REVIEW OF THE YEAR 2022 AND OUTLOOK 2023

Information on data protection I January 2023

Introduction

In 2022, data protection law continued to be shaped by various decisions of the authorities and courts on data protection, while the official legal framework remained unchanged. Many decisions relate to the increasing processing of personal data in the course of our society's digital transformation. The Corona situation has somewhat eased in the past year, but developments caused by the pandemic, such as working from home and the increased use of online tools to conduct video conferences or to work on documents and projects together, for example, were still highly relevant for companies.

On September 15, 2022, our BRANDI Data Protection Law Day took place for the third time. This year, Mr. Carl Christoph Möller, in-house lawyer and consultant for data protection & data security at the consumer advice center NRW, was a guest at BRANDI in Bielefeld. We talked to Mr. Möller about the topic of "Data Protection Incidents – Stakeholders, Consequences and Safeguards". We gained exciting insights into various data protection topics, current procedures and the daily work of the consumer advice center. Since February 2022, we have also made our data protection newsletter available in English.

We have taken the start of a new year as an opportunity to bring together the main debates and particularly relevant developments and events of 2022 in our traditional annual review, while also venturing an outlook on the year ahead.

Main topics of the data protection newsletter from BRANDI

In our data protection newsletter, we report every month on current events in data protection law. In the respective main topic, we also provide in-depth information on a selected data protection topic and summarize the relevant aspects and special features from a data protection perspective, as well as provide practical tips. We have summarized the main topics of our 2022 data privacy newsletter for you once again below:

> Current developments on data protection regarding the use of Google Analytics
>
> The right of access under data protection law
>
> Direct advertising and data protection
>
> Data processing based on legitimate interests
>
> Data transfers within organizations
>
> Employee data protection – general principles
>
> Data protection in online trade
>
> New guidelines on the calculation of administrative fines
>
> BRANDI-Data Protection Law Day on the topic "Data Protection Incidents"
>
> Transparency of data processing
>
> Employer access to employee e-mail accounts

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

Jurisdiction

Below you will find – sorted thematically and by instance – some particularly relevant court decisions from 2022.

In April 2022, the European Court of Justice (ECJ) ruled that European Union law precludes national legislation that allows the general and indiscriminate retention of traffic and location data relating to electronic communications for the purpose of combating serious crime (ECJ, judgment of 05.04.2022 – Ref. C-140/20, see also the ECJ press release). The ECJ pointed out that data retention could only be considered under certain, narrowly defined conditions, thus confirming its established case law on this subject. In another decision from September 2022, the ECJ ruled that the German regulation on data retention also violates Union law (ECJ, judgment of 20.09.2022 – Ref. C-793/19, C-794/19). In its decision, the ECJ again stated that general and indiscriminate data retention of traffic and location data is not compatible with EU law unless there is a serious threat to national security. The ECJ justified its decision by stating, among other things, that the German regulation allows very precise conclusions to be drawn about the private lives of the persons concerned and, above all, permits the creation of profiles of these persons.

In June 2022, the ECJ came to the conclusion in a decision that a national special protection against dismissal, which generally excludes an ordinary termination of the employment relationship of a data protection officer, irrespective of whether it occurs because

of the performance of his duties, does not conflict with the provisions of the GDPR (ECJ, judgment of 22.06.2022 – Ref. C-534/20). The case on which the decision was based involved the termination of an employee appointed as internal data protection officer due to a restructuring measure. In justification, the ECJ referred to the objectives of the GDPR and in particular of Article 38 (3) (2) GDPR, which aims at the functional independence of the data protection officer as well as at ensuring that the provisions of the GDPR are complied with.

