BRANDI
RECHTSANWÄLTE

REVIEW OF 2024 AND OUTLOOK FOR 2025

Information on data protection I January 2025

Introduction

Data protection law in 2024 was characterized by various decisions by authorities and courts on the interpretation and application of the provisions of the GDPR. Questions regarding the scope of possible claims for damages under Art. 82 GDPR and the scope of the right of access under Art. 15 GDPR have taken up a lot of space. In addition, the legal classification of various user tracking technologies and the permissibility of data processing for advertising purposes continued to be discussed intensively. The new AI Regulation, which is also relevant to the processing of personal data, came into force in July 2024. The new regulation takes a risk-based approach and specifies, among other things, the requirements that providers, operators, retailers, and users of AI systems must comply with.

On May 24, 2024, our BRANDI-Data Protection Law Day took place for the fifth time. Guests at BRANDI were Dr. Thilo Weichert, the former head of the data protection supervisory authority in Schleswig-Holstein (ULD), and Prof. Dr. Eckhard Koch, the Vice President for Research, Development and Transfer at the FHDW Paderborn. We exchanged views with Dr. Weichert and Prof. Dr. Koch on various issues relating to "Security begins with data protection". In discussions with lawyers from BRANDI, the guest speakers provided fascinating insights into various data protection issues, current proceedings by the supervisory authorities, and their day-to-day work.

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 an outlook for the new year and the developments to be expected in 2025.

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 each main topic, we also provide in-depth information on a selected data protection law topic and summarize the relevant aspects and special features from a data protection law perspective as well as practical tips. We have summarized the main topics of our data protection newsletter from 2024 for you again below:

> Data protection-compliant design of a cookie banner
>
> The record of processing activities – What is a procedure and how many procedures must be documented?
>
> Data erasure – online and offline
>
> Messenger services within the company
>
> The use of Microsoft 365 in the company
>
> BRANDI-Data Protection Law Day on the topic of "Security begins with data protection"
>
> Joint controllership within the group
>
> Use of chatbots based on AI systems
>
> Driving license check by the employer
>
> Data protection in the BEM procedure
>
> Data protection with company bike leasing

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 – sorted by topic – some particularly relevant court decisions from 2024.

After the ECJ had already specified the requirements for a claim for non-material damages under Art. 82 GDPR in two decisions from December 2023 (ECJ, decision dated 14.12.2023 – Ref. C-340/21 and ECJ, decision dated 14.12.2023 – Ref. C-456/22), in January 2024 the court dealt with the question of whether a theoretical risk of misuse of data already justifies a claim for damages (ECJ, decision dated 25.01.2024 – Ref. C-687/21). The court ruled that the claim for damages pursuant to Art. 82 GDPR only fulfills a compensatory function, but not a punitive function. It also stated that the person claiming damages must not only prove the infringement, but

