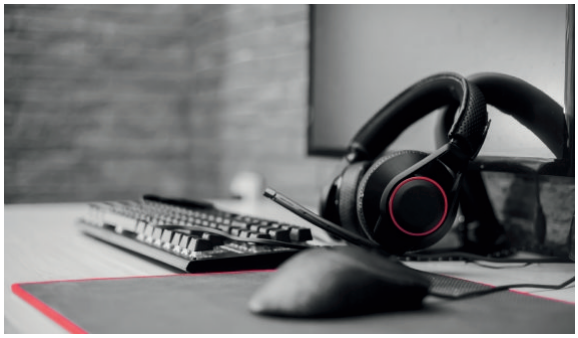
ADVANT Beiten

Privacy Ticker

March 2024



+++ EU PARLIAMENT ADOPTS AI ACT AND CYBER RESILIENCE ACT +++ ECJ: EUROPOL AND MEMBER STATE JOINTLY LIABLE FOR DATA PROTECTION BREACH +++ HIGHER ADMINISTRATIVE COURT OF LOWER SAXONY: BIRTH DATE AS COMPULSORY FIELD IN WEBSHOP UNLAWFUL +++ FINE OF USD 16.5 MILLION DUE TO SALE OF BROWSER DATA +++ EUROPE-WIDE INVESTIGATION INTO THE RIGHT TO INFORMATION +++

1. Changes in Legislation

+++ AI ACT ADOPTED BY EU PARLIAMENT +++

The European Parliament has passed the Artificial Intelligence Act (AI Act). According to its own statement, this will be the world's first binding law on AI. The Act aims to ensure that only AI systems that are both safe and respect the fundamental rights and values of the EU are brought onto the European market and are used in the EU. The AI Act follows a risk-based approach, according to which certain AI systems are prohibited, e.g. emotion recognition systems in the workplace and the evaluation of social behaviour. High-risk AI systems are only permitted if certain obligations are complied with. AI systems that are used in the areas of critical infrastructure, migration, border controls, education or employment are considered high-risk. In addition, information and transparency obligations apply to all systems. As soon as the Council has adopted the AI Act, it will apply directly throughout the EU and - with a few exceptions - will be fully applicable 24 months after its entry into force.

To the Text of the AI Act (dated 13 March 2024)

To the press release of the EU Parliament (dated 13 March 2024)

+++ EU PARLIAMENT ADOPTS CYBER RESILIENCE ACT +++

The EU Parliament has also adopted the text for the regulation on horizontal cybersecurity requirements for products with digital elements, also known as the Cyber Resilience Act (CRA). The CRA is intended to supplement the NIS2 Directive, which primarily deals with the security of information and communication technology in critical infrastructure (see AB blog post dated 8 February 2024, in German). Software or hardware products and associated cloud solutions are covered by the CRA. The main addressees are manufacturers, importers and distributors. The principle of "security by design" obliges them to continuously ensure the cyber security of products and remain responsible for this throughout the entire life cycle of the product. This requires a continuous risk assessment, including information obligations to be fulfilled and product documentation. The CRA provides for fines of up to EUR 15 million or 5 per cent of the total annual global turnover in the event of violations. The CRA has yet to be adopted by the Council and will then enter into force after 36 months.

To the Text of the CRA (dated 12 March 2024)

To the press release of the EU Parliament (dated 12 March 2024)

2. Case Law

+++ ECJ: EUROPOL AND MEMBER STATE JOINTLY LIABLE FOR DATA PROTECTION BREACH +++

The European Court of Justice (ECJ) has ruled that Europol and a Member State are jointly and severally liable if damage has occurred as a result of unlawful data processing within the framework of cooperation between Europol and that Member State. The Slovakian criminal authorities were investigating the plaintiff in a murder case and asked Europol to extract data from his mobile phones. After Europol had sent the requested data to the authorities, the Slovakian press published information from the plaintiff's intimate communications. The plaintiff brought an action against Europol for a data protection violation and claimed non-material damages. The ECJ ruled that the disclosure of the intimate data to the press constituted a data breach for which Europol and Slovakia were jointly liable. According to the ECJ, the data subject only has to prove that unlawful data processing occurred during the cooperation between the authorities. The data subject is not required to prove which of the two authorities is responsible for the unlawful processing. The plaintiff was awarded damages in the amount of EUR 2,000.