In its decision of March 2022, the German Federal Court of Justice (BGH) referred several questions to the ECJ for a preliminary ruling on the right of access under Article 15 GDPR (BGH, decision of 29.03.2022 – Ref. VI ZR 1352/20). In the case on which the decision was based, the plaintiff requested that the defendant hand over, free of charge, a complete copy of all the medical records relating to him that existed in the defendant's files. The reason for the demand for surrender was what the plaintiff considered to be incorrect treatment by the defendant. In particular, it was questionable whether the plaintiff's right of access under data protection law also exists if its sole purpose is to obtain information for the assertion of claims under medical liability law, but no other purposes under data protection law are pursued. Specifically, the ECJ should clarify, among other things, whether the right to receive a copy of the personal data stored about the data subject also exists if the data subject requests the documents for the pursuit of legitimate but non-privacy purposes. In a further decision in May 2022, the Federal Court of Justice (BGH) then decided that judicial disputes relating to the obligation to surrender copies can be suspended until the ECJ has ruled, without the issue having to be referred to the ECJ again (BGH, decision of 31.05.2022 – Ref. VI ZR 223/21). In another case in which the plaintiff asserted a claim for information under data protection law against his insurance company, although he was not pursuing any objectives under data protection law, but was rather aiming to recover tariff contributions, the Regional Court Erfurt also considered consultation of the ECJ to be necessary and announced a stay of the proceedings and an intended ECJ referral with reference to the BGH referral proceedings (LG Erfurt, decision of 07.07.2022 – Ref. 8 O 1280/21).

In January 2022, the Regional Court München I ruled that the transmission of the IP address to Google in the context of the use of Google Fonts cannot be justified by a legitimate interest within the meaning of Article 6 (1) (1) (f) GDPR, and that it may be appropriate in this respect to award a user immaterial damages if the dynamic reloading of fonts within the scope of the use of Google Fonts results in an outflow of user data to the USA (LG München I, judgment of 20.01.2022 – Ref. 3 O 17493/20). The court reasoned that the data transfer could be prevented without great effort by storing the fonts locally on the company's own servers, and that a different design – specifically the integration of Google Fonts through a server call-up from Google – was accordingly unnecessary and contrary to data protection. The decision of the Regional Court has led to a veritable "wave of warning letters" in the wake of the decision, in the course of which targeted searches for violations in the integration of Google Fonts were carried out and claims for damages were asserted against companies. Regardless of the existence of the alleged data privacy violation, the main question with regard to the corresponding claim letters was whether the assertion of a claim for damages through the targeted search for the data privacy violation and the targeted provocation of the damage was abusive.

Activities of the European Commission and the European Parliament

After the ECJ declared the EU-US Privacy Shield invalid in its Schrems II decision in 2020 (ECJ, judgment of 16.07.2020 – Ref. C-311/18) due to the level of data protection in the U.S., in particular the far-reaching access powers of the U.S. intelligence agencies, an agreement in principle on a new "transatlantic data protection framework" ("Trans-Atlantic Data Privacy Framework") was reached in Spring 2022 by the European Commission and the U.S. Based on this new framework, the aim is to enable secure transfers of data between the EU and participating U.S. companies and to ensure adequate protection of data transferred to the U.S., taking into account the requirements of the Schrems II ruling (Communication from the European Commission and the White House). In particular, the new regulations provide for stricter requirements for intelligence access to data of Europeans and procedures to ensure effective control of the new standards. In October 2022, U.S. President Joe Biden signed a decree that creates the legal basis on the U.S. side for the new legal framework for data transfers to the United States.

The European Parliament adopted the final recommendations of the Special Committee on Artificial Intelligence in the Digital Age (AIDA) in May 2022 (press release dated 03.05.2022). The final report, which also incorporated the results of numerous hearings and debates, included a "roadmap" and recommendations for action on how to deal with artificial intelligence (AI) by 2030. Among other things, the recommendations are intended to serve as a basis for further parliamentary work on the AI issue and, in particular, the AI Act. The European Data Protection Supervisor also published in October 2022 his opinion on the European Commission's Recommendation for a Council Decision authorizing the opening of negotiations on behalf of the European Union on a Council of Europe Convention on artificial intelligence, human rights, democracy and the rule of law. In April 2022, a committee was tasked with negotiating an appropriate legal instrument for AI by November 2023. In parallel, the European Commission's proposal for an AI Regulation from April 2022 is currently going through the legislative process.

Activities of supervisory authorities

In 2022, the data protection supervisory authorities of the EU member states once again addressed different data protection topics, with the individual authorities often taking an autonomous approach. In addition to the imposition of fines for data privacy violations, the focus was also on the publication of statements and notices on selected topics. Below we have listed various fines imposed in the past year along with statements and notices published, sorted thematically and by the amount of the respective fine.

