GDPR enforcement trends in German privacy practice

Lars Lensdorf, **Moritz Hüsch** and **Evangelos Karalias** of Covington & Burling report on the evolving legal environment in Germany.

The number of data protection enforcement proceedings has been increasing constantly over the years, a trend that is expected to persist. This increase applies not only to the frequency of proceedings but also to the size of the fines imposed. Significant factors driving the anticipated continuation of this trend are the various new decisions by the European Court of Justice (ECJ) and the Federal Court of Justice (BGH) in relation to the interpretation of the GDPR and national data protection laws. In this article, we explain some key decisions of the ECJ and the BGH and illustrate their possible impact on enforcement practice.

ECJ judgment on EU GDPR enforcement

In a judgment dated 5 December 2023, the ECJ laid down formal requirements for issuing enforcement requirements under Article 83 GDPR (see below).[1]

Background: In 2021, the Higher Regional Court of Berlin (KG Berlin) requested a preliminary ruling from the ECJ whether Arts. 83(4) to (6) EU-GDPR preclude the application of national provisions with regard to EU-GDPR enforcement. Amongst other things, national enforcement provisions in Germany require that a natural and identified person within the controller's organisation committed the administrative offence. For example, pursuant to Section 30 of the German Act on Regulatory Offences (*Ordnungswidrigkeitengesetz* or OWiG) a fine could only be imposed against a company if a member of the management committed a reproachable act.[2] If authorities and courts were to apply these strict national rules, it would have been quite difficult (in many cases, impossible) to prove such an act by a member of the management, and would, in any event, require material time and effort to try and collect the relevant facts.

ECJ decision on enforcement requirements: The ECJ decided in favour of the authorities and declined the applicability of the national enforcement rules. These rules were, in the Court's view, incompatible with the EU GDPR and their application would impose additional requirements that would ultimately restrict the enforcement of the EU GDPR.

However, the ECJ also restricted the conditions for the imposition of fines in such a way that the underlying infringement must be linked to at least negligent behaviour on the part of the controller (or processor). Unfortunately, the ECJ did not clarify when this requirement is met, which leaves significant room for interpretation. Consequently, some German Data Protection Authorities may need to change their enforcement practice. For example, the Berlin Data Protection Authority has taken the stance that an infringement of a data protection rule is sufficient for the imposition of a fine. However, now, these Data Protection Authorities will have to demonstrate that there was (or is) a negligent or intentional infringement, which is a higher hurdle to overcome.

Consequences for German EU-GDPR enforcement: As set out above, courts will now have to set out criteria for the analysis of whether an infringement was negligent, intentional, or not. Where Data Protection Authorities and courts applied the national enforcement rules, these new requirements will make it less burdensome for them to demonstrate that the requirements for a fine are met. However, for other Data Protection Authorities (e.g., Berlin), these new requirements will make it more burdensome (compared to their previous practice) to demonstrate that the requirements for a fine are met.

ECJ Judgment of 4 October 2024 on Litigation in Privacy

In recent decisions, the ECJ set out key principles for German privacy litigation. These principles are likely to significantly boost the relevance of German competition law to the EU-GDPR.

EU-GDPR alongside competition claims – Background: In a case concerning the online distribution of medical products, a pharmaceutical company argued against its competitor's practice of collecting health data without explicit customer consent, as required by Articles 6 and 9(1) and (2)(a) of the EU-GDPR. This challenge led the BGH to refer the case to the ECJ, questioning if competitors have the right to claim data protection infringements against each other. [3]

ECJ decision on unlawful competition claims: The ECJ ruled in that case that the EU GDPR does not exclusively determine legitimacy for data protection claims, and widened potential claims for violation of data protection requirements also to competitors from the angle of unfair business practices under German competition law.[4]

Consequences for infringements of the German EU GDPR: While the full impact of this case on controllers is not yet fully clear, controllers should prepare for data infringement claims not only from data subjects or supervisory authorities but also from competitors. This could shift privacy litigation strategies, with competitors aiming to hinder business activities rather than prevent privacy infringements.[5] However, the impact of competition claims may be limited by Section 13(4) No. 2 of the Act against Unfair Competition (*Gesetz gegen den Unlauteren Wettbewerb,* UWG) which excludes reimbursement claims for warnings related to EU GDPR infringements by companies with a certain number of employees. Moreover, German legislators are drafting measures to prevent abusive legal actions for excessive warning letters, excluding the relevant Section 3a UWG

 © 2024 PRIVACY LAWS & BUSINESS

from EU GDPR infringements.[6]

Representative Actions – Background: The emergence of competition law in addressing privacy infringements has led to a new trend in enforcement. EU law allows for representative actions, enabling consumers to collectively claim injunctive reliefs or seek damages for data protection infringements.[7]

