



## 1. Changes in legislation

### +++ NEW STANDARD DATA PROTECTION CLAUSES ADOPTED +++

On 4 June 2021, the EU Commission adopted new standard data protection clauses for the transfer of personal data to third countries (Art. 46 (2) lit. c) GDPR). The new clauses have a modular structure and cover four constellations of data transfers:

- Controller to Controller (Module 1)
- Controller to Processor (Module 2)
- Processor to (Sub-)Processor (Module 3)
- Processor to Controller (Module 4)

In terms of content, the new clauses are intended to take into account, among other things, the Schrems II case law of the European Court of Justice (ECJ). It is now mandatory for the contracting parties to carry out and document a risk assessment for the specific data transfer (also called "Transfer Impact Assessment"), which must be submitted to the authorities upon request. The new standard data protection clauses replace the previously applicable standard contractual clauses. Companies that base their data transfer on the previously applicable clauses must replace them within a transition period of 18 months.

[To the EU Commission's decision on the new standard data protection clauses](#)  
[To the press release of the EU Commission of 4 June 2021](#)

## **+++ IT SECURITY ACT 2.0 ENTERS INTO FORCE +++**

The Second German Act to Increase the Security of Information Technology Systems (IT Security Act 2.0) was promulgated on 27 May 2021. The IT Security Act 2.0 extends the competences and tasks of the Federal Office for Information Security (BSI) and makes amendments to the German Act on the BSI (BSIG): In future, in addition to "critical infrastructures" and "digital services", "companies in the special public interest" will also be subject to the duties of the BSIG. This includes, for instance, companies and suppliers with particularly great economic importance for Germany. A majority of the IT Security Act 2.0 already came into force on 28 May 2021, but individual provisions will only become effective on 1 December 2021.

[To the German IT Security Act 2.0](#)

[Brief overview of the BSI on the IT Security Act 2.0](#)

---

## **+++ WORKS COUNCIL MODERNISATION ACT: EMPLOYER RESPONSIBLE FOR DATA PROCESSING OF THE WORKS COUNCIL +++**

The German Act on the Promotion of Works Council Elections and Works Council Work in a Digital Working World (Works Council Modernisation Act) came into force on 18 June 2021. Among other things, the Act provides that the employer is responsible under data protection law for the processing of employee data by the works council. However, this only applies if the works council processes the data to fulfil the tasks within its competence. Thus, the employer's data protection officer is also competent for the works council's data processing. The above issues were strongly disputed before this legal clarification.

[To the Works Council Modernisation Act](#)

---

## **2. Case Law**

### **+++ ECJ: BELGIAN DATA PROTECTION AUTHORITY RESPONSIBLE FOR GDPR VIOLATIONS BY FACEBOOK IRELAND +++**

The ECJ has ruled that, in exceptional cases, national data protection authorities can take action against a company's GDPR violations before a domestic court, even though the company's principal place of business –and thus the actual competent so-called lead authority – is located in another Member State. In the case in question, the Belgian data protection authority had brought an action before a domestic court against Facebook Ireland, based in Ireland, for breaches in the processing of data of Belgian users. Facebook had argued that the authority was acting outside its

jurisdiction processing was domiciled in Ireland. The ECJ has now clarified that the Belgian authority may take action against Facebook Ireland under the consistency mechanism (Art. 60 et seq. GDPR) and may also bring an action before Belgian courts in this respect, even if Facebook does not have its own establishment in Belgium.

[To the press release of the ECJ \(of 15 June 2021 – C-645/19\)](#)

---

### **+++ WIESBADEN LOCAL COURT: COLLECTION OF SEVERAL CONTRACTS IN A FOLDER LEADS TO APPLICABILITY OF THE GDPR +++**

The Local Court of Wiesbaden found that the tenant of a flat was entitled to a claim for information under Art. 15 GDPR against the landlord, who rented out several flats as a private individual. The landlord had not stored her rental contracts digitally, but only physically filed them in a folder. According to the court, this collection constituted a file system within the meaning of the GDPR, so that the provisions of the GDPR were applicable. The landlord had also stored the tenant's name and telephone number in a mobile phone. The court found this to be automated data processing, so that the GDPR was also for this reason applicable.

[To the judgement of the Wiesbaden Local Court \(of 26 April 2021, file ref. 93 C 2338/20\)](#)

---

### **+++ COLOGNE REGIONAL COURT ON THE WORDING OF COOKIE BANNERS +++**

The Regional Court of Cologne has ruled that the following wording in a cookie banner is unlawful:

*"To optimally design our website for you and to be able to continuously improve it, we use cookies. If you continue to use the Website, you consent to our use of cookies."*

The provision violates Section 15 (3) of the German Telemedia Act (TMG). The Federal Court of Justice interprets this provision to mean that users must give their express consent to the creation of user profiles for advertising purposes (see the [BB special newsletter May 2020](#)).