also the damage incurred. Although the concept of non-material damage is to be understood broadly and the fear of data misuse can in principle constitute non-material damage, this must nevertheless be proven. A purely hypothetical risk of misuse by an unauthorized third party cannot lead to compensation. In April, the ECJ further differentiated the existing case law (ECJ, decision dated 11.04.2024 – Ref. C-741/21). Following on from its previous case law, it emphasized that although the "loss of control" falls under the concept of damage in principle, the violation of provisions that confer rights on the person concerned is not in itself sufficient to justify a claim for damages. With regard to the assessment of the claim, the court ruled that it is up to the Member States to establish criteria for determining the amount of compensation, while respecting the principles of effectiveness and equivalence under EU law. However, the amount of compensation should not be made dependent on the severity or frequency of the infringements. Furthermore, the ECJ found that it is not possible to exempt the responsible party from liability by making a blanket reference to the misconduct of subordinates, but must be strictly limited to cases in which the responsible party can prove that there is no causal link between its conduct and the damage. In two further decisions from June 2024, the ECJ then reiterated that Art. 82 GDPR requires a breach of the GDPR, damage and a causal link between the breach and the damage, that a mere breach does not necessarily give rise to a claim for damages, and that the damage must be proven by the data subject, whereby the respective court is free to award even minor damages (ECJ, decision dated 20.06.2024 – Ref. C-182/22 and C-189/22). The court also reiterated that the determination of the criteria for determining the extent of damages is a matter for the law of the individual member states, whereby the principles of equivalence and effectiveness must be observed. According to the ECJ, an additional infringement of national provisions is to be taken into account in the assessment just as little as the degree of seriousness and intentionality of the infringement. In a decision from October 2024, the question was again whether damage can already be assumed if personal data falls or could fall into the hands of third parties due to a data leak at the controller or whether further circumstances such as illegal disclosure or misuse are required (ECJ, decision dated 04.10.2024 – Ref. C-200/23). The ECJ confirmed the trend indicated in its previous rulings on this topic and once again explicitly formulated that the loss of control alone can be regarded as non-material and therefore compensable damage. Additional justification for any fears and concerns about misuse is not necessarily required. With reference to the aforementioned case law of the ECJ, the BGH finally affirmed claims for damages in connection with a data protection incident at the social network Facebook in November 2024 (BGH, decision dated 18.11.2024 – Ref. VI ZR 10/24). The decision of the BGH is significant for many similar lawsuits that are currently pending in Germany and in which the courts of lower instances may be guided by the BGH's leading decision.

In February 2024, the BGH once again ruled that Art. 15 (1) and (3) GDPR does not give rise to a fundamental right to disclosure of copies of the explanatory letters including attachments to premium adjustments in private health insurance (BGH, decision dated 06.02.2024 – Ref. VI ZR 15/23). He explained that although the concept of personal data is to be understood broadly, taking into account the case law of the ECJ, the letters sent by a controller to a data subject are only to be classified as personal data to the extent that they actually contain information about the data subject. In this respect, the term "copy" also does not refer to a document as such, but only to the personal data contained therein. A reproduction of documents or entire documents would subsequently only have to be made available if the contextualization was necessary to ensure comprehensibility. The Federal Court of Justice then commented again on the interpretation of the term "copy of personal data" in Art. 15 (3) GDPR in March 2024 (BGH, decision dated 15.03.2024 – Ref. VI ZR 330/21). It stated that personal data exists if any kind of information about a person is provided. This is to be assumed if the information has a link to a specific person due to the content, purpose, or effect of the information. In this respect, the Federal Court of Justice stated that a data subject's own statements or letters always have a link to their person and must therefore be made available as a copy, as they contain a personal reference in their entirety. In the case of letters from third parties, on the contrary, a case-by-case examination is required. If documents only contain isolated pieces of personal data, these should only be made available as a copy in their entirety if contextualization is necessary in order to understand the data processing and to be able to make use of the data subject's rights.

In its judgment of July 2024, the ECJ once again clarified the requirements for representative actions (ECJ, decision dated 11.07.2024 – Ref. C-757/22). The court ruled that Art. 80 (2) GDPR must be interpreted in such a way that an authorized body can bring an action by association if it claims that the rights of a data subject have been infringed "as a result of processing". In this respect, a significant breach could also result from a failure to comply with the obligation to provide information in accordance with Art. 12 and 13 GDPR. Since the processing of personal data in violation of the right to information violates the provisions of the GDPR, the violation of this right is to be regarded as a violation of the rights of the data subject "as a result of processing" within the meaning of Art. 80 (2) GDPR. As a result, the right to information, and thus indirectly also the duty to inform, is a right that, if violated, can be invoked by the representative action mechanism.

