

## **Country Report BfDI for 75<sup>th</sup> IWGDPT Berlin Group Meeting**

**1<sup>st</sup> / 2<sup>nd</sup> – 3<sup>rd</sup> July 2025**

**Tbilisi, Georgia**

### News and information from the BfDI –

#### Federal Commissioner for Data Protection and Freedom of Information, Germany

#### **Enforcement:**

##### **- Fine on Vodafone**

BfDI has imposed two fines totalling 45 million euros on Vodafone GmbH. Due to malicious employees in partner agencies who broke contracts to customers, there had been fraud cases due to fictitious contracts or contract changes at the expense of customers, among other things.

A fine of 15 million euros was imposed because in terms of data protection law (Article 28 (1) sentence 1 GDPR), Vodafone GmbH had not adequately reviewed and monitored partner agencies working on its behalf. Moreover, as vulnerabilities in certain distribution systems had been identified, the BfDI issued a warning to Vodafone for violating Article 32(1) of the GDPR.

A further fine of 30 million euros was imposed for security deficiencies in the authentication process for the combined use of the online portal 'MeinVodafone ("My Vodafone")' with the Vodafone Hotline. The identified authentication vulnerabilities enabled, among other things, unauthorized third parties to access eSIM profiles.

Vodafone GmbH has now improved its processes and systems and in some cases even completely replaced them in order to eliminate such risks in the future. BfDI will review this again in the future.

##### **- Coordinated Enforcement Action of EDPB on the Right to Erasure (Art. 17 GDPR)**

BfDI and several German data protection supervisory authorities of the federal states (Baden-Württemberg, Brandenburg, Mecklenburg-Western Pomerania, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate) are participating this year (2025) in the Europe-wide 'Coordinated Enforcement Framework' (CEF) review action of the European Data Protection Board (EDPB). A total of 32 European supervisory authorities will take part in this coordinated action.

CEF 2025 is about the right to erasure under Art. 17 GDPR. The right to erasure is one of the most frequently exercised data subject rights and one about which the data protection supervisory authorities receive many complaints.

One of the aims of this coordinated action is to assess the implementation of this right in practice. This will be done using a jointly developed questionnaire, for example by analysing and comparing the procedures put in place by different data controllers. The aim is to identify the most important aspects of compliance with this law and to gain an overview of best practice.

The results of the joint initiative will be analysed within the framework of the EDPB and published in a report upon completion.

The coordinated action on the right to erasure is the fourth initiative under the CEF, which aims to improve the enforcement of the GDPR and cooperation between data protection authorities within the EU. Previous coordinated actions dealt with the right of access (2024), the appointment and role of data protection officers (2023) and the use of cloud services by the public sector (2024).

#### **- Largely-automated check of internet websites**

The BfDI has started to develop a largely automated procedure for checking websites under data protection law. Certain predefined if-then statements are used as part of the check routine. The result provided is always checked by a human and utilised further.

The aim of the procedure is to support the BfDI employees entrusted with monitoring and advisory activities and to advise the supervised organisations on the implementation of data protection-friendly alternatives. This is intended to increase the overall efficiency of the BfDI's activities in this area.

As part of its responsibilities, the BfDI has audited websites of federal public bodies in a first round. So far, this has involved around 180 websites with around 500,000 URLs. The automated website check has already produced good results. The check procedure and the associated processes are to be further developed and the scope of the websites to be checked is to be expanded.

#### **BfDI Office:**

#### **- BfDI engages in a pilot project on AI real-world laboratories (“Sandbox”)**

BfDI is participating in a pilot project to simulate an AI real-world laboratory together with the Federal Network Agency (BNetzA) and the Hessian Ministry for Digitalisation and Innovation.

AI real-world laboratories offer companies controlled environments in which AI systems can be developed and tested under the most realistic conditions possible before they are launched on the market. This makes them an important tool for accelerating innovation.

The aim of the project is to simulate key requirements, processes and challenges of AI real-world laboratories under realistic conditions in line with the European AI Regulation (AI Regulation), which came into force in August 2024, and thus increase knowledge and understanding of real-world laboratories. The results of the project should be available by the end of 2025.

