CMS Data Protection Update EU and Germany, August 2024

Europe · 16/08/2024

I. The latest from the data protection authorities and current topics

1. AI Act: Legislative proceedings finalised

The legislative proceedings for the AI Act have been completed and came into effect on 1 August 2024. The CMS homepage provides an overview: Looking ahead to the EU AI Act (cms.law). The data protection authorities have published the following notifications and are gearing up for their new duties:

- Statement 3/2024 of the European Data Protection Board (**EDPB**) on data protection authorities' role in the Artificial Intelligence (**AI**) Act framework adopted on 16 July 2024;
- Position paper of the Data Protection Conference (**DSK**) dated 3 May 2024;
- Press release from the Hamburg Commissioner for Data Protection and Freedom of Information (**HmbBfDI**) dated 12 July 2024;
- Q&A on the AI Act from the French data protection authority (**CNIL**) dated 12 July 2024;
- Press release from the State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia (**LDI NRW**) dated 25 July 2024;
- Press release from the State Commissioner for Data Protection and Freedom of Information of Rhineland-Palatinate dated 1 August 2024.

2. EU Data Protection Board: Annual Report 2023 & Strategy 2024-2027

In late April, the European Data Protection Board (**EDPB**) released its Annual Report 2023. The EDPB uses the report to draw attention to its guide for small and medium-sized enterprises (**SME**s) and to the EU-US Data Privacy Framework (**DPF**), among other goals. The EDPB is also looking to the future and on 18 April 2024 adopted its Strategy 2024-2027, which sets out the priorities (divided into four pillars) and the main measures to achieve these goals. The four pillars are (1) enhancing harmonisation and promoting compliance with data protection legislation; (2) reinforcing a common enforcement culture and effective cooperation; (3) safeguarding data protection in the developing digital and cross-regulatory landscape; and (4) contributing to the global dialogue on data protection. New guidelines are to be developed to these ends. As top issues, the EDPB identifies platform regulation through the Digital Markets Act (DMA) and the Digital Services Act (**DSA**) and the spread of AI.

3. EDPB: FAQ on the EU-US Data Privacy Framework (DPF)

Since mid-July, the EDPB has provided an FAQ on the DPF for Individuals and for businesses. These contain information on how the DPF works, how to submit complaints, how to join the DPF and how to transfer data to the US.

4. EDPB: Report from the ChatGPT Taskforce

In May, the EDPB released the first preliminary Report of the work undertaken by the ChatGPT Taskforce. Regarding data scraping and a possible legitimate interest in this, the taskforce emphasises a high risk to the rights of data subjects and points out the need for particularly stringent data protection measures. The report also comments on fairness, transparency obligations and data accuracy.

5. EDPB: Opinion on "consent-or-pay models"

This spring, the EDPB also published an opinion on "consent-or-pay models", in which the EDPB addresses the validity of consent to the processing of personal data for the purpose of behavioural advertising in the context of the "consent-or-pay models" used by large online platforms (Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms). The EDPB calls for users to be given real choice and for large online platforms to consider providing individuals with an equivalent payment-free alternative when they are developing alternative models. The State Commissioner for Data Protection of Lower Saxony (*LfD Niedersachsen*), among others, has welcomed the EDPB's opinion in a statement, as users should not be forced to "consent to in-depth tracking of their behaviour for personalised advertising or alternatively to pay for a subscription".

6. DSK: Guidance on AI and data protection

In May 2024, the German Data Protection Conference (**DSK**) published a guidance on the topic of AI and data protection. According to the Associated Press release dated 6 May 2024, the guidance for companies, public authorities and other organisations is intended as a manual for controllers under the GDPR when selecting, implementing and using AI applications. The DSK also made its first comments on generative AI models such as large language models (**LLMs**). The North Rhine-Westphalia Commissioner called the guidance "practical" in a statement dated 8 May 2024 (as did the Lower Saxony Commissioner).

Since July 2024, the State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg (*LfDI*) has provided the AI & Data Protection Guidance Navigator (ONKIDA), which provides an overview of the various materials.

