It's just not fair! The ambiguity of GDPR fairness principle

Paul Maynard and **Madelaine Harrington** of Covington assess the interpretation of this principle by the EDPB and Member State DPAs.

One of the foundational EU GDPR principles, set out in Article 5(1)(a), is that personal data must be processed "lawfully, fairly and in a transparent manner in relation to the data subject". Article 6 sets out concrete circumstances in which processing will be "lawful", and Articles 12-14 provide further specific requirements for ensuring that processing is "transparent". But the text of the GDPR—like the Data Protection Directive before it—contains very little additional guidance on when processing will be "fair" i.e., when processing will have "the quality of treating people equally or in a way that is reasonable", as the Oxford English Dictionary defines fairness.

In the absence of legislative guidance, and of a definitive interpretation from the Court of Justice of the European Union (CJEU), guidance and enforcement decisions from the European Data Protection Board (EDPB) and Member State Data Protection Authorities (DPAs) have begun to fill this gap. However, at present, there is some tension between different strands of EDPB and DPA guidance and enforcement. On the one hand, DPAs appear to believe that fairness is a general principle that is independent of other GDPR obligations. On the other hand, however, there is EDPB guidance stating that controllers must comply with specific, positive obligations to process data "fairly", many of which replicate other compliance obligations, suggesting that in the EDPB's view, non-compliance with those other obligations would also contravene the fairness principle.

This article first explains how the GDPR itself, and other relevant EU legislation, refers to "fairness", and then describes how the EDPB and DPAs have articulated the requirements for compliance with this principle in guidance and enforcement decisions.

Fairness in the text of the GDPR

The GDPR did not create the fairness principle. Article 6 of the 1995 Data Protection Directive (the DPD, which the GDPR replaced) required personal data to be "processed fairly and lawfully". Similarly, Article 8 of the EU Charter of Fundamental Rights (Charter)—which sets out the right to protection of personal data—states that personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law".

Recitals 39 and 60 GDPR state that providing information to data subjects is one aspect of fair processing. In addition, Recital 71 of the GDPR, in discussing the steps that controllers should take to ensure that profiling complies with the GDPR, indicates that "to ensure fair and transparent processing in respect of the data subject", controllers should take steps to minimize potential risks to data subjects, including by: ""us[ing] appropriate mathematical or statistical procedures for the profiling, implement[ing] technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secur[ing] personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect".

This Recital suggests that ensuring fairness is a matter of implementing appropriate technical and organizational measures to minimize potential risks to data subjects. As a general matter, this is already required by Article 25 GDPR, which requires controllers to, by design, implement measures that "integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects". More specifically, all of the suggested measures in this Recital are also required by other GDPR requirements:

- The accuracy principle in Article 5(1)(d) and Article 16 require controllers to ensure that personal data is accurate, and to rectify inaccurate data;
- The integrity and confidentiality principle in Article 5(1)(f) and Article 32 require controllers to take steps to ensure the security of personal data; and
- The lawfulness principle in Article 5(1)(a) and Article 9 require controllers to have a valid basis for processing special category data, which are designed to prevent discrimination.

The GDPR does not make any further references to fairness. On a plain reading of these requirements—and of the dictionary definition of fairness—one interpretation is that it is a general principle that generally requires controllers and processors to prevent inequitable, discriminatory, or unreasonable outcomes arising from the processing of personal data. On that basis, non-compliance with other obligations under the GDPR would not necessarily rise to the level of an infringement of the fairness principle unless they meet this threshold.

Regulatory interpretations

Despite the lack of specificity in the GDPR, the EDPB and national DPAs have begun to interpret the fairness principle in a way that requires organizations to take specific compliance steps to comply.

The EDPB has stated in its

guidelines on deceptive dark patterns in social media platform interfaces that fairness serves an "umbrella function" and requires that "personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject"[1]. Positioning fairness as an "umbrella function" suggests that—in line with the interpretation above—it does not impose specific, positive obligations, but instead requires controllers and processors to, as a general matter, ensure their processing is not discriminatory, detrimental, unexpected, or misleading.

In its guidelines on data protection by design and by default,[2] the EDPB also appears to take the view that the fairness principle requires controllers to take specific steps to comply with it (suggesting it is not simply a general requirement to prevent detrimental, discriminatory etc. behavior). Some of the specific steps the EDPB suggests indicate that non-compliance with other GDPR obligations could automatically lead to an infringement of the fairness principle.