Fines

The Irish Data Protection Commission (DPC) fined Meta subsidiary Instagram € 405 million in September 2022 and ordered various remedies (press release dated 15.09.2022). The reaon for the investigation and the imposition of the fine, in the view of the supervisory authority, was the insufficient protection of minors' data by Instagram. Instagram commented on the allegations to the effect that the offending processes have already been revised and further functions have been introduced to protect minors. In addition, Instagram announced that it would take action against the decision. The fine against Instagram is the second-highest fine ever imposed in the EU for a data breach.

A further fine of € 265 million and a number of remedial measures were also imposed on Meta Group by the Irish data protection supervisory authority in November 2022 (press release dated 28.11.2022). The supervisory authority criticized the fact that data from Facebook and Instagram users was accessible online on a large scale. The DPC's decision related to a feature that allows users to find friends by importing contacts stored in their smartphone into the Facebook or Instagram app. The background to the supervisory authority's action was an investigation that was

launched back in April 2021 after it became known that data records of almost 533 million users were publicly accessible. The investigation also involved coordination with the other EU data protection supervisory authorities, which agreed with the decision.

CNIL, the French data protection supervisory authority, has also once again imposed fines on the providers Facebook and Google for the unlawful design of cookie consents (press release dated 06.01.2022). Furthermore, the CNIL threatened to impose additional fines if the groups did not adapt their processes within three months. In both cases, the supervisory authority criticized the fact that optional cookies could be confirmed with one click, while several steps were required to reject those very cookies. Google is to pay € 150 million for the faulty implementation on the search portal google.fr and the video portal YouTube. A fine of € 60 million was imposed on Facebook.

In 2022, the German supervisory authorities also took action. For example, the Bremen State Commissioner for Data Protection and Freedom of Information imposed a fine of € 1.9 million on the housing association BREBAU GmbH because the company processed more than 9,500 data records on prospective tenants without having a legal basis for doing so (press release dated 03.03.2022). In more than half of the cases, the data processed was particularly sensitive data within the meaning of Article 9 GDPR, such as skin color, ethnic origin, religious affiliation, sexual orientation and state of health. The company's extensive cooperation with the supervisory authority led to a reduction in the fine.

The State Commissioner for Data Protection of Lower Saxony also imposed a fine of € 1.1 million on Volkswagen AG (press release dated 26.07.2022). The reason for this was data protection violations in connection with the use of a service provider during research trips for a driving assistance system to prevent traffic accidents. During a traffic check in 2019, it was noticed that the test vehicles had cameras that recorded traffic activity around the vehicle for error analysis, among other things. The supervisory authority criticized, among other things, the lack of signs informing data subjects in accordance with Article 13 GDPR, the lack of a data processing agreement with the service provider used to carry out the journeys, and the improper documentation in the list of processing activites. According to the regulator, the company has cooperated fully and accepted the fine.

In May 2022, the European Data Protection Board (EDPB) also adopted new guidelines on the assessment of fines, thus achieving progress with regard to the uniform sanctioning of data protection violations in Europe (press release dated 16.05.2022). The data protection supervisory authorities may impose fines to sanction data protection violations pursuant to Article 83 GDPR. In order to create more transparency in this respect, the Data Protection Conference (Datenschutzkonferenz, DSK) had already published its own concept for the assessment of fines in October 2019, which was to be applied until uniform requirements were established at the European level. A core element of the new guidelines is the establishment of a basic amount, which is determined on the basis of various components, such as the classification of the offense based on the standard violated, the severity of the offense, and the company's turnover. The guidelines provide for a five-stage calculation model.

Statements and notices

The State Commissioner for Data Protection and Freedom of Information in North Rhine-Westphalia (LDI NRW) published an opinion on the designation of reasons for absence in its 27th data protection report (report from Spring 2022). The background to the statement was a complaint filed by an employee. The LDI clarified that it was not necessary to know the specific reason for the absence in order to plan staffing. Rather, it is sufficient if the absence is identified as such.

In April 2022, the State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg (LfDI) published a statement in which he demanded that schools offer their students alternatives to the Microsoft 365 cloud service for school operations by the summer vacations of 2022 (press release dated 25.04.2022). As of the following school year, the use of Microsoft 365 in schools must be terminated or its data protection-compliant operation must be clearly demonstrated by the responsible schools. The reason for the LfDI's intervention was the high data protection risks, particularly in view of the processing of data on minors, which had already been pointed out by the Baden-Württemberg Ministry of Education and Cultural Affairs.