You can also find out more about AI and data protection here: Using AI and responsibility for data privacy (cms-lawnow.com).

7. Hamburg: Theses on personal references in LLMs

In mid-July, the Hamburg Commissioner for Data Protection and Freedom of Information established three Theses on Personal References in LLMs. These theses are as follows:

- Simply storing an LLM without any personal data does not constitute processing within the meaning of Article 4 (2) of the GDPR. Processing operations in an AI system based on an LLM, and in particular their output, only need be adapted to the requirements of the GDPR if personal data are processed.
- Data subject rights such as the right of access, erasure or rectification can relate to the input and output of an AI system, but not to the model itself.

- If LLMs are trained with personal data, there is an obligation to design them in compliance with data protection regulations and to safeguard the rights of data subjects. The legality of using an LLM in an AI system remains unaffected by data protection violations during its training.

8. Hamburg: Position paper on applicant data protection in recruiting

On 6 June 2024, the Hamburg Commissioner published a position paper on the topic of applicant data protection and recruiting with reference to AI and digitalisation. The reason for the position paper is the decision of the Court of Justice of the European Union (CJEU) dated 30 March 2023 in the case C-34/21 and the subsequent discussion surrounding section 26 (1) German Federal Data Protection Act (*BDSG*). The Hamburg Commissioner points out that a large amount of sensitive data is generated in the application process and provides advice on subjects including the use of AI-based systems in the recruitment process.

9. Saxony: Review of 30,000 websites

The Data Protection and Transparency Commissioner of Saxony (**SDTB**) issued a press release dated 13 June 2024 stating that in May 2024 it examined around 30,000 websites based in Saxony for data protection violations with the help of an IT lab to check matters including how the web analytics service Google Analytics is used and whether the website owners have corresponding consent. The Saxony Commissioner reports that it identified over 2,000 breaches and has written to the companies concerned with requests to rectify the GDPR breaches and erase data collected unlawfully.

10. BayLfD: New guidelines

In May 2024, the Bavarian State Commissioner for Data Protection (**BayLfD**) published guidance on the Data Governance Act (DGA) titled "Data Governance Act: Moving towards a single European market for data". The guidance presents the three major topics of the Data Governance Act (**DGA**) – re-use of certain categories of protected data held by public sector bodies, data intermediation services and data altruism – as well as their legal framework and their relationship to the GDPR. In some places, the paper contains practical tips for the application of the law.

The Bavarian Commissioner has also published new guidance on the topic of "joint responsibility". In it, the Bavarian Commissioner provides tips and recommendations for action relating to Article 26 of the GDPR. In addition, the Commissioner presents CJEU case-law and explains joint responsibility using examples.

11. Brandenburg, Hesse, Lower Saxony, Saarland, Saxony and Schleswig-Holstein: Activity reports 2023

Some authorities used the spring of 2024 to finalise and release their activity reports for the previous year. In June 2024, the Lower Saxony Commissioner released the activity report for 2023. Both in the year of the reporting period and in the future, the Commissioner sees AI and digitalisation as some of the areas where new challenges for data protection and increased demand for advice will emerge. The Commissioner also reported an increase in the number of complaints and

data protection violations.

The State Commissioner for Data Protection and the State Commissioner for Access to Information of Schleswig-Holstein also released the activity report for 2023 in April. The Commissioner identifies the following as particularly relevant topics in the report: processing of data concerning health, data protection in research, data transfers to third countries, credit scoring, chat monitoring and employee data protection. In late April, the Saxony Commissioner also published its activity report for 2023 in which the Commissioner records an increase of over 10% in the number of reported data breaches and a peak in the number of data breaches reported to the authority. The Commissioner provided a summary of this in a press release dated 24 April 2024. The Saarland State Commissioner for Data Protection and Freedom of Information also reported a record number of reported data breaches to the Independent Data Protection Centre of Saarland in its activity report for 2023.

