

# Privacy Ticker

March 2022



**+++ Digital data files may need to be blackened +++ Employer ordered to pay EUR 1000 in damages per incomplete GDPR disclosure +++ EUR 17 million fine against Meta +++ EUR 20 million fine against Clearview AI +++ Increased data protection controls in direct marketing, employee monitoring and cloud computing in France +++ New FAQ on tracking and cookies +++**

## 1. Changes in Legislation

### **+++ UTAH PASSES DATA PROTECTION LAW +++**

Utah was the fourth US American federal state (after California, Virginia and Colorado) to pass a data protection law. The Utah Consumer Privacy Act (UCPA) is similar to the Virginia Consumer Data Privacy Act of the federal state of Virginia. In contrast to the GDPR, the UCPA only protects personal data of consumers; employees are explicitly excluded from the scope of application of the law. The UCPA grants consumers a right to access, copy and erase data, as well as a right to object to the sale of data. The concept of controller and processor was also adopted from the GDPR. Overall, the UCPA is considered somewhat more industry-friendly than the GDPR or other US data protection laws. The law is supposed to come into force on 31 December 2023.

[To the text of the UCPA](#)

## 2. Case Law

### **+++ HIGHER REGIONAL COURT OF FRANKFURT: UNLAWFUL TRANSFER OF APPLICANT DATA DOES NOT LEAD TO GDPR DAMAGES +++**

The Higher Regional Court of Frankfurt has dismissed the claim of a rejected applicant for damages under the GDPR. The plaintiff had applied for a job at a bank via the Xing platform. In the course of the application procedure, the bank had mistakenly forwarded

a message intended for the applicant to a third Xing user and did not inform the applicant of this until several months later. Because of this data protection violation, the defendant bank was ordered to pay EUR 1,000 in damages in the first instance. The Higher Regional Court of Frankfurt now ruled differently. The plaintiff had not succeeded in showing concrete non-material damage, "which also includes anxiety, stress and loss of comfort and time". The question of whether and to what extent concrete damages must be proven in the context of the GDPR damages claim is answered inconsistently by the courts (the Regional Labour Court of Berlin-Brandenburg, for instance, ruled differently, see below).

[To the decision of the Higher Regional Court of Frankfurt a.M. \(dated 2 March 2022, 13 U 206/20, German\)](#)

---

### **+++ REGIONAL LABOUR COURT OF BERLIN-BRANDENBURG: EUR 1,000 GDPR DAMAGES PER INCOMPLETE GDPR INFORMATION +++**

The Berlin-Brandenburg Regional Labour Court ordered an employer to pay damages under the GDPR totalling EUR 2,000 for two incomplete information disclosures (Article 15(1) GDPR). The employee had requested information on two specific facts (a warning and a works council hearing). According to the Court, the information provided was "obviously incomplete" because, among other things, information on the recipients and the storage period of the data was missing. With regard to the damage, the Court held that the erroneous information had led to a "loss of control" on the part of the plaintiff, which made it difficult to verify the lawfulness of the data processing. The plaintiff was entitled to a non-material claim for damages "irrespective of whether a materiality threshold had been reached in the case of violations of the provisions of the GDPR". The amount of damages of EUR 1,000 per violation was appropriate and ensured that Article 15 of the GDPR was enforced. In its reasoning, the Court referred to a similar ruling by the Lower Saxony Regional Labour Court (see [AB Privacy Ticker December 2021](#)).

[To the judgement of the Berlin-Brandenburg Regional Labour Court \(dated 18 November 2021 - 10 Sa 443/21, German\)](#)

---

### **+++ HIGHER REGIONAL COURT OF DRESDEN ON THE ERASURE OF DATA IN CASE OF RETENTION PERIODS +++**

The Dresden Higher Regional Court obliged a debt collection agency to partially erase a database, even though it is in principle subject to the statutory retention obligations pursuant to Section 147 of the German Fiscal Code. Earlier, the plaintiff had requested the debt collection agency to erase the data concerning his person, but the request for

erasure was rejected with regard to the statutory retention periods. The Court took the view that the statutory retention period only existed for individual pieces of information in the data record (name, address and date of birth). But insofar as the electronic data stock contains further data that does not have to be retained, these would have to be deleted or at least provided with access restrictions. For instance, the "digital blackening" of identifying data on business correspondence could be considered. In this case, it is the responsibility of the controller to organise the data accordingly.

[To the decision of the Higher Regional Court of Dresden \(dated 14 December 2021, 4 U 1278/21, German\)](#)

---

## 3. Regulatory Investigations and Enforcement Actions

### +++ DATA PROTECTION AUTHORITY BREMEN IMPOSES MILLION-EURO FINE ON HOUSING ASSOCIATION +++

The Bremen State Commissioner for Data Protection and Freedom of Information has fined BREBAU GmbH EUR 1.9 million. The company had processed more than 9,500 data of potential tenants without a legal basis. This included particularly sensitive data such as information on skin colour, ethnic origin, religious affiliation, sexual orientation and state of health, but also information on hair styles, body odour and personal appearance. The authority emphasised that due to the "extraordinary severity" of the violation, a "significantly higher fine would have been appropriate". However, the company's extensive cooperation and efforts to reduce damages led to a "significantly" reduced fine.

