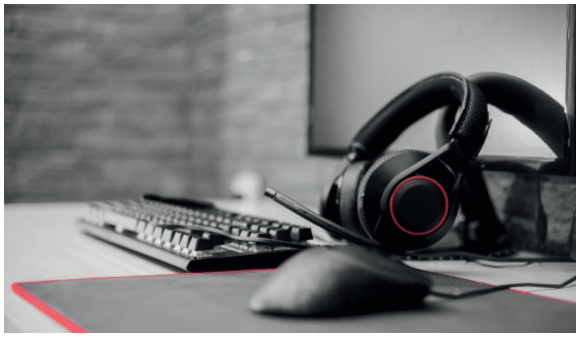
ADVANT Beiten

Privacy Ticker

June 2024



+++ COUNCIL OF EUROPE ADOPTS AI CONVENTION +++ ECJ ON DAMAGES FOR IDENTITY THEFT +++ FEDERAL COURT OF JUSTICE RESTRICTS SCOPE OF THE RIGHT TO A COPY +++ FINE OF EURO 400,000 AGAINST GREEK MINISTRY OF THE INTERIOR FOR DISCLOSURE OF VOTERS LIST +++ EUROPEAN DATA PROTECTION SUPERVISOR PUBLISHES GUIDELINES ON AI +++ GERMAN DATA PROTECTION CONFERENCE: DATA PROTECTION WHEN CLOSING HOSPITALS +++

1. Changes in Legislation

+++ COUNCIL OF EUROPE ADOPTS AI CONVENTION +++

The Council of Europe has adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. This Convention is intended to ensure the responsible use of AI that respects the rule of law and democracy. The AI Convention sets out transparency and monitoring requirements for both the public and private sectors. Thus, states must ensure that AI systems respect the prohibition of discrimination and the right to privacy. However, research and development activities and the use of AI to protect national security interests are excluded from the scope of the AI Convention. The Council of Europe's AI Convention should not be confused with the European Union's AI Act, which was also adopted in May (see AB Privacy Ticker May 2024). The Council of Europe is independent of the European Union and is particularly committed to the protection of human rights. Countries around the world can now accede to the AI Convention.

To the information brochure of the Council of Europe

To the wording of the AI Convention (dated 9 May 2024)

2. Case Law

+++ ECJ ON DAMAGES FOR IDENTITY THEFT +++

The European Court of Justice (ECJ) has dealt with the scope and extent of claims for compensation for non-material damage in the event of data theft. In the case presented, two users of the Scalable Capital trading platform sued for non-material damages. Due to a hacker attack, the name, date of birth, address, e-mail address and a digital copy of the identity card of the data subjects were stolen. The ECJ first clarified that the claim for damages only has a compensatory function and not a punitive function. The severity and intentional nature of a breach of the GDPR, on the other hand, are not relevant to the existence of the claim. In terms of severity, the court considers a breach of the protection of personal data to be comparable to bodily harm. A national court is nevertheless free to award minor compensation in the event of minor damage, provided that this is suitable to fully compensate for the damage incurred. Above all, the ECJ states that identity theft only exists if a third party has actually assumed the identity of a data subject. Only the theft and possession of data that makes a person identifiable is not sufficient for identity theft or identity fraud.

To the ECJ ruling (dated 20 June 2024, C-182/22 and C-189/22)

+++ FEDERAL COURT OF JUSTICE RESTRICTS SCOPE OF THE RIGHT TO A COPY +++

The Federal Court of Justice has restricted the scope of the right to a copy in accordance with Art. 15 (3) GDPR. In the legal dispute, an investment client requested copies of all personal data held by her financial advisor. The financial advisor provided details of the information, but did not provide copies. The plaintiff filed an action for disclosure of copies of all personal data, in particular in the form of telephone notes, file notes, minutes, e-mails, letters and signing documents. The court ruled that the claim for copies of the e-mails and letters sent to the defendant was justified. These are all personal data of the data subject, so that copies must be provided. However, this does not automatically apply to letters from the defendant to the plaintiff as well as telephone notes, file notes and minutes of conversations. There was no entitlement to disclosure of these documents in their entirety.