In addition, in May 2024, the Brandenburg State Commissioner for Data Protection and the Right of Access to Files published its activity report for 2023. In April, the Hessian Commissioner for Data Protection and Freedom of Information (**HBDI**) also released its activity report for 2023 and identified AI and credit scoring, among other things, as particularly relevant data protection issues.

12. NRW: Activity report 2023 and changed view on the application of telecommunications secrecy for private email use

The North Rhine-Westphalia Commissioner presented its activity report for 2023 that caused a stir with one issue in particular concerning data protection law. According to the activity report (page 76 f.), the Commissioner does not consider employers who allow or tolerate their employees to use the internet and email privately at work to be bound by secrecy of telecommunications and therefore are not potential addressees of section 206 German Criminal Code (**StGB**). This decision is contrary to the previous assessment of the data protection authorities. A further consequence of this assessment by the Commissioner would be that the employer would no longer have to rely on the employee's consent to access the data, but that only the GDPR applies. The Commissioner, however, recommends including explicit provisions in the employment contract.

The topics of AI and cyber security were also relevant to the Commissioner in 2023 since estimates state that 58% of German companies were the target of a cyber-attack in the previous year.

13. Digital Services Act comes into force in Germany

After the German Digital Services Act (**DDG**) was promulgated in the Federal Law Gazette within the framework of a consolidated law after being signed by the Federal President, it came into force on 14 May 2024. This triggered a need for action by website operators since the German Telemedia Act (**TMG**) expired at the same time. In addition, many other laws required amending as a result of the consolidated law. The German Telecommunications-Telemedia Data Protection Act (**TTDSG**) has now become the German Telecommunications Digital Services Data Protection Act (**TDDDG**). Among other things, the term "telemedia" has been replaced by "digital services". In addition, as of 14 May 2024, there are official regulations on fines and supervision for the implementation of the DSA in Germany. Stay up to date on the DSA with our DSA News Hub (cmshs-bloggt.de).

14. France: Recommendations for the development of AI systems

On 7 June 2024, the French supervisory authority (**CNIL**) published recommendations on the development of AI systems. In doing so, the CNIL aims to help harmonise innovation and the responsible use of AI, particularly in the context of data protection law. The recommendations were developed together with public and private interest groups and are intended to assist, among other things, with the legal categorisation and definition of a legal basis and with tests, checks and impact assessments. The recommendations are part of the authority's AI action plan and are to be supplemented on an ongoing basis.

II. New GDPR fines

1. Czech Republic: EUR 13.9m fine for unlawful disclosure of data

In April this year, the Czech data protection authority imposed a EUR 13.9 million fine on a company that had disclosed the personal data of around 100 million users of a software application to a US company. The data were transferred including the users' pseudonymised internet browsing history in connection with a unique ID, which was falsely identified as anonymised. The data subjects were informed of the transfer of anonymised data. In reality, the data was not anonymised since it was possible to identify some of the data subjects.

2. Italy: EUR 100,000 fine for non-compliance with the general principles of data processing

In April 2024, the Italian data protection authority imposed a EUR 100,000 fine. During an investigation, it found that data subjects had received advertising calls on behalf of the controller without their consent or despite being registered in an objection register. The data protection authority concluded that the controller had failed to take appropriate technical and organisational measures (**TOM**s) to ensure that the processing of personal data is carried out in accordance with data protection regulations throughout the supply chain. For the same reason, the authority fined another Italian company the same amount.

3. Spain: EUR 360,000 fine for insufficient technical and organisational measures (TOMs)

At the beginning of May 2024, the Spanish data protection authority imposed a EUR 360,000 fine on a financial services provider. The controller suffered a data breach that led to unlawful access to customer profiles. During its investigation, the data protection authority found that the controller had failed to take appropriate TOMs to protect personal data and to prevent such an incident. The original GDPR fine of EUR 600,000 was reduced to EUR 360,000 due to voluntary payment and acknowledgement of responsibility.