As part of the project, the processes of an AI real-world laboratory will be simulated using specific cases from participating companies. Necessary requirements and resources for real-world laboratories will also be determined. The results of the pilot project are intended to serve as a guide for all those involved in the future establishment and operation of genuine AI real-world laboratories. The findings will be made available to other federal states and public institutions in order to support the establishment of real-world laboratories nationwide in Germany and to be able to fully utilise the opportunities that real-world laboratories open up for the economy, especially in the field of AI.

#### **Guidance:**

##### **- EDPB on Pseudonymization**

The BfDI welcomed the further clarification given by the European Data Protection Board (EDPB) in January 2025 on the concept of pseudonymisation, which is relevant in practice, because BfDI considers that pseudonymisation is an effective method of reducing risks in data processing.

The General Data Protection Regulation (GDPR) describes pseudonymisation as a measure that can reduce risks for data subjects and support controllers and processors in complying with their data protection obligations. The EDPB's guidelines are now intended to assist controllers in fulfilling their data protection obligations through technology design and data protection-friendly default settings and security.

The EDPB has made the guidelines available for public consultation for 8 weeks in order to give stakeholders the opportunity to comment and to enable the inclusion of current developments in case law.

##### **- Expertise on AI commissioned from EDPS Support Pool of Experts**

On the initiative of the BfDI, the European Data Protection Board (EDPB) has commissioned an expert opinion on artificial intelligence (AI) applications via its Support Pool of Experts programme.

If personal data is processed using AI procedures, data protection requirements must also be observed. In his study, expert Dr Kris Shrishak looks at the challenges involved in identifying and removing discriminatory bias and the effective implementation of data subjects' rights in the various lifecycle phases of an AI application.

The results are now available and can be freely accessed on the EDPB website.

## **Policy and Jurisdiction:**

### **- Consent Regulation entered into force in January 2025**

The Regulation pursuant to Section 26 (2) of the Telecommunications Digital Services Data Protection Act (TDDDG), known as the Consent Regulation (EinwV), has created the legal framework for an alternative consent procedure to cookie banners.

This enables new consent management services to be recognised by the Federal Commissioner for Data Protection and Freedom of Information (BfDI). The services should be able to provide user-friendly and competition-compliant procedures to manage the consent of end users required under the TDDDG. The effectiveness of the new consent regulation is to be evaluated within two years. It will then be reviewed whether the regulation and the associated security measures are sufficient to actually have a positive effect for users. In addition, the aim is to work towards a Europe-wide solution for service providers to manage consent.

### **- AI responsibility to Federal Network Agency**

BfDI has not been assigned responsibility for overseeing AI regulation in Germany.

Currently, Germany is in the process of transposing the EU AI Regulation—effective since 1 August 2024—into national law. This will be done via the “AI Market Surveillance Act” (KIMÜG), proposed in December 2024, which designates the Federal Network Agency (BNetzA) as the lead market surveillance and notifying authority, supported by two internal bodies (UKIM and KoKIVO) and managed under conformity assessment frameworks. EU Member States must establish these structures by 2 August 2025, prior to full application of the EU AI regulation in 2026.

To foster innovation, BNetzA is expected to operate AI sandboxes offering legal clarity for developers— BfDI is engaging in AI real-world laboratories in this context

(see one of the previous bullet points) and will be ready to provide its expertise to the BNetzA.

The new federal government administration, in office since May 2025, has expressed that it will support an “innovation-friendly” rollout and expansion of AI infrastructure.

- **New Federal Government published plans for “centralization”; BfDI responsible for private sector**

In May 2025, a new Chancellor was elected by the members of the Federal Parliament (“Bundestag”) in Germany, after two parties – the Christian Democrats and the Social Democrats – had reached an agreement to form a new coalition and government. According to this coalition agreement, these parties are endeavoring to bundle data protection supervision of the private sector with the Federal Data Protection Commissioner (BfDI), which was described as “centralisation” of supervisory competences. The BfDI is now already responsible for the supervision of a number of nationwide commercial enterprises with data-driven business models and different locations, such as telecommunications and postal services.

The centralisation would need to be implemented during the mandate of the coalition government, which will expire after four years in Spring 2029.