To the ECJ ruling (dated 5 March 2024, C 755/21 P)

To the press release of the ECJ (dated 5 March 2024)

+++ HIGHER ADMINISTRATIVE COURT OF LOWER SAXONY: BIRTH DATE AS COMPULSORY FIELD IN WEBSHOP UNLAWFUL +++

The Higher Administrative Court of Lower Saxony has ruled that a pharmacy may not ask customers for their date of birth as mandatory information in its online shop. The pharmacy in question was initially requested by the State Commissioner for Data Protection of Lower Saxony to refrain from requesting the date of birth of customers, regardless of the type of medication ordered. The pharmacy brought an action against this order before the Hanover Administrative Court, which dismissed the action. The Higher Administrative Court of Lower Saxony confirmed this view. The processing of the date of birth is not usually required under data protection law for the fulfilment of a contract. In particular, the date was not required to identify the customer. Even to verify whether minors are ordering from the online shop, the operator can ask whether they are of legal age and does not need the exact date of birth. There is also no legal obligation to request the date of birth because the pharmacy only offers online ordering for non-prescription products on its website. Nor could it rely on legitimate interests, since instead of requesting the date of birth, the milder, equally efficient means of requesting the age of majority was available. Also, the date of birth is not necessary for the possible collection of outstanding debts.

To the decision of the Higher Administrative Court of Lower Saxony (dated 23 January 2024, 14 LA 1/24, in German)

To the press release of the LfD Lower Saxony (dated 20 March 2024, in German)

+++ ADMINISTRATIVE COURT OF BERLIN: RIGHT TO INFORMATION ALSO JUSTIFIED IN CASE OF HIGH RESEARCH EFFORT +++

The Administrative Court of Berlin has ruled that a right to information under Art. 15 GDPR is not disproportionate even if fulfilment involves considerable effort for the controller. The plaintiff demanded that a public authority provide him with information about the personal data processed about him and send him copies of all processes containing this data. The authority then provided the plaintiff with information about the data stored in the IT systems, the categories and the recipients of this data.

Copies of the documents were not provided. The plaintiff then filed an action for surrender of the copies. In its defence, the defendant invoked, among other things, a disproportionate effort, as it would have to examine more than 5,000 pages of files to fulfil the claim. The court ruled in favour of the plaintiff and fully approved the claim for copies. The plaintiff had a legitimate interest in the handover of the files to identify potential recipients himself. The considerable amount of work for the defendant associated with the claim also did not lead to disproportionality or an abuse of rights.

To the judgment of the Administrative Court of Berlin (dated 6 February 2024, 1 K 187/21, in German)

3. Regulatory Investigations and Enforcement Actions

+++ FINE OF EUR 2.8 MILLION AGAINST UNICREDIT AFTER CYBER ATTACK +++

The Italian Data Protection Authority Garante per la Protezione dei Dati Personali (GPDP) has imposed a fine of EUR 2.8 million on the Italian bank UniCredit S.p.A. The bank reported a security incident to the authority back in 2018, which led to extensive investigations by the GPDP. Due to a cyberattack on UniCredit's banking portal, the first and last names, login numbers and identification codes of around 778,000 customers were exposed. In almost 7,000 cases, the perpetrators had also captured the PINs for accessing the portal. The GDPD identified several data protection breaches during its investigation. In particular, the bank had not taken any technical and organisational security measures that would have been suitable to effectively ward off cyber attacks. Also, no precautions had been taken to prevent customers from using weak PINs. In connection with the investigation, a further fine of EUR 800,000 was also imposed on NTT Data Italia, a processor working for UniCredit. The processor had delayed informing the bank about the data breach and had also outsourced certain services to other subcontractors without authorisation.

