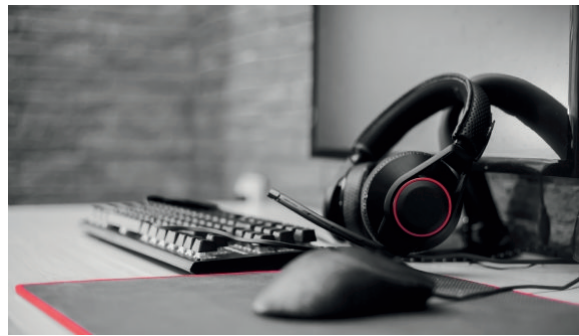


Privacy Ticker

December 2023



**+++ EU: AGREEMENT ON THE FINAL VERSION OF THE AI ACT +++
ECJ: NON-MATERIAL DAMAGES ALREADY IN CASE OF FEAR OF
DATA MISUSE +++ ECJ: SCHUFA SCORING GENERALLY
PROHIBITED +++ HIGHER REGIONAL COURT OF COLOGNE: DATA
TRANSFER TO GOOGLE INADMISSIBLE DESPITE EU-US DATA
PRIVACY FRAMEWORK +++ FINE OF EUR 1.7 MILLION AGAINST
NORWEGIAN LABOUR AND WELFARE ADMINISTRATION +++**

1. Changes in Legislation

+++ EU: AGREEMENT ON THE FINAL VERSION OF THE AI ACT +++

In the EU's trilogue procedure, the Commission, Council of Ministers and Parliament have agreed on a final version of the planned AI Regulation (AI Act). This is intended to be the cornerstone for the regulation of artificial intelligence in the EU and create the legal framework for the development, deployment and use of AI systems in the EU. Depending on the risk class of the AI system, the AI Act sets different levels of requirements for authorisation, documentation obligations and compliance with technical standards. Until recently, the automatic classification of people with biometric recognition into certain particularly sensitive categories, systems for recognising emotions and the subsequent analysis of video recordings for criminal prosecution were particularly controversial.

[To the report on heise.de \(dated 9 December 2023, in German\)](#)

**+++ GERMAN PARLIAMENT ADOPTS ELECTRONIC PATIENT FILE+
++**

The German parliament has passed the laws introduced by Federal Health

Minister Lauterbach to accelerate the digitalisation of the healthcare system and improve the use of healthcare data. The core element is the mandatory introduction of the electronic patient file ("ePA") as from 2025. A patient's entire medical history is to be stored in the file and can be accessed by doctors and patients. If insured persons do not want this, they must actively object to the use of the ePA (opt-out). They will also have the option of blocking access to certain data in the ePA. The data stored in the ePA may be used in pseudonymised form for research purposes. In addition to the ePA, the e-prescription is also to be further developed and established as a binding standard. Furthermore, telemedicine is to be expanded and digital health applications extended.

[To the report on tageschau.de \(dated 14 December 2023, in German\)](#)

2. Case Law

+++ ECJ: NON-MATERIAL DAMAGES ALREADY IN CASE OF FEAR OF DATA MISUSE +++

The ECJ has ruled that the mere fear of a possible misuse of personal data can in itself constitute non-material damages within the meaning of the GDPR. The case concerned a woman whose personal data had been published on the internet by the perpetrators of a hacker attack on a Bulgarian tax authority. According to the ECJ, in cases of a data breach, the mere concern that the data could be misused by third parties is sufficient. However, it is up to the national court to examine whether this fear can be considered justified in the specific case. The ECJ also clarified that unauthorised access to the data does not automatically mean that the controller's IT security measures were inadequate. However, the controller bears the burden of proof in this respect. If this proof is successful, liability may be waived under certain circumstances.