[To the press release of LfDI Bremen \(dated 3 March 2022, German\)](#)

---

### +++ IRISH DATA PROTECTION AUTHORITY IMPOSES EUR 17 MILLION FINE ON META +++

The Irish Data Protection Commission (DPC) has imposed a fine of EUR 17 million on the Irish offshoot (Meta Platforms Ireland Ltd.) of the Meta Group, operator of Facebook, Instagram and WhatsApp, among others. According to the authority, the company had not taken sufficient technical and organisational measures to protect the data of European users and thus violated the obligations under Article 32 GDPR, among others, after twelve data breaches had occurred in 2018. The company argues that it only violated documentation obligations. In this respect, the GDPR accountability obligations stipulate that any security measures taken must always be documented (Art. 5(2) GDPR).

[To the DPC press release \(dated 20 March 2022\)](#)

### **+++ ITALIAN DATA PROTECTION AUTHORITY IMPOSES EUR 20 MILLION FINE AGAINST CLEARVIEW AI +++**

The Italian Data Protection Authority Garante per la Protezione dei Dati Personali (GPDP) has imposed fines totalling EUR 20 million on the US company Clearview AI. The company had compiled more than 10 billion publicly available photos of faces in a database and created biometric profiles of Italian citizens, among others, on this basis. These were partly complemented with further data (including geolocation data). According to the GPDP, this procedure violated numerous provisions of the GDPR. Among other things, there was no legal basis for the processing of biometric data (Art. 6 and Art. 9 GDPR) and data subjects were not sufficiently informed (Art. 12, 13 and 14 GDPR). Moreover, the company did not have an EU representative (Art. 27 GDPR). The GPDP prohibited the company from using the software.

[To the administrative fine notice of GPDP \(dated 10 February 2022, Italian\)](#)

[To the press release of the European Data Protection Board \(dated 20 March 2022\)](#)

---

### **+++ FRENCH DATA PROTECTION AUTHORITY: FOCUS ON DIRECT MARKETING, EMPLOYEE MONITORING AND CLOUD COMPUTING IN 2022 +++**

The French Data Protection Authority Commission Nationale de l'Informatique et des Libertés (CNIL) has announced that in 2022 the authority will focus on direct marketing, home office employee monitoring and cloud computing. Companies with headquarters or business activities in France must therefore expect increased data protection controls in these areas. According to CNIL, software tools used in companies that allow remote access to the working environment will be examined for possible tracking measures. In the examination of cloud services, on the other hand, the focus will be on third-country transfers and the (correct) configuration of the services. The use of cloud services in the public sector is also the focus of a Europe-wide coordinated data protection initiative of the European Data Protection Board (EDPB).

[To the CNIL press release \(dated 15 February 2022\)](#)

[To the EDPB press release \(dated 15 February 2022\)](#)

---

## **4. Opinions**

### **+++ DATA PROTECTION CONFERENCE: UPDATED GUIDANCE FOR DIRECT MARKETING +++**

The body of German Data Protection Authorities (*Datenschutzkonferenz, DSK*) has published a new version of the guidance on the processing of personal data for direct marketing purposes. Among other things, the DSK provides practical advice and

recommendations on the data protection requirements of classic direct advertising, such as by post, e-mail or telephone (except for address trading). As compared to the original version of 2018, the DSK now no longer makes the general assumption that consent once given is forfeited after a certain period of time. Instead, it unfortunately remains unclear when profiling measures can possibly still be based on legitimate interests and (as of) when consent is required.

[To the DSK's orientation guide \(as of February 2022, German\)](#)

---

### **+++ DATA PROTECTION AUTHORITY OF BADEN-WUERTTEMBERG PUBLISHES FAQ ON TRACKING AND COOKIES +++**

In an FAQ, the State Commissioner for Data Protection and Freedom of Information of Baden-Wuerttemberg provides information on the use of cookies and tracking mechanisms in compliance with data protection regulations. Among other things, the FAQ answers very practical questions on the use of external media content and social plugins on websites, on coverage analysis and on the design of cookie banners (especially cookie banner texts) from the perspective of public authorities. Readers are made aware of typical "standard errors" in consent management and the use of cookie banners by means of negative examples. As expected, the requirements of the Data Protection Authority are very high. However, the FAQ contains many useful tips for companies and operators of websites, apps or networked devices, even outside of Baden-Wuerttemberg.

[To the FAQ of the LfDI Baden-Wuerttemberg \(as of March 2022, German\)](#)

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)

Your Contacts of the  
Privacy Team



[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 2022

**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.