To the administrative fine notice of the GPDP (dated 8 February 2024, in Italian)

To the GDPD press release (dated 7 March 2024, in Italian)

+++ FINE OF USD 16.5 MILLION FOR SALE OF BROWSER DATA+++

The US Federal Trade Commission (FTC) has imposed a fine of USD 16.5 million, or approximately EUR 15.1 million, on Avast Limited and itssubsidiaries Avast Software and Jumpshot. The software sold by Avast is designed to protect the privacy of customers by preventing online tracking by third parties. However, the browser extensions and anti-virus software, such as AVG Online Security, themselves secretly collected customer data, e.g. search terms, cookie data and URLs of the websites visited. Avast sold this data to over 100 companies, including Google and Microsoft. The FTC considered this to be a breach of data protection and fraudulent behaviour on the part of Avast, as the data was passed on in clear form and without consent and the special confidence of customers in the protection of their privacy was exploited. An aggravating factor was that the data could be used to draw conclusions about sensitive information such as religious and political views as well as customer health data. Avast was obliged to delete the data already collected and to obtain the customer's consent before passing on the data.

To the decision of the FTC (dated 19 January 2024)

+++ EUROPEAN COMMISSION VIOLATES DATA PROTECTION WHEN USING MICROSOFT 365 +++

The European Data Protection Supervisor (EDPS) has found that the European Commission is using Microsoft 365 in violation of data protection law and is therefore in breach of the GDPR. According to the view of the EDPS, the Commission has in particular failed to provide sufficient safeguards for the processing of personal data outside the EU/EEA. Furthermore, the Commission did not sufficiently specify in its contract with Microsoft which types of personal data are collected for which explicit and specified purposes when using Microsoft 365. The EDPS has therefore imposed comprehensive remedies on the Commission, which are listed in the annex to his press release and must be completed by 9 December 2024. Also as of this date, the Commission is obliged to suspend all data flows to Microsoft and its sub-processors in third countries for which no adequacy decision exists.

To the press release of the EDPS (dated 11 March 2024)

4. Opinions

+++ EUROPE-WIDE INVESTIGATION INTO THE RIGHT TO INFORMATION +++

At the suggestion of the Federal Commissioner for Data Protection and Freedom of Information, the European Data Protection Board (EDPB) has selected the implementation of the right of access as the subject of its third coordinated review action, which has now been launched. In Germany, the data protection authorities of Bavaria (BayLDA), Brandenburg, Mecklenburg-Western Pomerania, Lower Saxony, Rhineland-Palatinate, Saarland and Schleswig-Holstein as well as the Federal Data Protection Commissioner are taking part. The campaign is aimed at assessing how private and public organizations implement the right of access in practice and to what extent further measures or clarifications by the data protection authorities are useful. In a first step, questionnaires will be sent to companies and organizations. On this basis, further official investigations will be initiated in a second step if necessary. The results of the campaign will be jointly analyzed and further measures decided on. The EDPB will publish the results of this analysis once the measures have been completed.

To the press release of the Data Protection Conference (dated 28 February 2024, in German)

To the EDPB press release (dated 28 February 2024)

+++ EDPB PUBLISHES OPINION ON THE NOTION OF MAIN ESTABLISHMENT +++

The European Data Protection Board (EDPB) has adopted an opinion on the notion of main establishment and the criteria for the application of the one-stop-shop mechanism following a request from the French data protection authority. Identifying the main establishment is important to determine the lead supervisory authority in cross-border cases. The EDPB considers that the place of central administration can only be considered as the main establishment if decisions on the purposes and means of the processing of personal data are taken there and if it is authorized to implement such decisions. In the opinion of the EDPB, there is no main establishment if the decision on the purposes and means is taken outside the European Union. In this case, the one-stop-shop mechanism should not be applicable.

To the opinion of the EDPB (dated 13 February 2024)

To the EDPB press release (dated 14 February 2024)

EDITOR IN CHARGE
Dr Andreas Lober | Rechtsanwalt
©Beiten Burkhardt
Rechtsanwaltsgesellschaft mbH

BB-Datenschutz-Ticker@advant-beiten.com
www.advant-beiten.com

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 Freiburg

Heinrich-von-Stephan-Straße 25 | 79100 Freiburg

Dr Birgit Münchbach

+49 761 150984-22
vCard

Office Munich

Ganghoferstrasse 33 | 80339 Munich

Katharina Mayerbacher

+89 35065-1363
vCard

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.