[To the press release of the ECJ \(dated 14 December 2023\)](#)

[To the ECJ ruling \(dated 14 December 2023, C-340/21\)](#)

+++ ECJ CONFIRMS ADMISSIBILITY OF FINES AGAINST LEGAL PERSONS +++

The ECJ has ruled that the fining of a legal person for a data breach does not require that the breach was committed by a management body or that this body had knowledge of it. The ECJ thus confirms the sanctioning practice of the German data protection authorities. In addition, the ECJ confirms that an infringement can only be deemed to have occurred if it was committed culpably, i.e. intentionally or negligently. The case concerns the fine of around EUR 14.5 million imposed on Deutsche

Wohnen SE in 2019 (see [AB Privacy-Ticker January 2022](#)). The ECJ clarifies that a company as a legal entity is directly liable for data protection violations, even if the specific person acting cannot be identified and the managers have no knowledge of the violation. Insofar as German law sets stricter requirements here, this is not compatible with the GDPR. A culpable breach occurs if the controller could not have been unaware of the unlawfulness of their behaviour, regardless of whether they were aware of a breach of the GDPR.

[To the press release of the ECJ \(dated 5 December 2023\)](#)

[To the ECJ ruling \(dated 5 December 2023, C-807/21\)](#)

+++ ECJ: SCHUFA SCORING GENERALLY PROHIBITED +++

The ECJ has ruled that SCHUFA scoring generally constitutes profiling that is prohibited under Art. 22 (1) GDPR and is only permissible under certain conditions. The case was based on complaints brought before the Wiesbaden Administrative Court by data subjects who were defending themselves against the decision of the Hessian data protection authority to take action against SCHUFA scoring. Scoring is a mathematical-statistical procedure that makes it possible to predict the probability of future behaviour, such as the repayment of a loan. In practice, it is often mainly the SCHUFA score that determines whether a consumer is granted a loan, for example. The ECJ ruled that scoring is to be regarded as an automated decision making, which is generally prohibited by the GDPR, if SCHUFA's customers, such as banks, attribute a decisive role to it in the context of granting a loan. The Wiesbaden Administrative Court must now decide whether Section 31 of the German Federal Data Protection Act constitutes a valid exception to this prohibition and whether scoring was therefore permissible in this case.

[To the press release of the ECJ \(dated 7 December 2023\)](#)

[To the ECJ ruling \(dated 7 December 2023, C-634/21\)](#)

+++ ECJ: SCHUFA MAY STORE INFORMATION RELATING TO THE GRANTING OF A DISCHARGE FROM REMAINING DEBTS FOR A MAXIMUM OF 6 MONTHS +++

On the same day and in connection with the above-mentioned ruling on scoring, the ECJ also decided that information relating to the granting of a discharge from remaining debts may be stored by SCHUFA for a maximum of 6 months. The case concerned the complaints of two individuals who were granted a discharge from remaining debts following insolvency

proceedings. According to the German Insolvency Code, these entries are deleted after 6 months. SCHUFA, on the other hand, stores this information for 3 years. The plaintiffs objected to this and demanded deletion, which SCHUFA rejected and the Hessian data protection authority confirmed as lawful. The ECJ ruled in favour of the plaintiffs and decided that it is contrary to the GDPR for private credit agencies to store data relating to the granting of a discharge from remaining debts for longer than the public insolvency register. After the six-month period has expired, the storage of the data at SCHUFA is therefore unlawful and data subjects are entitled to have the data deleted.

[To the press release of the ECJ \(dated 7 December 2023\)](#)

[To the ECJ ruling \(dated 7 December 2023, C-26/22 and C-64/22\)](#)

+++ REGIONAL LABOUR COURT OF DÜSSELDORF: NO COMPENSATION FOR DELAYED DATA ACCESS +++

The Regional Labour Court of Düsseldorf has rejected a claim for non-material damages for delayed access to information under Art. 15 GDPR. In March 2023, the previous instance had awarded the plaintiff non-material damages of EUR 10,000 because his former employer had only responded to a request for information with a delay. The Court of Appeal has now ruled in favour of the employer and dismissed the claim in its entirety. According to the court, it was true that the employer had breached the GDPR by not providing the information within the deadline and initially providing incomplete information. However, in the court's opinion, a breach of Art. 15 GDPR does not fall within the scope of Art. 82 GDPR. This presupposes data processing in breach of the GDPR, which, in the court's view, does not exist in the case of a mere breach of the obligation to provide information. Furthermore, the plaintiff had not sufficiently demonstrated any damage. The mere allegation of a loss of control over data associated with the breach was not sufficient.