4. Spain: EUR 96,000 fine for insufficient cooperation with the data protection authority

In May 2024, the Spanish data protection authority imposed a GDPR fine on a company because the

information requested by the data protection authority was not provided. The original fine of EUR 160,000 was reduced to EUR 96,000 due to voluntary payment and acknowledgement of responsibility.

5. Enforcement Tracker Report 2023/2024

The latest edition of the CMS GDPR Enforcement Tracker Report 2023/2024 has been published.

Here you will find a summary of all publicly known fines imposed by the German and other European data protection authorities under the GDPR, which totalled EUR 4.48 billion in the period under review.

III. Recent case-law

1. CJEU: Representative action for infringement of GDPR rights

In Case C-757/22 pending before the CJEU, on which the Opinion of the Advocate-General has been available since 25 January 2024, the CJEU delivered its judgment on 11 July 2024. In the same case, the CJEU ruled in the spring of 2022 (C-319/20) that an action brought by consumer protection associations is also admissible if there is no specific mandate from a consumer. The German Federal Court of Justice (**BGH**), however, referred another question to the CJEU with its ruling of 10 November 2022 (I ZR 186/17), concerning the condition "as a result of the processing" under Article 80 (2) of the GDPR. The German Federal Court of Justice wanted to know whether an infringement of law is asserted "as a result of the processing" if a consumer protection association bases an action on the fact that the rights of a data subject have been infringed through non-fulfilment of the obligations under Article 12 (1) sentence 1 and Article 13 (1) c) and e) of the GDPR. Like the CJEU Advocate-General in his Opinion, the CJEU came to the conclusion that consumer protection associations may bring actions against infringements of these information obligations.

2. CJEU: Ruling relating to the referral by Wesel Local Court regarding Article 82 of the GDPR

The CJEU has continued its case-law on Article 82 of the GDPR with two further decisions. In a judgment of 20 June 2024, the CJEU ruled on Questions referred by Wesel Local Court (C-590/22). In the facts underlying this case, the tax consultancy firm (defendant) inadvertently sent tax documents to an old address of the client (claimant), even though the client had previously informed the defendant of its new address. The data subjects are demanding compensation pursuant to Article 82 of the GDPR in the amount of EUR 15,000.

On some of the questions referred, the CJEU was able to refer to its rulings from the recent past and reconfirmed that a GDPR infringement alone is not sufficient to justify a claim for compensation under Article 82 of the GDPR. Rather, the data subject must prove the existence of damage caused by the infringement, which does not have to be of a certain severity level or exceed a threshold of seriousness. Article 83 of the GDPR, which applies to fines, cannot be used to interpret Article 82 of the GDPR either. The CJEU also reiterated its view that Article 82 of the GDPR does not have a deterrent function.

In the ruling, the Court also stated that it is sufficient for the claim for compensation pursuant to

Article 82 (1) of the GDPR to prove the data subject's fear that personal data have been disclosed to third parties as a result of a GDPR infringement and the negative consequences of this. It is not necessary to prove that personal data were actually disclosed. Furthermore, the CJEU clarified that, when assessing the amount of a claim for compensation pursuant to Article 82 GDPR, infringements of national provisions that relate to the protection of personal data, but are not intended to clarify the GDPR, should not be taken into account.

3. CJEU: Ruling in the Scalable Capital proceedings regarding Article 82 of the GDPR

In Joined Cases C-182/22 and C-189/22, which are based on questions referred from Germany regarding the Scalable Capital cases, the CJEU also issued a judgment on 20 June 2024. The referrals related in particular to the questions of whether identity theft within the meaning of recitals 75 and 85 of the GDPR should only be affirmed for the assertion of non-material damage under Article 82 of the GDPR if the identity of the data subject has been assumed, or whether the fact that criminals have data that make the data subject identifiable is sufficient to affirm identity theft. The Opinion of the Advocate-General has been available in the proceedings since October 2023 (and reported in our blog).