To the ruling of the Federal Court of Justice (dated 5 March 2024, VI ZR 330/21, in German)

+++ LOCAL COURT OF GELNHAUSEN: INADMISSIBLE VIDEO SURVEILLANCE WITH SWIVELLING CAMERA +++

The Local Court of Gelnhausen has ruled that surveillance cameras are already inadmissible if there is a theoretical possibility of recording the neighbour, thus creating surveillance pressure. The plaintiff took legal action against the installation of a swivel camera on his neighbor's property. The Local Court confirms a violation of the plaintiff's personal rights. In the court's opinion, it does not matter whether the camera actually captures the plaintiff's property. Rather, the existence of surveillance pressure is sufficient for a claim for injunctive relief. This is already the case if the fear of surveillance by existing cameras appears reasonable based on specific circumstances. In the present case, the court affirmed this as there was a tense neighbourly relationship and the camera could be directed electronically towards the neighbouring property. Whether the camera was actually aimed at the plaintiff's property is irrelevant.

To the ruling of the Local Court of Gelnhausen (dated 4 March 2024, 52 C 76/24, in German)

3. Regulatory Investigations and Enforcement Actions

+++ FINE OF EURO 400,000 AGAINST GREEK MINISTRY OF THE INTERIOR FOR DISCLOSURE OF VOTERS LIST +++

The Greek data protection authority has imposed fines of EUR 400,000 on the Greek Ministry of the Interior and EUR 40,000 on a Member of the European Parliament. Following several complaints, the authority found that the Ministry of the Interior had sent a list with personal data of all registered Greek voters abroad to a Greek Member of the European Parliament. In addition to the known data from the voters' register, both the telephone number and the e-mail address of the persons were listed. The data was used by the Member of Parliament to send a politically motivated e-mail to each of the named voters. With regard to the Ministry, the authority assumed a breach of confidentiality and a violation of the protection of personal data. Deficiencies were identified in the data protection policy, the clarification of the facts and the presentation of the processing activities. With regard to the Member of Parliament, it was found that the use of electronic contact data violated the principles of legality, objectivity and transparency. There was neither a legal basis nor were information obligations fulfilled.

To the press release of the authority (dated 27 May 2024)

To the administrative fine notice of the authority (dated 27 May 2024, in Greek)

4. Opinions

+++ EUROPEAN DATA PROTECTION SUPERVISOR PUBLISHES GUIDELINES ON AI +++

The European Data Protection Supervisor (EDPS) has published guidelines on the use of generative AI. As the European data protection authority, the EDPS is responsible for the institutions, bodies and agencies of the European Union. The guidelines are therefore primarily addressed to EU institutions and are intended to serve as a guidance for the use of generative AI systems. The guidelines first clarify the question of what AI is and how it is defined. It is then discussed how AI can be used in EU institutions, how personal data is used in AI systems, what role data protection authorities play in the development and implementation of AI systems and how personal data is lawfully processed in the design, development and validation of an AI system. The guidelines also highlight the importance of data minimisation and data accuracy in AI systems and address the question of how data subjects are informed about the processing of their personal data in an AI system.

To the EDPS press release (dated 3 June 2024)

To the EDPS's guidelines (dated 3 June 2024)

+++ BERLIN GROUP PUBLISHES WORKING PAPER ON FACIAL RECOGNITION TECHNOLOGY +++

The International Working Group on Data Protection in Technology, the so-called "Berlin Group", chaired by the Federal Commissioner for Data Protection and Freedom of Information, has adopted a working paper on facial recognition technology. The working paper deals with the potential uses of facial recognition in the private and public sectors and the associated risks. It also presents practical recommendations for data protection-compliant use. Facial recognition is a biometric technology that analyses people's facial features and compares them with corresponding databases for identification purposes. Facial recognition is used, for instance, to control access to buildings and IT devices, for surveillance in public places and for border controls. The Berlin Group points out that their use in public spaces in particular entails high risks for the freedoms and rights of the data subjects. Facial recognition technologies that can recognize emotions or derive character traits from certain biometric

characteristics are rejected outright due to their inaccuracy and the high discrimination potential.

To the press release of the Federal Commissioner for Data Protection (dated 5 June 2024)

To the working paper of the Berlin Group (dated 5 June 2024)

+++ DATA PROTECTION AUTHORITY PUBLISHES CHECKLIST ON TIKTOK RULES FOR PUBLIC BODIES +++

The State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg has published a checklist for the use of TikTok by public bodies. Authorities, political parties and politicians are increasingly using TikTok as an information and advertising platform, but also to communicate with citizens. As this also results in considerable data protection risks, the authority has drawn up an overview with questions and requirements to determine whether the use of TikTok is possible in the respective context in compliance with data protection law. The most important issues include the question of responsibility, finding a suitable legal basis, fulfilling information obligations and configuring the TikTok account to be as data protection-compliant as possible. Controllers are instructed to develop a concept for use and to provide sufficient technical and organisational protective measures. In addition, citizens are to be provided with an alternative means of contact and interaction.