ECJ decision on (non-material) damages: However, the possibility of obtaining remedies through representative actions still remains unclear in privacy litigation.[8] The decisions of the ECJ suggest that the assertion of (non-material) damages pursuant to Art. 82 EU GDPR may not be suitable for representative actions. According to the ECJ, a claimant must demonstrate non-material damages on a case-by-case basis taking into account the individual consequences of the data protection infringement.[9] In contrast, representative actions require a certain uniformity in claims and assessable damages. This appears to conflict with the requirements regarding the assertion of immaterial damages.[10]

Despite these challenges, representative actions are gaining momentum in Germany, as evidenced by emerging cases like the representative action by North Rhine-Westphalia's consumer advice center against a telecommunications provider for an alleged unlawful data transfer to a scoring agency.[11]

Consequences for infringements of the German EU GDPR: The relevance of these cases moving forward will depend on the outcome of cases still pending, as well as any further clarification by the ECJ to resolve contradictions in the applicability for remedies in representative actions. In any event, controllers should be aware that data privacy infringements may result not only in individual claims but may also pose a risk of triggering representative actions.

Eventually, the opening of data protection infringements for privacy litigation may lead to an increase of efforts for achieving compliance with the EU GDPR.

BGH Decision of 12 March 2024 on covert video

Background: A recurring question that had previously been addressed in proceedings before the Federal Labour Court (BAG)[12] has now also been addressed before the BGH[13]. The question concerns the inadmissibility of covert video recording evidence in court proceedings. In the underlying case, the landlord of apartments, a state-owned housing company, hired a detective agency to find out whether the tenants were subletting the apartment without authorisation. The agency used hidden cameras to observe the tenants in the entrance area of the private apartment.

BGH decision on covert video recordings: In this context, the BGH had to clarify whether the recordings could be used as evidence or whether this is prohibited because of an infringement of the EU GDPR. According to the BGH, a court will have to weigh all factors relevant in a case in making its decision as to whether the use of covertly obtained data for evidence is compatible with the general personality right of tenants.

Consequences for infringements of the German EU GDPR: This relates to the general issues that the requirements of the EU GDPR are often not sufficiently taken into account in the context of covert video recordings, and that the knowledge gained from these recordings can also lead to bans on the use of such evidence.

Infringements of the EU GDPR through unlawful video observations regularly constitute the basis for various decisions of Data Protection Authorities, whether due to infringements by public authorities or private entities.

Conclusion

The increase of EU GDPR enforcement will likely continue, and this applies to both enforcement by Data Protection Authorities and through civil law claims. The decisions highlighted here illustrate the impact of the EJC and the BGH on this trend.

As a consequence, controllers will need to prioritise EU GDPR compliance to effectively navigate through the complexities of this evolving legal environment. Effective and robust compliance and thorough documentation are essential to mitigate the risk of enforcement fines and to provide a solid defence against unjustified claims.

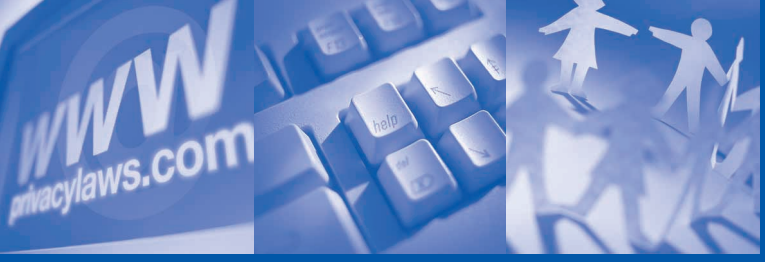
As the enforcement landscape continues to evolve, controllers must stay vigilant and proactive in adapting their practices to meet the stringent requirements set forth by the ECJ, the BGH and national laws.

AUTHORS

Dr Lars Lensdorf and Dr Moritz Hüsch are Partners at Covington Germany and Evangelos Karalias is an Associate in the same office.
Emails: llensdorf@cov.com
mhuesch@cov.com
ekaralias@cov.com

REFERENCES

1 ECJ, Judgment of 5 December 2023, C-807/21.
2 Ashkar/Schröder, BB 2023, 2956,; Wybitul/Brink ZD 2024, 137, p. 138.
3 BGH, Decision of 12 January 2023, I ZR 223/19
4 ECJ, Judgment of 04 October 2024, C-21/23.
5 See Ashkar, BB 2024, 2508, p. 2515.
6 BT-Drucksache 20/11879 available in German: dip.bundestag.de/vorgang/gesetz-zum-abbau-datenschutzrechtlichen-gold-platings-im-wettbewerbsrecht/311324; Voßberg, GRUR-Prax 2024, p. 690.
7 EU-Directive 2020/1828; transposed into a National Consumer Rights Enforcement Act; (*Verbraucherrechtedurchsetzungsgesetz* – VDuG), entered into force on 13 October 2023.
8 Schultze-Moderow/Hamann, BB 2024, 1539, p. 1544.
9 ECJ, Judgement of 04 May 2023, C-300/21; ECJ, Judgement of 14 December 2023, C-340/21; ECJ, Judgement of 11 April 2024, C-741/21.
10 Schultze-Moderow/Hamann, BB 2024, 1539, p. 1547.
11 Pending since May 2022; www.bundesjustizamt.de/DE/Themen/Verbraucherrechte/VerbandsklageregisterMusterfeststellungsklagenregister/Verbandsklagenregister/Unterlassungsklagen/Klagen/2024/050/UKlag_50_2024_node.html#doc112824bodyText4
12 BAG, Decision of 20 October 2016, 2 AZR 395/15.
13 BGH, Decision of 12 March 2024, VI ZR 1370/20.