According to the CJEU, identity theft can only be affirmed if a third party has actually assumed the identity of the data subject, whereby compensation for non-material damage caused by the theft of personal data pursuant to Article 82 GDPR cannot be limited to cases in which it is proven that the theft of data subsequently led to identity theft or identity fraud. When determining the amount of compensation owed for non-material damage pursuant to Article 82 (1) of the GDPR, the CJEU also states that damage caused by an infringement of the protection of personal data is, by its nature, no less serious than physical injury. However, if low compensation is sufficient to fully make up for the damage suffered, which lacks seriousness, it is a matter for the national courts to award such compensation. Regarding the other questions referred, the CJEU was also able to refer to its previous judgments regarding Article 82 of the GDPR.

Munich Regional Court I ruled in a similar case on 19 April 2024 (see below).

4. Advocate-General: Competitors' standing to bring an action for GDPR infringements

In Case C-21/23 pending before the CJEU, the Opinion of the Advocate-General responsible has been available since 25 April 2024. One of the key issues in these proceedings is whether infringements of data protection law by competitors of the controller under the GDPR can be asserted via the provisions of the German Unfair Competition Act (**UWG**) instead of by data subjects as parties authorised to bring an action. In each case, a competitor of a pharmacist with a mail-order licence had brought an action, claiming that the pharmacist was in breach of the GDPR. According to the Advocate-General, the provisions of Chapter VIII of the GDPR do not preclude any national provisions that grant companies the right to argue that competitors have breached the GDPR on the basis of a prohibition of acts of unfair competition.

The proceedings also concern the question of whether data concerning health within the meaning of Article 9 (1) of the GDPR are transmitted when ordering non-prescription pharmacy-only medicines via an online platform. The Advocate-General’s Opinion rejects this, stating only hypothetical or inaccurate conclusions could be drawn about the health of the person placing the order. It remains to be seen whether the CJEU will agree with the Advocate-General's view. The referral to the CJEU

comes from the German Federal Court of Justice (**BGH**) (which we reported on: Prosecution of data protection breaches by competitors (cmshs-bloggt.de)).

5. German Federal Court of Justice: It is not mandatory to state the name of the data protection officer

In its judgment of 14 May 2024 (VI ZR 370/22), the German Federal Court of Justice ruled that it is not mandatory to state the name of the data protection officer when providing their contact details as long as it is possible to reach them. It is sufficient to provide the information required to reach the competent body.

6. Latest developments on social media scraping

According to our analyses, most German courts that have dealt with social media 'scraping' cases have tended to reject the claims for compensation asserted by the claimants pursuant to Article 82 of the GDPR for a lack of proven compensable damage, either because this could not be individually proven in the statements of claim merely by means of identical template letters and with clause components for parallel use in several proceedings or by hearing the data subject in court (e.g. Saarbrücken Higher Regional Court, judgment of 3 May 2024 – 5 U 72/23; Munich Higher Regional Court, judgment of 24 April 2024 – 34 U 2306/23 e). In contrast, Oldenburg Higher Regional Court affirmed the data subjects' claim against the operator of the social network for some cases in the amount of EUR 250 since in these cases an individual compensable damage had been proven (see Oldenburg Higher Regional Court, judgments of 30 April 2024 – 13 U 108/23; 13 U 89/23; 13 U 109/23). In judgments dated 16 April 2024, which rejected a claim by the data subject in comparable cases, Oldenburg Higher Regional Court still emphasised that being affected by the scraping incident was not in itself sufficient for a claim for compensation (13 U 59/23; 13 U 79/23; 13 U 60/23).

The German Federal Court of Justice will decide on the social media scraping cases in the near future. Firstly, the hearing in the proceedings VI ZR 22/24 is scheduled for 8 October 2024. The previous rulings were those issued by the lower courts, Stuttgart Higher Regional Court (judgment of 13 December 2023 – 4 U 51/23) and Cologne Higher Regional Court (judgment of 7 December 2023 – 15 U 108/23). Stuttgart Higher Regional Court had found that future damages attributable to the scraping were to be compensated while Cologne Higher Regional Court rejected the claim for compensation in a comparable case.