To the checklist of the authority (dated 28 May 2024, in German)

+++ GERMAN DATA PROTECTION CONFERENCE: DATA PROTECTION WHEN CLOSING HOSPITALS +++

The Conference of Independent Federal and State Data Protection Supervisory Authorities has published a resolution on data protection during the closure of hospitals. In this resolution, the authorities call on relevant stakeholders - in particular hospital management, owners and interest groups - as well as the responsible players in politics and administration and the federal and state legislators to take measures to overcome the challenges posed by data protection law. The sharp increase in hospital closures and insolvencies brings about a number of data protection issues. In the event of insolvency, the secure storage of patient data and the protection of data subjects' rights are often not guaranteed. The authorities thus propose mandatory retention concepts for data controllers. Hospital management and interest groups are called upon to jointly develop data protection-compliant solution concepts. In addition, the federal states are to develop financing solutions for the

transitional periods. Finally, politicians are called upon to address the issue and develop possible solutions.

To the authorities' resolution (dated 15 May 2024, in German)

+++ NEW RULES OF CONDUCT FOR CREDIT AGENCIES APPROVED +++

The Hessian Commissioner for Data Protection and Freedom of Information has approved the new rules of conduct of the association "Die Wirtschaftsauskunfteien e.V.". The association represents the interests of the largest German credit agencies. The rules of conduct had to be revised because they were objected to by the Hessian authority and contradicted several resolutions of the German Data Protection Conference and the European Data Protection Board. In particular, they had to be adapted to the ECJ ruling on Schufa scoring (see AB Privacy Ticker December 2023). The rules of conduct regulate the review and storage periods for lawfully stored personal data by German credit agencies. Storage regulations for positive data and account misuse data are no longer included. The storage of contract data is limited to contractual relationships in accordance with the German Banking Act. The rules of conduct specify the regulated storage by providing definitions in a glossary and by referring to legal provisions.

To the authorities' press release (dated 3 June 2024, in German)

To the rules of conduct (dated 25 May 2024, in German)

UPCOMING EVENT

Webinar: EU AI Act: What you (really) need to know

Join us live on **July 11, 2024 at 4 p.m.** for comprehensive insights into the latest developments and implications of the AI Act. Find out what this regulation means for you, what types of AI systems are regulated and what the consequences of non-compliance are. Take the opportunity to ask your questions in the Q&A afterwards. Further information can be found in the invitation.

invitation

Your Contacts

If you have any questions, please address the ADVANT Beiten lawyer of your choice or contact the ADVANT Beiten Privacy Team directly:

Office Frankfurt
Mainzer Landstrasse 36 | 60325 Frankfurt am Main

Dr Andreas Lober

+49 69 756095-582
vCard

Susanne Klein, LL.M.

+49 69 756095-582
vCard

Lennart Kriebel

+49 69 756095-582
vCard

Fabian Eckstein, LL.M.

+49 69 756095-582
vCard

Jason Komninos, LL.M.

+49 69 756095-582
vCard

Office Dusseldorf
Cecilienallee 7 | 40474 Dusseldorf

Mathias Zimmer-Goertz

+49 211 518989-144
vCard

Christian Frederik Döpke, LL.M.
+49 211 518989-144
vCard

Office Munich
Ganghoferstrasse 33 | 80339 Munich

Katharina Mayerbacher

+89 35065-1363
vCard

Dr Birgit Münchbach

+89 35065-1312
vCard

Update Preferences | Forward

Please note

This publication cannot replace consultation with a trained legal professional. If you no longer wish to receive information, you can unsubscribe at any time.

Imprint

This publication is issued by Beiten Burkhardt Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33, 80339 Munich, Germany
Registered under HR B 155350 at the Regional Court Munich / VAT Reg. No.: DE811218811
For more information see:
www.advant-beiten.com/en/imprint

Beiten Burkhardt Rechtsanwaltsgesellschaft mbH is a member of ADVANT, an association of independent law firms. Each Member Firm is a separate and legally distinct entity, and is liable only for its own acts or omissions.