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The Digital Markets Act – data portability re-booted?

Claudia Berg and **Tom Reynolds** of the UK Information Commissioner's Office[1] argue that data portability is enhanced by the EU Digital Markets Act, and explore its interactions with the GDPR.

Given the critical role of data in the digital economy, data portability is often mentioned as part of a digital competition policy reform agenda. Recently, it has gained traction under Regulation (EU) 2022/1925[2], commonly referred to as the Digital Markets Act (DMA). Data portability is not a new concept, however, and many will be familiar with the data portability rights granted to individuals under Article

Continued on p.3

Chile enacts new Data Protection Law

The new law, inspired by the GDPR, establishes a Data Protection Authority. **Natalia Jara Fuentealba** of Data Driven Legal explains.

After several unsuccessful attempts to amend Chile's current Law No. 19.628, entitled "Protection of Private Life" (the Data Protection Law), Congress and the Constitutional Court have approved the consolidated text of Bill No. 11144-07, merged with Bill No. 11092-07 (the Bill). The Bill was approved by the Constitutional Court on 14 November and will soon be published in the Official Gazette.

Continued on p.5

Data opportunities in Ireland

6 February 2025, McCann FitzGerald, Dublin

This one-day *PL&B* conference, in association with McCann FitzGerald, will cover a range of regulatory issues which organisations should consider when expanding their data use.

Keynote address: **Data opportunities in Ireland within the law**
Dr Des Hogan, Data Protection Commissioner, Ireland

www.privacylaws.com/ireland2025

Issue 192 **DECEMBER 2024**

PL&B Services: Conferences • Roundtables • Content Writing
Recruitment • Consulting • Training • Compliance Audits • Research • Reports

INTERNATIONAL report

ISSUE NO 192 DECEMBER 2024

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Natalia Jara Fuentealba
Data Driven Legal, UK

Claudia Berg and Tom Reynolds
Information Commissioner's Office, UK

Marc Schlegel
Federal Data Protection Authority, Germany

Katharina A. Weimer and Celin Fischer
Fieldfisher, Germany

Lars Lensdorf, Moritz Hüsch and Evangelos Karalias
Covington & Burling, Germany

Amit Ashkenazi
Law and Technology Expert, Israel

Graham Greenleaf
Independent Scholar, Australia

Abigail Dubiniecki
Independent Consultant, Canada

Nicholas Shepherd and Daniel Cooper
Covington & Burling, US and Belgium

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X
Copyright: No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.
© 2024 Privacy Laws & Business

comment

Data protection is a constantly evolving concept

When attending the Global Privacy Assembly (GPA) in Jersey this October (p.8), it was evident that while data protection principles are widely recognised, the Data Privacy Authorities' priorities differ depending on their jurisdiction's privacy maturity. For example, we heard that in Africa, 65% of the jurisdictions now have a DP law, but enforcement often needs to be stepped up. AI is of increasing importance but so are mobile payments, for example, and the privacy issues they bring.

In the EU, DPAs are still grappling with interpretations of the GDPR, and now also the interaction with the new EU digital legislation, such as the Digital Markets Act (see p.1). In Germany, there is some new case law that tries to clarify enforcement requirements and competition claims (see p.20).

Next year, the GPA goes to South Korea. It will be interesting to see which topics will be chosen – we have seen many new privacy laws emerge from the region in the last few years. This edition includes an analysis of Vietnam's new draft law which could be in force in 2026 (p.22), and Chile's new law which is about to be published in the Official Gazette (p.1).

As we start preparing for our own International Conference in Cambridge (7-9 July 2025), we are paying attention to the concept of human-centric data protection. After all, the laws are there to protect individuals who need to understand what rights they have and how to use them. Clear communication from DPAs and organisations is a key component. Nowhere is this needed more than in the field of AI as most people struggle to understand how their data is being used behind the scenes. Fulfilling the right to be forgotten in AI chatbots is easier said than done (p.29).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked in advance of the free-place deadline. Excludes the Annual Conference. More than one place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> "Given the rate of change in law, regulation and business practice, it is essential to have concise and up to date information. *PL&B* is always relevant and continues to offer great value."
>
> **Adam Green, Chief Risk Officer, Equiniti**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the UK GDPR and related regulatory changes, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.