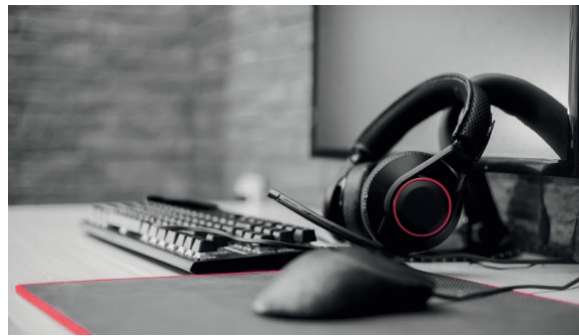


# Privacy Ticker

August 2024



**+++ DATA TRANSFERS TO THE USA: NEW AGREEMENT BETWEEN SWITZERLAND AND THE USA ADOPTED +++ FEDERAL COURT OF JUSTICE: EXPLICIT NAMING OF DATA PROTECTION OFFICER NOT MANDATORY +++ ADMINISTRATIVE COURT OF STUTTGART: CITY ORDERED TO PAY EUR 2,500 COMPENSATION FOR UNAUTHORIZED PUBLICATION OF HEALTH DATA +++ FINE OF EUR 290 MILLION AGAINST UBER BECAUSE OF DATA TRANSFER TO THE US +++ GUIDELINES FOR LOCAL AUTHORITIES AND ADMINISTRATIONS ON THE RIGHT TO INFORMATION UNDER ARTICLE 15 GDPR +++**

## 1. Changes in Legislation

**+++ DATA TRANSFERS TO THE USA: NEW AGREEMENT BETWEEN SWITZERLAND AND THE USA ADOPTED +++**

The Swiss Federal Council has approved a new framework agreement (Swiss-U.S. Data Privacy Framework) that facilitates the transfer of personal data between Switzerland and the USA. Previously, the EU standard contractual clauses adapted to Switzerland and a transfer impact assessment were required for data transfers to the USA. In future, the new agreement will allow the transfer of personal data from Switzerland to certified companies in the USA without additional guarantees. The certification for US companies ensures that the level of protection provided by Swiss data protection law is complied with. The

changes will apply as of 15 September 2024. The EU-U.S. Data Privacy Framework has already been in force between the EU and the USA since July 2023 ([see AB Privacy Ticker July 2023](#)). With the Swiss-U.S. Data Privacy Framework, the Federal Council is now creating comparable framework conditions for private individuals and companies in Switzerland.

[To the press report of the Swiss Federal Council \(dated 14 August 2024\)](#)

[To the adequacy decision \(dated 30 April 2024, in German\)](#)

## 2. Case Law

### **+++ FEDERAL COURT OF JUSTICE: EXPLICIT NAMING OF DATA PROTECTION OFFICER NOT MANDATORY +++**

The Federal Court of Justice has ruled that the GDPR does not require a data protection officer to be named. The customer of a bank requested information from the bank about the personal data it had stored in accordance with Art. 15 GDPR. In the customer's opinion, the information provided by the bank was incomplete, so she demanded further information in court and also requested the name of the data protection officer. Contrary to the court of first instance, which still considered the naming of the data protection officer to be mandatory, the Federal Court of Justice denied such an obligation under Art. 13 GDPR. According to the wording of the provision and the structure of the law, there is no obligation to name the data protection officer but only to provide contact details. In the opinion of the court, the meaning and purpose of the provision does not necessarily require the name to be mentioned either. This is because it does not depend on the person but on their function. It is sufficient for the data subject to provide the information required for accessibility. Moreover, the asserted claim does not arise from Art. 15 (1) GDPR. In view of the unambiguous legal situation, the Federal Court of Justice does not consider a referral to the Court of Justice of the European Union to be necessary.

[To the ruling of the Federal Court of Justice \(dated 14 May 2024, VI ZR 370/22, in German\)](#)

### **+++ ADMINISTRATIVE COURT OF STUTTGART: CITY ORDERED TO PAY EUR 2,500 COMPENSATION FOR UNAUTHORIZED PUBLICATION OF HEALTH DATA +++**

The Administrative Court of Stuttgart ordered a city to pay EUR 2,500 in compensation for a data protection violation because it had published the health data of a civil servant in a job advertisement without authorization. The plaintiff was the head of the main office at the defendant city and suffered a stroke, meaning that he was unable to continue working there. The responsible authority decided to reassign the position and sent out an internal job vacancy. In this job advertisement, the authority justified the awarding of the position with a transfer into retirement due to established incapacity to work (Dienstunfähigkeit). The plaintiff saw this as an unauthorized publication of his health data and claimed compensation in the amount of EUR 20,000. The court affirmed a violation of data protection but only awarded the plaintiff compensation of EUR 2,500. According to the court, the disclosure of the incapacity to work constituted processing of health data, which was not necessary for the job description. With regard to the amount of compensation, the authority benefited from the fact that the job advertisement was only sent internally, and the recipients were bound to confidentiality as public officials.

[To the judgement of the Administrative Court of Stuttgart \(dated 20 June 2024, 14 K 870/22, in German\)](#)

### **+++ ADMINISTRATIVE COURT OF ANSBACH: DATA SUBJECT HAS RIGHT TO DEMAND INTERVENTION FROM DATA PROTECTION AUTHORITY +++**

According to a ruling by the Administrative Court of Ansbach, data subjects may in certain cases demand that the competent data protection authority take measures against third parties if they violate the GDPR. After attending a seminar, the subsequent plaintiff demanded information from the organizer in accordance with Art. 15 GDPR. As the company did not provide complete information, the plaintiff turned to the Bavarian data protection authority (BayLDA). However, even after being requested to do so by the BayLDA, the plaintiff did not receive any proper information. Since the authority considered the proceedings to be completed, the plaintiff called on the BayLDA to take legal action. The Administrative

Court followed the plaintiff's opinion and justified this with a so-called reduction of discretion to zero. Hence, the plaintiff could demand that the BayLDA take action. If a data protection authority discovers a breach of the provisions of the GDPR at the end of its investigation, it is obliged to respond in an appropriate manner, according to the court. However, the authority has discretionary powers when choosing the means (e.g. fines or warnings).

