



## 1. CASE LAW

### **+++ HIGHER REGIONAL COURT OF MUNICH: RIGHT TO COPIES OF DATA INCLUDES E-MAILS, LETTERS, TELEPHONE NOTES, MEMOS AND MINUTES OF CONVERSATIONS +++**

The Higher Regional Court of Munich has ruled that a data subject can demand a copy of internal telephone notes, file notes, minutes of conversations, e-mails and letters, each of which contains information about him or her, from the company being the controller under data protection law. The Court thus interprets the scope of the so-called right to copy data pursuant to Article 15 (3) GDPR, which has always been controversial, in an extremely broad manner. The Court is of the opinion, similar to the recent decision of the Federal Supreme Court ([see BB Privacy Ticker July 2021](#)), that the right to copy data, just like the right to information under Article 15 (1) GDPR, basically covers all personal data and thus also the entire content of opinions, evaluations or internal memos relating to the data subject.

[To the decision of the Higher Regional Court Munich \(dated 4 October 2021 – 3 U 2906/20, German\)](#)

### **+++ HIGHER REGIONAL COURT OF DRESDEN: NO FURTHER DUTY TO PROVIDE INFORMATION AFTER NEGATIVE GDPR NOTICE +++**

The Dresden Higher Regional Court has ruled that a data subject's request for information pursuant to Article 15 (1) GDPR is fully satisfied upon the provision of negative information. In a negative notice, data subjects are informed that no personal data about them is being processed. In the case in question, the data subject received such negative notice and requested further information from the defendant company on previous processing activities. The Court rejected this request as the GDPR does not provide for such a further obligation to provide information.

[To the judgment of the Dresden Higher Regional Court \(dated 31 August 2021 – 4 U 324/21, juris, German\)](#)

### **+++ ADMINISTRATIVE COURT OF WIESBADEN: NO RIGHT TO INTERVENTION BY THE DATA PROTECTION AUTHORITY +++**

The Wiesbaden Administrative Court dismissed the action against a data protection authority by which the data subject wanted to oblige the authority to issue a deletion order. The data subject had turned to the data protection authority after unsuccessfully seeking the deletion of his debtor data, which had been stored at a credit agency. The data protection authority refused to intervene against the credit agency. The legal action against this remained unsuccessful. The Court stated that a claim for intervention by the authority could only exist if the authority's discretion was reduced to zero. However, the authority had acted without any discretionary fault. The plaintiff's submission also did not show such a reduction of discretion in the specific case.

[To the judgment of the Wiesbaden Administrative Court \(dated 24 September 2021, 6 K 442/21, JurPC, German\)](#)

### **+++ PFAFFENHOFEN LOCAL COURT: UNAUTHORISED ADVERTISING E-MAIL LEADS TO EUR 300 IN DAMAGES UNDER THE GDPR +++**

The Pfaffenhofen Local Court has ordered a company to pay GDPR damages of EUR 300 for the unauthorised sending of an e-mail advertising FFP2 masks. The defendant company had not obtained

consent from the recipient to receive direct advertising. Thus, the recipient's e-mail address was processed unlawfully, which led to the damages claim under Article 82 GDPR. The Court argued that damage on the recipient's side "could also already lie in the uneasy feeling [...] that personal data have become known to unauthorised persons". The fact that the defendant had only very hesitantly and vaguely disclosed information about the origin of the e-mail address had furthermore had the effect of increasing the damage.

[To the judgment of the Pfaffenhofen Local Court \(dated 9 September 2021, 2 C 133/21, German\)](#)

## 2. REGULATORY INVESTIGATIONS AND ENFORCEMENT ACTIONS

### **+++ ITALIAN DATA PROTECTION AUTHORITY IMPOSES MILLION DOLLAR FINE FOR ILLEGAL ADVERTISING CALLS +++**

The Italian data protection authority Garante per la Protezione dei Dati Personali (GPDP) has imposed a fine of EUR 3.2 million on Pay-TV provider Sky Italia S.r.l. for systematic data protection violations in the field of telephone advertising. Sky had acquired lists of contact data from various companies without informing the data subjects of this in a privacy statement. In addition, the company allegedly made advertising calls without the required consent and without comparing the telephone numbers with an objection register. The authority has additionally imposed a number of remedial measures on Sky.

