

2023

2024

ANNUAL REVIEW

2023 AND OUTLOOK 2024

Information on data protection | January 2024

Introduction

In 2023, data protection law was characterized by various decisions by authorities and courts. In particular, issues relating to the right of access under Article 15 GDPR and the right to compensation under Article 82 GDPR were discussed last year. In addition, topics such as the use of tracking tools and cookie banners as well as the transfer of data to third countries continued to be relevant. The European Commission has adopted a new adequacy decision for the EU-US Data Privacy Framework for data transfers to the USA. The Whistleblower Protection Act (HinSchG) also came into force in July 2023. According to this law, companies that generally employ at least 50 people or perform certain activities have been obliged to set up an internal reporting office since December 17, 2023, through which employees can report legal violations. As the implementation of the requirements involves the processing of personal data, the data protection regulations must also be complied with and documented in this context.

Our BRANDI-Data Protection Law Day took place for the fourth time on May 12, 2023. As a guest of BRANDI in Bielefeld we were honored to have Prof. Dr. Alexander Roßnagel, Hessian Commissioner for Data Protection and Freedom of Information (HBDI). We exchanged views with Prof. Dr. Roßnagel on various issues relating to data protection in the cloud and cybersecurity. In conversation with lawyers from BRANDI, he gave an exciting insight into various data protection issues, current procedures and the daily work of the Hessian Data Protection Supervisory Authority and the Data Protection Conference (DSK).

We have taken the turn of the year as an opportunity to review the main topics and particularly relevant developments and events of the past year in our traditional annual review. We also venture a look ahead to the new year 2024.

Main topics of the data protection newsletter from BRANDI

In our monthly data protection newsletter, we report on current events in data protection law. In each main topic, we also provide in-depth information on a selected data protection law topic, summarize the relevant aspects and special features from a data protection law perspective and provide practical tips. We have summarized the main topics of our data protection newsletter from 2023 for you below:

[Procedure in the event of data protection incidents](#)

[Requirements for sending newsletters](#)

[Data protection requirements for the use of AI tools](#)

[User tracking, cookie banners and pure subscription models](#)

[BRANDI Data Protection Law Day on the topic "Data Protection in the Cloud and Cybersecurity"](#)

[Data protection in the implementation of the Whistleblower Protection Act](#)

[Third country transfers - new adequacy decision for the U.S.](#)

[Data minimization, storage limitation and data deletion](#)

[Protection of personal data of minors](#)

[Video surveillance](#)

[Processing of health data](#)

Many of these topics have their origins in current cases from our consulting practice or refer to statements and information published by the supervisory authorities or court decisions and are particularly relevant in practice.

Case law

Below you will find some particularly relevant court decisions from 2023, sorted by topic and instance.

In January 2023, the European Court of Justice (ECJ) initially ruled on the highly controversial question of whether it is sufficient in the context of a request for information under Article 15 GDPR to merely name the categories of recipients in the case of disclosure of data to third parties or whether the recipients must be named individually ([ECJ, decision dated 12.01.2023 - Ref. C-154/21](#)). The court stated that the controller is obliged to inform the data subject in detail about the identity of the recipients as part of the request for information. It bases this in particular on the principle of transparency. The data subject must be able to check whether their data is being processed and disclosed in a lawful manner. In a further decision from May 2023, the ECJ also commented on the scope of the right to information. It ruled that the right to receive a "copy" of their personal data must be understood to mean that the data subject receives a faithful and intelligible reproduction of all their data ([ECJ, decision dated 04.05.2023 - Ref. C-487/21](#)). According to the ECJ, this also includes copies of documents or extracts from databases,

