ticket purchasing system". In particular, they discussed the different responsibility concepts in the GDPR and the distinction between order processing and joint responsibility using the example of cloud services. They described the concept of commissioned processing as being characterised by the subordination of the processing of the data within the processor's sphere of control to the purposes and will of the client, with the processor only having an auxiliary function. In contrast, joint controllership exists if a joint decision is made on the means and purposes of data processing. Mr. Möhle and Mr. Schwarzenberg then drew attention to the fact that the distinction ultimately depends not on the contractual arrangement, but on the actual relationships between the companies involved. If data processing consists of several processing phases, these must be assessed individually, so that partial order processing and partial joint responsibility can also result with regard to the entire data processing operation. The distinction is sometimes not easy, which is why a precise examination of the specific circumstances of the cooperation is necessary, especially taking into account the obligations arising from the different concepts and the sanctions that may be imposed in the event of non-compliance with the requirements.

Data protection classification of the framework conditions of AI tools

In the second presentation, Ms. Johanna Schmale and Ms. Gesche Kracht reported on the data protection classification of selected framework conditions of AI tools. After a brief introduction to the requirements for the use of AI tools resulting from the AI Regulation and the GDPR, the two speakers used various clauses from the terms of use and privacy policies of the Deep Seek, ChatGPT and Mistral services to highlight key data protection challenges. With regard to the data protection principle of purpose limitation, it is particularly problematic that the AI tools use the users' data, including in particular the data entered by them, for a wide variety of own and sometimes unspecified purposes and that there are often subsequent changes of purpose. Challenges would also arise in this respect with regard to the principle of transparency, the information obligations arising from Articles 13 and 14 GDPR and the data subject's right to information. The transfer of data to third countries in the course of using the tool could also prove to be problematic if this is not adequately secured. In practical terms, there is also the question of how data entered into the system can be filtered out again in the event of a deletion request. Ms. Schmale and Ms. Kracht then noted that in some cases, protection under data protection law could be achieved by concluding a data processing agreement with the respective service provider. A review of the agreement with regard to unfavourable clauses is recommended in any case. As part of the introduction of the AI tool, care should also be taken to ensure that employees are sensitised to the issue and trained in the specific use of the tool.

Manipulation of invoices sent electronically

Finally, Mr. Harold Derksen and Mr. Habib Majuno reported on the manipulation of electronically sent invoices based on a judgement by the Higher Regional Court of Schleswig. After a brief introduction to the facts of the case and a technical excursus on "man in the middle" attacks, the two speakers focussed on the reasons for the court's decision and the practical implications. In the case underlying the decision, an invoice sent by the plaintiff by email had been intercepted by a third party in an unexplained manner and manipulated, particularly with regard to the IBAN stated in the invoice. As a result, the defendant did not transfer the invoice amount to the plaintiff, but to an unknown third party. The question was whether the plaintiff could demand renewed payment from the defendant. The Higher Regional Court of Schleswig answered this question in the negative, as it was of the opinion that the defendant was entitled to claim damages in the amount of the payment made to the unknown third party under Art. 82 (1) GDPR due to the lack of end-to-end encryption of the email. A breach of data protection law pursuant to Art. 32 GDPR exists, as pure transport encryption does not

guarantee sufficient protection against attackers. Interception and manipulation of emails can only be effectively countered by means of end-to-end encryption. The court also considers it sufficient that unauthorised access to the defendant's data was also possible when the plaintiff's account details were manipulated. Although the decision of the Higher Regional Court of Schleswig can be criticised from various points of view, it can be taken as a practical lesson that companies should question their security standards when sending invoices. It is advisable to choose secure email encryption and a secure transmission method, use digital signatures, send PDF files with password protection and sensitise the company's employees to the issue. Detailed information on this topic can be found in the main topic of the June newsletter.

Gesche Kracht / Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Gesche Kracht
Research Associate

T +49 521 96535 - 984
F +49 521 96535 - 113
M gesche.kracht@brandi.net

Christina Prowald
Research Associate

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