[To the press release of the Regional Labour Court \(dated 28 November 2023, 3 Sa 285/23, in German\)](#)

+++ HIGHER REGIONAL COURT OF COLOGNE: DATA TRANSFER TO GOOGLE INADMISSIBLE DESPITE EU-US DATA PRIVACY FRAMEWORK +++

The Higher Regional Court of Cologne has ruled that the transfer of personal data from a website to Google in the USA was unlawful despite the EU Commission's new adequacy decision, the "Data Privacy Framework" (see [AB Privacy-Ticker July 2023](#)). The court thus ruled in

favour of the action brought by the consumer organisation North Rhine-Westphalia against Telekom Deutschland GmbH. In addition to other points, the consumer organisation criticised the fact that when the Telekom website was accessed, the IP address and information about the browser and end device used by the consumer were transmitted to Google servers in the USA. The court deemed this data transfer to be unlawful despite the existing adequacy decision, as there was no effective consent in this case. In the opinion of the court, the users were not sufficiently informed about the data processing and the transfer of their data to Google in the cookie banner and the privacy policy.

[To the press release of the consumer organisation \(dated 12 December 2023, in German\)](#)

[To the ruling of the Higher Regional Court \(dated 3 November 2023, 6 U 58/23, in German\)](#)

+++ FEDERAL FISCAL COURT: TAX OFFICE MAY ANALYSE ACCOUNT STATEMENTS OF A LAWYER +++

The Federal Fiscal Court has ruled that the German tax office may analyse a lawyer's account statements as part of a tax audit. The German Fiscal Code authorises the analysis of personal data. The plaintiff, who works as a lawyer, defended himself against the tax office's request to hand over his business account statements for an external audit and the handover of the account statements to the tax office by his bank. The court emphasised that the Fiscal Code constitutes an authorisation under data protection law for all measures of the tax proceedings. The law justifies the processing of data to fulfil a legal obligation and, in the opinion of the court, does not have to list which documents the tax office may request. Furthermore, it was not recognisable to the court that the provisions of the Fiscal Code violate the right to informational self-determination under the German Constitution or the protection of personal data under the EU Charter of Fundamental Rights.

[To the ruling of the Federal Fiscal Court \(dated 5 September 2023, IX R 32/21, in German\)](#)

3. Regulatory Investigations and Enforcement Actions

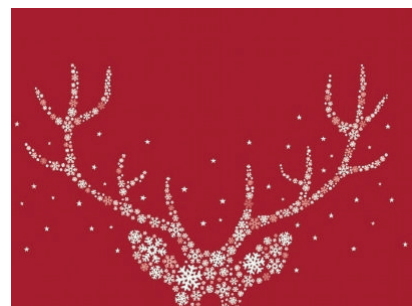
+++ FINE OF EUR 1.7 MILLION AGAINST NORWEGIAN LABOUR AND WELFARE ADMINISTRATION +++

The Norwegian data protection authority Datatilsynet has imposed a fine of around EUR 1.7 million on the Norwegian Labour and Welfare Administration (NAV). NAV processes a large amount of personal and sensitive data on the Norwegian population, including data relating to pensions, child benefit and social assistance. The data protection authority found gross violations in the handling of the data. In particular, NAV did not adequately protect the confidentiality of its IT systems. Too many employees had unauthorised access to the data. Access to the data was also not logged. Furthermore, the particularly sensitive data was not adequately protected by technical and organisational measures. In addition to the fine, NAV was instructed to set up a comprehensive and suitable system along with technical and organisational measures to ensure and demonstrate compliance with data protection regulations. The Norwegian supervisory authority had already warned NAV in the past.

[To the Datatilsynet press release \(dated 28 November 2023, in Norwegian\)](#)

[To the fine notice from Datatilsynet \(dated 27 November 2023, in Norwegian\)](#)

The entire **ADVANT Beiten** data protection team wishes you happy holidays and a good start into 2024!



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. This data protection ticker was created in cooperation with the ADVANT partner law firms Nctm and Altana.

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 Berlin

Luetzowplatz 10 | 10785 Berlin

Dr Ariane Loof

+49 30 26471-282

[vCard](#)