insofar as the provision of such copies is essential to enable the data subject to effectively exercise their rights, provided that the rights and freedoms of others are taken into account. In this respect, the term “copy” does not refer to a document as such, but to the personal data it contains, which must be complete. The data subject must not only be able to check whether their data is correct, but also whether it is being processed in a lawful manner. In particular, if personal data is generated from other data or is based on missing information, the respective context is required in order to obtain transparent and comprehensible information. In June 2023, the ECJ also ruled that everyone has the right to know at what time and for what reasons their personal data was collected ([ECJ, decision dated 22.06.2023 - Ref. C-579/21](#)). The ECJ stated that information concerning queries of personal data and relating to the timing and purposes of these processes is information that the data subject may request from the controller on the basis of Article 15 GDPR. However, the GDPR does not provide for a right to know which employee carried out the corresponding queries unless the information is essential to enable the data subject to exercise their rights, and only if the rights and freedoms of employees are sufficiently taken into account. In its reasoning, the ECJ points out that the right of access is characterized by the wide range of information that can be requested. At the same time, it emphasizes that a balance must be struck in the event of a conflict between the rights and freedoms of different persons. In April 2023, the Advocate General of the ECJ also commented on the assertion of the right of access for reasons unrelated to data protection ([Opinion dated 20.04.2023 - Ref. C-307/22](#)). He explained that the data controller is obliged to provide the data subject with a copy of their personal data even if the data subject requests the copy for reasons unrelated to data protection. In his opinion, the right of access is not dependent on whether the data is to be used for data protection purposes. In October 2023, the ECJ agreed with the Advocate General’s opinion ([ECJ, decision dated 26.10.2023 - Ref. C-307/22](#)) and ruled that the controller’s obligation to provide the data subject with a first copy of their personal data free of charge also applies if the request in question is based on a purpose other than those stated in recital 63 of the GDPR. Neither according to the wording of Article 12 GDPR nor Article 15 GDPR is the provision dependent on the data subject justifying his or her request. Recital 63 cannot be interpreted to the effect that a request must be rejected if it has a purpose other than to take note of the processing and verify its lawfulness. In contrast, the Higher Regional Court of Brandenburg ruled in June 2023 that it is an abuse of law for a customer to assert a claim for information under data protection law against their insurance company in order to check whether a premium increase is lawful ([OLG Brandenburg, decision dated 16.06.2023 - Ref. 11 U 9/23](#)). In this respect, it pointed out that the purpose of the right of access is to enable data subjects to check whether the data concerning them is correct and is being processed in a lawful manner. If the request for information is not based on a data protection objective or any other legitimate purpose, the request must be classified as an abuse of rights in the opinion of the court. In August 2023, the Regional Court of Kleve also rejected an obligation to provide information because the focus was not on the information requested, but on an irrelevant motive (LG Kleve, decision dated 10.08.2023 - Ref. 6 O 143/22, juris). The court stated that the right to information was ruled out because the applicant was not seeking to verify the lawfulness of the data processing or to assert further claims under data protection law. Furthermore, in September 2023, the BGH rejected a right of access under Article 15 GDPR in the case of an irrelevant motive ([BGH, decision dated 27.09.2023 - Ref. IV ZR 177/22, press release of 27.09.2023](#)). It based its decision on the fact that the requested information is not personal data. A right to a copy of the data within the meaning of Article 15 (3) GDPR only exists in relation to data to which information must be provided in accordance with Article 15

(1) GDPR. The disclosure of copies of certain documents is not the subject of the claim. Article 15 cannot be interpreted in such a way as to grant a different right in para. 3 than that provided for in para. 1.

In May 2023, the ECJ ruled that a mere breach of the GDPR does not justify a claim for damages ([ECJ, decision dated 04.05.2023 - Ref. C-300/21](#)). It stated that the claim for damages provided for in the GDPR provides for three connecting factors which must be cumulative: a breach of the GDPR, material or immaterial damage and a causal link between the damage and the breach. The court also found that the claim for damages is not limited to immaterial damage that has exceeded a materiality threshold. Such a requirement does not arise from the GDPR, nor is it compatible with the broad understanding of the concept of damage. The amount of damages is to be determined on a case-by-case basis, whereby the principles of equivalence and effectiveness must be observed. In September 2023, the BGH once again referred questions to the ECJ for a preliminary ruling on the concept of non-material damage within the meaning of Article 82 GDPR (BGH, decision dated 26.09.2023 - Ref. VI ZR 97/22, [press release of 26.09.2023](#)). He wanted to know whether non-material damage can be justified merely by negative emotions and whether, on the one hand, the degree of fault and, on the other, the fact that the person concerned is entitled to injunctive relief should be taken into account when assessing the amount of non-material damage.