In October 2024, the ECJ dealt with two cases concerning data processing for advertising purposes. The content of the first decision concerned the question of how long online social services such as Facebook may store data collected for advertising purposes and whether the online services must take into account what type of data is involved (ECJ, decision dated 04.10.2024 – Ref. C-446/21). The ECJ stated that the principle of data minimization precludes unlimited and indiscriminate processing with regard to the type of data. Furthermore, the publication of a specific date does not entitle online social services such as Facebook to link thematically related data that was not published in the same way and then use these links for advertising purposes. In the second decision, the ECJ specified the conditions under which the transfer of personal data for marketing purposes can be based on the legal basis of legitimate interests within the meaning of Art. 6 (1) (1) (f) GDPR (ECJ, decision dated 04.10.2024 – Ref. C-621/22). The court stated that data processing on the basis of legitimate interests is lawful under three cumulative conditions: the controller or a third party must have a legitimate interest, the processing must be necessary to realize the legitimate interest, and the interests or fundamental rights and freedoms of the data subject must not be overridden. Furthermore, the required legitimate interest does not have to be regulated by law, but merely lawful.

Developments in legislation

The Digital Services Act (DSA), which came into force on November 16, 2023, has been fully applicable since February 17, 2024. The DSA creates various new obligations for providers of digital services that provide consumers with goods, services or content, including the obligation to set up a central contact point for authorities and users, explanatory obligations in the general terms and conditions and the obligation to publish annual transparency reports. In the event of a breach of the DSA, the competent authority – in Germany the Federal Network Agency – can impose fines of up to 6% of annual global turnover.

On May 14, 2024, the Telemedia Act (TMG) expired and was replaced by the Digital Services Act (DDG). As part of the introduction of the DDG, the name of the Telecommunications Telemedia Data Protection Act (TTDSG), which came into force at the end of 2021, was also changed to the Telecommunications Digital Services Data Protection Act (TDDDG).

The new regulation establishing harmonized rules for artificial intelligence (Artificial Intelligence Regulation, AI Regulation) was then published in the Official Journal of the EU on July 12, 2024 after the European Parliament approved the regulation in March. The AI Regulation came into force on August 1, 2024 and the implementation deadlines have begun. With some exceptions, the new regulations will apply from August 2, 2026. The new regulation provides for various obligations for AI systems, depending on the respective risks and impacts. Systems classified as high-risk include those used in the areas of critical infrastructure, general and vocational education or employment, and those used for private and public services in certain areas of law enforcement, migration and border management, justice and the democratic process.

Activities of the supervisory authorities

In 2024, 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.

Fines

In April 2024, the Czech supervisory authority imposed a fine of 13.9 million euros for violating Art. 6 and 13 (1) GDPR. The company in question had collected data from users of its antivirus software and transferred this data to its sister companies without a legal basis. The supervisory authority also found that the company had not sufficiently informed users about the data transfer in question. In the view of the supervisory authority, the breach was particularly serious because the person responsible was one of the leading experts in cyber security.

In June 2024, the Italian supervisory authority (GPDP) imposed a fine of 6.4 million euros and various other measures on Eni Plenitude S.p.A. Società Benefrit for unsolicited telephone calls. The company contacted numerous people to advertise its products. As part of its investigation, the GPDP found that various contacts were made without the data subjects having given their prior consent. The GPDP subsequently found violations of Art. 5 (Principles of data processing), 6 (Lawfulness of processing), 24 (Responsibility of the controller), 25 (Data protection by design and by default), and 28 (Data processing) GDPR.

Because the Swedish Avanza Bank AB used the Facebook pixel and transmitted data of up to one million customers to Meta due to incorrect settings, the Swedish supervisory authority (IMY) imposed a fine of 15 million SEK in June 2024 for violation of Art. 5 (1) (f), 32 (1) GDPR. IMY was of the opinion that the company had not taken sufficient security measures to prevent the data transfer or at least to detect it at an early stage.

After the Dutch Data Protection Authority (AP) had already imposed a fine of 10 million euros on Uber in December 2023 for violating information obligations and the principle of transparency, the company received a further fine of 290 million euros from the AP in August 2024 for transferring the data of European drivers – including sensitive data such as account, payment and location data, identification documents and criminal and medical data – to the USA without sufficient safeguards.

Due to the partially unencrypted storage of user passwords, the Irish Data Protection Commission (DPC) imposed a fine of 91 million euros on Meta Platforms Ireland Limited in September 2024. Following its investigation, the DPC found that Meta had violated the requirements of the GDPR in several respects: reporting and documentation obligations in connection with data protection violations (Art. 33 GDPR) as well as Art. 5 (1) (f) GDPR and Art. 32 (1) GDPR due to inadequate technical and organizational measures.