In November 2022, the German Data Protection Conference also came to the conclusion once again that it was still not possible for the controller to prove that it was operating Microsoft 365 in a data protection-compliant manner, even taking into account the data protection addendum of 15.09.2022 provided by Microsoft (determination dated 24.11.2022). As long as the necessary transparency about the processing of personal data from the commissioned processing for Microsoft's own purposes is lacking and its lawfulness is not proven, the proof cannot be provided. In this respect, the DSK report shows that, among other things, the question of in which cases Microsoft is acting as a processor and in which cases as a controller could not be conclusively clarified.

In July 2022, the data protection supervisory authorities of Bavaria, Berlin, Lower Saxony, Rhineland-Palatinate, Saxony and Saxony-Anhalt also announced a coordinated review of data processing agreements by web hosters (press release dated 19.07.2022). The reason for the review was an increase in inquiries from data controllers as to whether the agreements provided by the web hosters meet the requirements of the GDPR. To this end, the authorities developed a checklist to be used to review sample contracts of selected web hosters. The new checklist offers for the first time a standard for the review of data processing agreements that can also be applied in other areas.

In October 2022, the LDI NRW finally approved criteria for the certification of processors within the meaning of Article 42 (1) GDPR for the first time (press release dated 07.10.2022). In the future, companies will be able to use the "European Privacy Seal" (EuroPriSe) certificate to prove that they comply with the data protection regulations of the GDPR when processing orders. EuroPriSe Cert GmbH is the first private company in Europe whose criteria for the certification of companies have been approved by the supervisory authority and Deutsche Akkreditierungsstelle GmbH (DAkkS) and which has thus been accredited as a certification body.

The CNIL, together with several other European supervisory authorities, has also analyzed the conditions under which data is transferred to the USA when Google Analytics is used (press release dated 10.02.2022). In the absence of sufficient safeguards, the CNIL considered the data transfer in the context of the use of Google Analytics to be unlawful and even requested a website operator to discontinue the use of the service under the current conditions. Similar requests were also made by the supervisory authorities in Austria and Italy (notices dated 22.12.2021 and 09.06.2022).

Outlook 2023

Various data protection topics from the previous year, such as the data protection-compliant use of Microsoft 365 or the protection of

data transfers to the USA, will continue to play a role in 2023. In addition, new data protection topics can be expected.

After the U.S. President signed a decree in October 2022 creating the legal basis on the U.S. side for a new legal framework for data transfers to the U.S., the European Commission submitted a draft adequacy decision for the U.S. in December 2022 and initiated the procedure for its adoption. The draft will now go through the further adoption procedure and, in a next step, will be examined by the European Data Protection Supervisor, among others. Provided there are no major objections to the draft, it is likely to be adopted in the first quarter of 2023. Should this be the case, it remains to be seen whether a "Schrems III" judgment will subsequently be issued.

The e-privacy regulation, which is intended to strengthen the confidentiality of electronic communications, has not yet resulted in any significant changes. Whether entry into force in 2023 is realistic seems questionable at present. In contrast, progress was made last year with regard to the AI Regulation, the first draft of which was presented by the European Commission in April 2021; in November 2022, the Council of the European Union presented a slightly adjusted compromise proposal. Further negotiations between the EU legislative bodies are expected in 2023. Provided there is no further need for major changes, entry into force of the regulation in 2023 cannot be ruled out. Likewise, further negotiations on the Data Act, a draft of which was presented by the European Commission in February 2022, are pending for 2023. The Data Governance Act, which came into force in June 2022 and establishes processes, structures and a legal framework for the sharing of personal and non-personal data, is also directly applicable in EU member states from 24.09.2023.

It also remains to be seen whether the ECJ will follow the opinion of the Advocate General on the requirements for a claim for immaterial damages, which is also held by many German courts. In this respect, the Advocate General stated in his Opinion that for the recognition of a claim for damages suffered by a person due to a breach of the GDPR, the mere breach of the standard as such is not sufficient if it is not accompanied by material or immaterial damage. He further commented that the immaterial damages claim regulated in the GDPR does not extend to mere annoyance.

Of course, BRANDI's data protection team will keep you up to date on the data protection events and challenges that 2023 will bring in its data protection newsletter in the new year. In addition, our 4th BRANDI Data Protection Law Day will take place on 12.05.2023, to which we cordially invite you already now.

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