CMS's continuously updated table of case-law on the claim under Article 82 of the GDPR provides the latest developments: GDPR compensation: Overview of current rulings and developments (continuously updated) (cmshs-bloggt.de)

7. Munich Regional Court I: Departure from case-law in Scalable Capital cases

In its judgment of 19 April 2024 (31 O 2122/23), Munich Regional Court I departed from its previous case-law in the Scalable Capital cases. These cases were based on the following facts: a website operator offering services including securities and brokerage services suffered a leak of personal data. This data leak occurred, among other causes, after admin passwords had not been changed following the termination of contractual relationships with an IT service provider. This service provider subsequently became the target of a hacker attack, which resulted in the personal data of

over 30,000 customers being made available on the darknet.

While more than two years ago, in its judgment of 9 December 2021 (31 O 16606/20), Munich Regional Court I affirmed a claim for compensation of EUR 2,500 by a data subject pursuant to Article 82 GDPR (reported in our blog), it now rejected the claim in the above-mentioned judgment from April 2024 due to a lack of evidence of damage attributed to the data incident. The Regional Court stated that formulaic general statements, which are presented in several court proceedings with the same wording, were not sufficient. For example, the Court was aware that people who were not customers of the defendant also received unsolicited contact attempts, text messages or fraudulent calls, which meant that no damage could be regarded proven as a result. According to Munich Regional Court I, there were no indications of a loss of control suffered regarding data over which the claimant had control until the incident, while unpleasant feelings and mere inconvenience were not a liability-related impairment. The fact that the claimant was still a customer of the defendant also precluded the assertion of non-material damage. In the new judgment from 2024, Munich Regional Court I does not explicitly address this departure from its own case-law from 2021.

8. Magdeburg Administrative Court: Confirmation of the ban on the processing of telephone numbers for advertising purposes for cold calls

The Saxony State Commissioner had issued an order prohibiting a portal operator from processing the telephone numbers of natural persons for advertising purposes and from calling them unless prior consent had been obtained or the operator could cite a material interest on the part of the persons on the basis of specific circumstances. The operator had contacted providers of holiday accommodation who had no relation to the platform with the aim of having them publish advertisements on the portal. The Magdeburg Administrative Court (**VG**) confirmed the order of the State Commissioner in June 2024. The State Commissioner and the Administrative Court saw neither explicit nor presumed consent, and in particular there was no interest in publishing advertisements on the platform in question.

IV. CMS events, pertinent blog posts and more

- CMS Client Academy | Introduction to Data Protection | E-learning.
- CMS GDPR Enforcement Tracker Report 2023/2024.
- Article 82 GDPR: Liability claims under the right of access under data protection law (cms-lawnow.com).
- Scope and implementation of the right of access under data protection law (cms-lawnow.com).
- Data protection pitfalls of internal investigations (cmshs-bloggt.de).
- German Podcast: CMS To Go - Virtual worlds, Metaverse, AI: Legal issues.
- Latest developments in our CMS AI blog series: When the AI Act applies (cmshs-bloggt.de); More is more (?): The AI governance structure according to the AI Act (cmshs-bloggt.de) and Enforcement of the AI Act at European level: EU AI Office (cmshs-bloggt.de).
- Our overview of case law on GDPR compensation has been updated: GDPR compensation: Overview of current rulings and developments (continuously updated) (cmshs-bloggt.de).

For more information on any of these briefs or regulations in the EU and Germany concerning data protection, digital marketing and AI, contact your CMS client partner or these CMS experts: Philippe Heinzke, Reemt Matthiesen, Julia Dreyer

KEY CONTACTS

Philippe Heinzke, LL.M.

Partner

Rechtsanwalt

Duesseldorf

T +49 211 4934 304

Dr. Reemt Matthiesen

Partner

Rechtsanwalt

Munich

T +49 89 23807 248

Dr. Julia Dreyer

Senior Associate

Rechtsanwältin

Hamburg

T +49 40 37630 309