The DPC imposed a further fine of 310 million euros on LinkedIn Unlimited Company in October 2024. The content of the fine concerned the processing of LinkedIn users' personal data for the purposes of behavioral analysis and targeted advertising, as well as the legality, fairness, and transparency of the processes. Among other things, the DPC found that there was no legal basis for the data processing procedures in question. In addition, there was a breach of the information obligations under Art. 13 and 14 GDPR and the principle of fairness under Art. 5 (1) (a) GDPR.

Opinions and notes

In February 2024, Bonn-based EuroPriSe Cert GmbH was the first body in Germany to be authorized by the State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia (LDI NRW) to certify data processing procedures of processors. The "European Privacy Seal" certificate issued by EuroPriSe Cert GmbH is intended to certify to processors that their data processing procedures comply with the requirements of European data protection law.

In May 2024, the Saxon Data Protection and Transparency Commissioner (SDTB) examined around 30,000 Saxon websites with regard to data protection violations. In particular, the SDTB also looked at the use of the Google Analytics service. As part of its review, the data protection officer found that website operators did not comply with the applicable requirements to the necessary extent in 2,300 cases. The affected parties were requested to rectify the data protection violations and delete all unlawfully collected data.

In view of the increasing relevance of digitalization and artificial intelligence in the application process, the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) published a position paper on applicant data protection and recruiting in June 2024. He first emphasized that application documents contain a large amount of sensitive data, which is why handling them in compliance with data protection regulations is of the utmost importance, and then went on to discuss the different phases of the recruiting process and some specific issues.

In June 2024, the State Commissioner for Data Protection and Freedom of Information Rhineland-Palatinate (LfDI) launched an information campaign on data protection rules for newsletters and email advertising. The aim of the campaign was to raise awareness of the issue among those responsible and to reduce the number of breaches.

Outlook 2025

Various data protection topics from previous years, such as issues relating to the right of access under Art. 15 GDPR, the design of user tracking, and the legally compliant obtaining and management of user consent, will also play a role in 2025. New data protection issues can also be expected.

The ECJ has currently received two preliminary references on the question of when a request for information is abusive (Case C-416/23). One of the two cases concerns the potentially manipulative use of the right to request information to an excessive extent.

The other case concerns requests for information that could be abusive due to their quantity. The decision of the ECJ in this case remains to be seen.

At the beginning of September 2024, the Federal Government adopted the Ordinance on Consent Management Services under the Telecommunications Digital Services Data Protection Act (EinwV) in implementation of Section 26 TDDDG. Among other things, the new regulation stipulates that the consent management service must save the end user's settings when they use a digital service for the first time and specifies which consents can be managed using the service. It also regulates which requirements an administration service must meet in order to be user-friendly. The Bundestag and Bundesrat still have to approve the new regulation.

In addition, the Federal Ministry of Labor and Social Affairs (BMAS) and the Federal Ministry of the Interior and Homeland (BMI) presented their draft bill to strengthen the fair handling of employee data and provide more legal certainty for employers and employees in the digital world of work (Employee Data Act, BeschDG) at the beginning of October 2024. The aim of the law is to create a balance between the interests of companies and employees and to protect employees in the digital world of work. Among other things, the draft bill provides for comprehensive regulations on the necessity test and the granting of consent in the employment relationship. It remains to be seen to what extent the project will be taken up again in the next legislative period after the new elections and what changes will then be made.

BRANDI's data protection team will of course keep you up to date on the data protection events and challenges that the year 2025 will bring. In addition, we would like to invite you to our next Data Protection Law Day now, in keeping with our established tradition. The event will take place on May 16, 2024. You can already look forward to interesting presentations and exciting discussions. Prof. Ulrich Kelber, former Federal Commissioner for Data Protection and Freedom of Information (BfDI), will be discussing with us.

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