In March 2023, the Regional Court of Cologne criticized Telekom’s cookie banner ([LG Köln, decision dated 23.03.2023 - Ref. 33 O 376/22](#)). It pointed out that the voluntary nature of consent presupposes that the consumer has a genuine choice when giving consent and is not unilaterally steered towards consent by the design of the cookie banner. While the option to accept the cookies was designed to be clear and eye-catching, the option to refuse was hidden within the body text. In the opinion of the court, the size, shape and design of such a design is not sufficient to be considered an equivalent option. Furthermore, a „Change settings“ button was not an unmistakable indication of an alternative option to opt out. The Regional Court of Cologne also ruled that the integration of Google Analytics on Telekom’s website was inadmissible, as this resulted in an inadequately secured transfer of data to the USA. In the opinion of the court, the data transfer could not be justified solely by the conclusion of standard data protection clauses, as this does not guarantee a level of data protection in accordance with the GDPR and the clauses do not protect against access by the authorities in the USA. In March 2023, the Regional Court of Munich I also ruled that the mass assertion of injunctive relief and claims for damages due to the integration of Google Fonts on websites is an abuse of rights and that the respective request is therefore unfounded (LG Munich I, judgment of 30.03.2023 - Ref. 4 O 13063/22). The court first determined that the dynamic integration of Google Fonts and the transmission of the IP address to the USA without compelling technical reasons and without consent constitutes a violation of the right to informational self-determination. This presupposes personal involvement, which could not be determined in the case in question, as the plaintiff did not visit the affected pages himself but rather used software to do so and provoked the infringement himself. Also in March 2023, the Higher Regional Court of Frankfurt ruled that a data subject is not entitled to injunctive relief against an online store if the latter transmitted the data subject’s personal data to third-party services such as Google Tag Manager, Google Fonts, YouTube and Facebook ([OLG Frankfurt, decision dated 30.03.2023 - Ref. 16 U 22/22](#)).

Activities at EU level

In January 2023, the European Data Protection Board (EDPB) com-

mented on the issue of cookie banners and reaffirmed its commitment to the harmonized application of regulations in the EU ([press release of 19.01.2023](#)). To this end, a task force was recently set up to coordinate responses to complaints about cookie banners. The report published in January contains, among other things, descriptions of various cookie banner designs and assessments of their admissibility.

In March, the EDPB also published guidelines on the right of access in accordance with Article 15 GDPR, which are intended to achieve a uniform implementation of the right of access within the EU. The EDPB describes that the general objective of the right of access is to provide data subjects with comprehensive and transparent information about the processing of their personal data and to enable data subjects to check the lawfulness of the processing and, if necessary, to assert further rights. In addition, the committee provides an overview of the structure of the regulation as well as the key principles and examines various issues relating to the right of access in more detail.

In July 2023, the European Commission adopted a new adequacy decision for the EU-US Data Privacy Framework. It determined that the United States ensures an adequate level of protection for personal data transferred from the EU to US companies under the new data protection framework. In order for a data transfer to an American company to be based on the adequacy decision, the company must participate in the new data protection framework and join the agreement. The European Commission and the US had already reached an agreement in principle on a new transatlantic data protection framework in spring 2022. After Joe Biden then signed a decree in October 2022 that created the legal basis for a new legal framework for data transfers to the US, the European Commission presented a draft adequacy decision in December 2022 and initiated the procedure. Subsequently, various bodies in the EU, including the [EDPB](#) and the [responsible committee of the EU Parliament](#), commented on the draft. According to the [European Commission](#), the new adequacy decision will allow personal data to be transferred securely to US companies participating in the Data Privacy Framework without the need for further data protection guarantees.

Activities of supervisory authorities

In 2023, the data protection supervisory authorities of the EU member states once again addressed various data protection issues. In addition to the imposition of fines for data protection violations, the focus was also on the publication of statements and notices on selected topics. The EDPB also published [guidelines on the calculation of fines](#) in July 2023. The guidelines are intended to harmonize the methodology used to calculate fines and create efficient cooperation between data protection authorities in cross-border cases. The calculation focuses in particular on the categorization of infringements according to their type, the severity of the infringement and the company's turnover.

Fines

Because there was no easy way to reject technically unnecessary cookies when searching with Bing, the French supervisory authority (CNIL) imposed a fine of 60 million euros on Microsoft in December 2022 ([press release of 22.12.2022](#)). CNIL based the amount of the fine on the scope of the data processing, the number of data subjects and the profits the company made from advertising revenue generated indirectly from the data collected using cookies.

In January, March and May 2023, the Irish Data Protection Commission (DPC) imposed fines on Meta Platforms Ireland Limited. The Group received the first fine of 390 million euros in connection with the provision of its Facebook and Instagram services ([press release](#)

[of 04.01.2023](#)). In particular, the DPC stated that Meta was not entitled to rely on the legal basis of contract performance in connection with the provision of behavioral advertising, and that the previous data processing constituted a breach of Article 6 GDPR. The second fine in the amount of 17 million euros concerned inadequate technical and organizational measures in connection with the protection of EU users' data ([press release of 15.03.2023](#)). The third fine of 1.2 billion euros was the highest fine ever imposed on the company in the EU ([press release of 22.05.2023](#)). The content of the fine concerned the question of the legal basis on which Meta transfers personal data to the USA in connection with the provision of its Facebook service. The DPC ruled that Meta violated Article 46 (1) GDPR when it continued to transfer personal data to the USA after the ECJ's Schrems II decision, as the standard contractual clauses used by Meta in combination with the additional measures taken by the company to secure them were not sufficient.