[To the decision of the Cologne Regional Court \(of 13 April 2021 – 31 O 36/21\)](#)

## **+++ CONSEIL D'ÉTAT DISMISSES LAWSUIT DUE TO THREAT OF DATA TRANSFER TO THE USA +++**

The French Supreme Administrative Court (Conseil d'État) has dismissed a lawsuit concerning the use of the hosting provider Amazon Web Services Sarl (AWS), a subsidiary of the American Amazon Web Services Inc. A processor of the French Ministry of Health used the services of AWS in connection with a platform for managing vaccination appointments. The plaintiffs feared that personal data could be transferred from this platform to the USA. The Conseil d'État clarified that sufficient additional measures had been taken to provide an adequate level of protection in the USA. The measures taken included encrypting the data before it was transferred to AWS, with the key held in trust by a third party based in France, so that AWS itself did not have access to clear data. The Conseil d'État explicitly pointed out that no health data considered particularly sensitive had been transferred to AWS. The context of the decision is the so-called Schrems II decision of the ECJ (Ruling of 16 July 2020, C311/18, see [BB Privacy Ticker July 2020](#)).

[To the decision of the Conseil d'État \(of 12 March 2021, n° 450163\)](#)

---

## **3. Regulatory Investigations and Enforcement Actions**

### **+++ GERMAN DATA PROTECTION AUTHORITIES MONITOR IMPLEMENTATION OF THE SCHREMS II RULING +++**

Various German data protection authorities have announced that they will review data transfers by companies to third countries as part of a coordinated cross-border monitoring process to ensure that the requirements of the ECJ's Schrems II ruling are implemented. For this purpose, companies are currently being sent extensive questionnaires concerning the following topics: the use of service providers for sending e-mails, for hosting websites, for web tracking, for managing applicant data as well as the intra-group exchange of customer data and employee data. According to current knowledge, the data protection authorities of Bavaria, Berlin, Brandenburg, Hamburg, Lower Saxony, Rhineland-Palatinate and Saarland are participating in these reviews.

[To the press release of the Hamburg Data Protection Commissioner, including questionnaires](#)

### **+++ DUTCH DATA PROTECTION AUTHORITY FINES EUR 525,000 FOR ABSENT UNION REPRESENTATIVE +++**

The Netherlands' data protection authority Autoriteit Persoonsgegevens (AP) has fined the non-European operator of a website in the amount of EUR 525,000. The operator had not appointed a Union representative, although according to the authority it should have done so under Article 27 GDPR. The provision obliges controllers and processors established exclusively in a third country to designate a representative within the Union as an obligation and enforcement subject.

[To the decision of the AP \(Dutch\)](#)

---

### **+++ LUXEMBOURG DATA PROTECTION AUTHORITY: RECORD FINE EXPECTED AGAINST AMAZON +++**

Luxembourg's data protection authority, the National Commission for Data Protection (CNPD), is planning to impose a fine of around EUR 350 million on Amazon, according to a newspaper report in the Wall Street Journal. As the lead authority, the CNPD is responsible for data processing by the Amazon Group in Europe. It had sent a draft of the decision to the other data protection authorities concerned as part of the consistency procedure (Art. 60 et seq. GDPR). It is currently not known which data protection violations Amazon is accused of in detail.

[To the freely available German report on Heise Online](#)

---

## **4. Opinions**

### **+++ EU AUTHORITIES PUBLISH UPDATED RECOMMENDATIONS ON THIRD COUNTRY TRANSFERS +++**

The European Data Protection Board (EDPB) has published an updated version of the recommendations on additional measures to secure data transfers to third countries. A first version of these recommendations already dates back to November 2020 (see [BB Privacy Ticker November 2020](#)). In the updated version, the EDPB also adheres to the recommended 6-step test for data transfers to third countries (*1. Know your transfer; 2. Verify transfer tool; 3. Assess legal system in the third country; 4. Consider supplementary measures; 5. Take formal procedural steps; 6. Re-evaluate*). Furthermore, the EDPB explains additional safeguards that companies should take in addition to concluding EU standard data protection clauses in order to ensure an adequate level of data protection in the third country.

[To the recommendations of the EDPB of 18 June 2021](#)

[To the EDPB's recommendations for the assessment of state access powers in the third country of 10 November 2020](#)

## Your contacts

**Editor in charge**

[Dr Andreas Lober](#)

[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 Rechtsanwaltsgesellschaft mbH

Ganghoferstrasse 33, 80339 Munich

Registered under HR B 155350 at the Regional Court Munich / VAT Reg. No.: DE811218811

For more information see: [www.beiten-burkhardt.com/en/imprint](http://www.beiten-burkhardt.com/en/imprint)