[To the judgment of the Administrative Court of Ansbach \(dated 12 June 2024, AN 14 K 20.00941, in German\)](#)

## 3. Regulatory Investigations and Enforcement Actions

### **+++ FINE OF EUR 290 MILLION AGAINST UBER BECAUSE OF DATA TRANSFER TO THE US +++**

The Dutch data protection authority Autoriteit Persoonsgegevens has imposed a fine of EUR 290 million against UBER B.V. and UBER TECHNOLOGIES INC. The French data protection authority Commission Nationale de l'Informatique et des Libertés (CNIL) had received a collective complaint from an association representing more than 170 drivers on the Uber platform. As part of the investigation, it was discovered that UBER processes a large amount of personal data, some of it sensitive, from drivers and stores it on servers in the USA. The data included cab licenses, GPS data, photos, payment information, ID documents and, in some cases, information on criminal offences and driver health data. The data was transferred to the USA over a period of two years without a sufficient legal basis and appropriate safeguards. There was no adequacy decision for the USA at the time. UBER had also not concluded any standard contractual clauses to safeguard the data transfers. The Dutch Data Protection Authority was responsible for the investigation in this case, as UBER has its European headquarters in the Netherlands. However, it was supported by the CNIL during the proceedings.

[To the press release of the Dutch Data Protection Authority \(dated 26 August 2024\)](#)

[To the CNIL press release \(dated 26 August 2024, in French\)](#)

### **+++ USD 60 MILLION FINE AGAINST T-MOBILE DUE TO UNAUTHORIZED DATA ACCESS +++**

The Committee on Foreign Investment in the United States (CFIUS) has imposed a fine of USD 60 million, equivalent to around EUR 55 million, on the US mobile communications subsidiary T-Mobile US, Inc. CFIUS is an inter-agency body of the US government that is also responsible for reviewing foreign investments in the USA for the purpose of protecting national security. The reason to the fine was unauthorized data access in the course of T-Mobile's merger with Sprint Corporation. According to CFIUS, T-Mobile violated the National Security Agreement (NSA) during the merger. The NSA is an agreement between companies and the US government to address national security concerns in corporate acquisitions. Specifically, T-Mobile had failed to take appropriate measures to prevent unauthorized access to sensitive data. Even after learning of this security breach, T-Mobile failed to notify CFIUS. Due to the violations, CFIUS deemed the national security interests of the United States to have been violated.

[To the website of CFIUS](#)

[To the article on reuters.com \(dated 15 August 2024\)](#)

## **4. Opinions**

### **+++ GUIDELINES FOR LOCAL AUTHORITIES AND ADMINISTRATIONS ON THE RIGHT TO INFORMATION UNDER ARTICLE 15 GDPR +++**

In February 2024, the European Data Protection Board (EDPB) launched its Europe-wide "Coordinated Enforcement Framework (CEF)" campaign, in which several German data protection supervisory authorities are also participating. The aim is to assess how organizations implement the right of access in practice ([see AB Privacy Ticker March 2024](#)). On this occasion, the Saxon Data Protection and Transparency Commissioner has now published guidelines for local authorities and administrations on providing information in accordance with Article 15 GDPR. The guidelines

are intended to provide recommendations and instructions for Saxon public bodies to comply with requests for information. It also takes into consideration the latest case law of the European Court of Justice. The document provides a good overview of the most important regulations for dealing with requests for access and the correct organization within the responsible bodies. If information is not properly provided, data subjects can take legal action against public authorities and bring an action for the issue of an administrative act (Verpflichtungsklage).

[To the guidelines of the data protection authority \(dated 18 July 2024, in German\)](#)

### **+++ EU COMMISSION: SECOND REPORT ON THE EVALUATION OF THE GENERAL DATA PROTECTION REGULATION +++**

The European Commission has published its second report on the application of the GDPR. As a result, the Commission considers the GDPR to be an effective instrument that imposes appropriate obligations on controllers and processors and ensures the protection of data subjects. In particular, the enforcement and implementation of the requirements of the GDPR were perceived more strongly compared to the first evaluation in 2020 and the authorities had more - albeit not enough - resources at their disposal to carry out their tasks effectively. However, there is still room for improvement in some areas. As in the first report, the Commission once again called for closer and more effective cooperation between supervisory authorities at national and European level. According to the Commission, cross-border cases in particular have become increasingly important in recent years and require effective European cooperation between authorities. In addition, the further standardization of the interpretation and understanding of the GDPR must be promoted throughout Europe, as has already been successfully done in the past through guidelines from the data protection authorities and the requirements of case law. In addition, the focus should once again be on supporting small and medium-sized enterprises in implementing the requirements of the GDPR.

[To the evaluation report of the EU Commission \(dated 25 July 2024\)](#)

# 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](#)



### Mirjam Kaiser

+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](#)



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](mailto:BB-Datenschutz-Ticker@advant-beiten.com)

[www.advant-beiten.com](http://www.advant-beiten.com)



[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.

© Beiten Burkhardt

Rechtsanwaltsgesellschaft mbH

All rights reserved 2024

**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](http://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.