In May, the Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI) imposed a fine of 300,000 euros on DKB for a lack of transparency regarding an automated individual decision ([press release dated 31.05.2023](#)). The bank refused to provide a customer with information about the automated rejection of his credit card application. DKB had not complied with the specific transparency obligations of the GDPR in relation to automated decisions.

In August, the BlnBDI imposed four fines totaling 215,000 euros ([press release dated 02.08.2023](#)) because a company had inadmissibly documented sensitive information about the health of individual employees or their interest in forming a works council in a list. These four fines were related to the processing of employee data for the purpose of creating the list, the failure to involve the data protection officer in the creation of the list, the late notification of a data breach and the failure to mention the list in the list of procedures.

Comments and notes

In order to create more clarity and legal certainty when using processors, the State Commissioner for Data Protection and Freedom of Information Baden-Württemberg (LfDI) approved the national code of conduct [„Requirements for processors under Article 28 GDPR - Trusted Data Processors“](#) in November 2022. According to the LfDI, making a voluntary commitment to the code of conduct can help processors demonstrate to the outside world that they follow the standards set out in the code of conduct and submit to monitoring by the monitoring body accredited by the LfDI.

In July 2023, the State Commissioner for Data Protection of Lower Saxony (LfD), together with other German data protection supervisory authorities, carried out a [coordinated review of the websites of 49 media companies](#). In particular, the new provisions of the TTDSG were taken into account and the use of so-called pure subscription models was examined. The comprehensive legal assessment was published in a corresponding resolution by the DSK, which, among other things, shows the fundamental permissibility of pure subscription models. In particular, it criticized the setting of cookies before the consent query, missing information, an insufficient scope of consent, manipulation of users and the lack of a button to reject cookies.

After the European Commission adopted the adequacy decision for the EU-US Data Privacy Framework in July 2023, the DSK published [application notes](#) in September 2023. In addition to an introduction to the topic of data protection in third country transfers and the relevant regulations, the document contains information for data exporters who transfer data to the USA and information for data

subjects regarding the legal protection and complaint options to which they are entitled.

In October 2023, the State Commissioner for Data Protection and Freedom of Information NRW (LDI NRW) issued [guidance](#) for data controllers on concluding a data processing agreement with Microsoft for the use of „Microsoft 365“. The main recommendations are highlighted in the document as „To-Do’s“. The LDI NRW also points out that, in addition to the mere drafting of the contract, responsible companies must also deal with all other aspects of data protection law, such as TOM.

Outlook 2024

Various data protection issues from previous years, such as the data protection-compliant use of Microsoft 365 or the legally compliant design of cookie banners and the use of tracking tools, will continue to play a role in 2024. New data protection issues can also be expected.

At the beginning of August 2023, the Federal Ministry of the Interior and for Home Affairs published the [draft of a first law to amend the Federal Data Protection Act](#). Over the course of the past year, various bodies, including the [DSK](#) and the [state data protection supervisory authorities](#), have commented on the draft. It remains to be seen which amendments will be adopted and when they will come into force.

The European Parliament, the Council of the European Union and the European Commission reached a compromise on the planned AI Regulation in their trilogue negotiations on December 9, 2023 ([press release of 09.12.2023](#)). The agreed text must now be formally adopted by both the Parliament and the Council in order to become EU law. The responsible parliamentary committees will vote on the agreement in one of the next sessions. With regard to the ePrivacy Regulation, which aims to strengthen the confidentiality of electronic communications, there have been no significant changes to date.

The BRANDI data protection team will of course keep you up to date on the data protection events and challenges that 2024 will bring with it in the new year. We would also like to invite you to our next Data Protection Law Day, as has become a tradition. The event will take place on May 24, 2024 in Paderborn. You can already look forward to interesting presentations and exciting discussions. Among others, we will be discussing with Dr. Thilo Weichert, who, as a long-standing jury member, helps to decide on the presentation of the annual Big Brother Awards, the “Oscars for data leeches”. Dr. Weichert is one of Germany’s best-known data protection experts and former head of the data protection supervisory authority in Schleswig-Holstein (ULD).

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