[To the administrative fine notice of GPDP \(dated 16 September 2021, Italian\)](#)

[To the GPDP press release \(dated 19 October 2021, Italian\)](#)

### **+++ AUSTRIAN DATA PROTECTION AUTHORITY SETS EUR 9.5 MILLION FINE FOR MISSING E-MAIL CONTACT +++**

According to press reports, the Austrian data protection authority has imposed a fine of EUR 9.5 million on Österreichische Post AG. The

company is accused of providing only incomplete contact options for data protection information as no requests could be made by e-mail. However, the company did provide contact options for data protection enquiries by post, web form and via customer service. The company argues that web forms are "customary in the market" compared to e-mails and "facilitate" data protection enquiries, as data subjects are guided to "correctly disclose everything they need to know right away instead of having to answer several follow-up questions". Hence, Österreichische Post AG announced its intention to appeal against the fine.

[To the press report at Der Standard \(dated 28 September 2021, German\)](#)

### **+++ FRENCH DATA PROTECTION AUTHORITY FINES COMMERCIAL PLATFORM FOR VARIOUS DATA PROTECTION VIOLATIONS +++**

The French data protection authority Commission Nationale de l'Informatique et des Libertés (CNIL) has fined trading platform Brico Privé in the amount of EUR 500,000. The company was charged with several violations at the same time. On the one hand, there was no sufficient deletion concept for the collected data, so that data was stored for too long, even though user accounts had not been active for several years; requests for deletion from data subjects were also ignored in parts. On the other hand, the company sent unauthorised e-mail advertising without obtaining the necessary consent of the addressees. Also, Brico Privé had installed cookies on the end devices of the data subjects without their consent. And finally, the CNIL criticised the insecure handling of passwords, both for customer accounts and for employees' access to the internal CRM system.

[To the administrative fine notice of CNIL \(dated 14 June 2021, French\)](#)

### **+++ EDPB FORMS "TASK FORCE" FOR COOKIE BANNER COMPLAINTS +++**

The European Data Protection Board, consisting of representatives of national data protection authorities and the European Data Protection Supervisor, has set up a "task force" to deal with complaints about unlawful cookie banners. The reason for this is the dispatch of over 500 complaints by the private organisation "None of Your Business" in May 2021.

The focus here was in particular on cookie banners that did not provide a simple option to reject all cookies (e.g. a "reject all" button). The focus here was in particular on cookie banners that did not provide a simple option to reject all cookies (e.g. a "reject all" button).

[On the EDPB press release \(dated 27 September 2021\)](#)

## 3. OPINIONS

### +++ THE FEDERAL OFFICE FOR INFORMATION SECURITY PUBLISHES FAQ ON IT SECURITY ACT 2.0 +++

The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) publishes FAQ on IT Security Act 2.0 ([see BB Privacy Ticker June 2021](#)). Among other things, the law makes strict specifications for the IT security of "critical infrastructures" and, newly added, for "companies in the special public interest". The FAQ contains information on which companies are classified as companies in the special public interest, what obligations these companies are subject to and how these obligations can be fulfilled. While parts of the IT Security Act 2.0 already became effective on 28 May 2021, the rest of the law will come into force on 1 December 2021.

[To the FAQ of BSI, 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 Privacy Ticker also contains contributions from ADVANT partner law firms Nctm and Altana.

#### EDITOR IN CHARGE

Dr Andreas Lober | Rechtsanwalt  
© BEITEN BURKHARDT  
Rechtsanwaltsgesellschaft mbH

Your contact of  
Privacy Team

[Datenschutz-Ticker@advant-beiten.com](mailto: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 2021

**Imprint**

This publication is issued by BEITEN BURKHARDT Rechtsanwalts-gesellschaft 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 Rechtsanwalts-gesellschaft 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.