Specifically, in those guidelines, the EDPB sets out a list of 14 "elements" of fairness that controllers will need to consider to comply with the principle (para. 70). Some of these elements are closely related to compliance with other GDPR obligations, for example:

- "Interaction", which the EDPB states means that "data subjects must be able to communicate and exercise their rights". Honoring data subjects' rights under Articles 12-22 may satisfy this requirement;
- "Truthful", which means that controllers "must make available information about how they process personal data, they should act as they declare they will and not mislead the data subjects". Complying with transparency requirements in Articles 12-14 may be sufficient here; and
- "Human intervention", which appears to require controllers to, in effect, ensure compliance with Article 22 GDPR where they carry out automated decision-making with a legal or similarly significant effect.

Other elements of fairness listed in these guidelines suggest that compliance with this principle requires controllers to take specific steps not otherwise mentioned in the GDPR. For example:

- "Autonomy", which requires data subjects to have "the highest degree of autonomy possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing". While not entirely clear, the reference to "the highest degree of autonomy possible" could be read to require controllers to rely on consent as their legal basis unless doing so is not "possible", as that legal basis may give data subjects the greatest autonomy;
- "Respect rights", which requires controllers to "respect the fundamental rights of data subjects and implement appropriate measures and safeguards and not impinge on those rights unless expressly justified by law". This suggests that the GDPR—whose objective is to ensure a high level of protection for individuals' rights to privacy and the protection of their personal data (Article 1 and CJEU, UZ v Germany, C-60/22, para. 641)—may also impose a positive obligation on controllers to respect all other fundamental rights in their processing of personal data;
- "Ethical", which indicates that controllers should "see the processing's wider impact on individuals' rights and dignity".

In practice, DPAs' decisions concluding that organizations have infringed the fairness principle have mostly arisen in circumstances where a controller has infringed other obligations, and the DPA took the view that infringement of other obligations was sufficiently serious to mean the processing in question was unfair. This was the case in each of the EDPB's binding decisions regarding Facebook, Instagram, WhatsApp and TikTok (Binding Decisions 3/2022, 4/2022, 5/2022, and 2/2023). Belgium's DPA also held that IAB Europe had infringed the fairness principle as a result of its processing of personal data in consent strings obtained through its Transparency and Consent Framework, but only in connection with its primary conclusion that IAB Europe had infringed the lawfulness principle. In fact, the Belgian DPA did not discuss IAB Europe's compliance with the fairness principle in any detail; instead, it focussed on lawfulness before ultimately determining that there had also been an infringement of the fairness principle.[3]

Conclusions

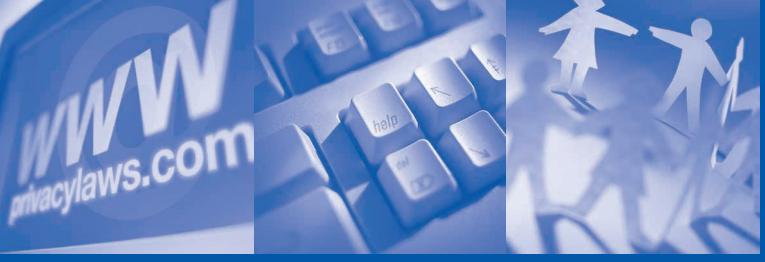
Perhaps due to the very limited guidance on the meaning of fairness within the text of the GDPR, the EDPB and the DPAs have begun to fill that gap. Their view in certain decisions, is that fairness is a distinct principle from other obligations. However, requiring organizations to take specific positive steps to comply with the fairness principle seems to run counter to the idea that fairness is a broad principle intended to prevent inequitable and discriminatory processing of data generally. Given this tension, it seems likely that the CJEU will ultimately have to give their judgment on how organizations and DPAs should understand fairness.

AUTHORS

Paul Maynard is Special Counsel, and Madelaine Harrington an Associate at Covington UK.
Emails: pmaynard@cov.com
mjharrington@cov.com

REFERENCES

1 'Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them' p.4 www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en
2 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' version 2.0 adopted on 20 October 2020, EDPB. www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
3 www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022.pdf



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

EU AI Act: Will there be Brussels effects?

The EU aims to establish a world-class AI hub. Will companies and legislators globally follow its regulatory lead? Independent scholar **Graham Greenleaf** assesses the situation.

The expression "the Brussels effect" is often used rather loosely to refer to any or all of the ways by which EU legislative standards come to be adopted in the practices of companies (or governments) in countries outside the EU ("third party countries"). These include both those required by law (*de jure*) and those adopted for other reasons (*de facto*), distinctions sometimes recognised.[1]

Continued on p.3

Germany debates changes to its federal data protection law

Julia Garbaciok and **Katharina Weimer** of Fieldfisher assess the upcoming changes to the German Federal Data Protection Act and their current status.

As data protection enforcement is spread across 18 different authorities in Germany, there have been calls for many years for simplification and harmonization regarding the application of the General Data Protection Regulation's (GDPR) requirements, especially to ensure a more innovation-friendly regime. According to a survey conducted by the digital industry association Bitkom[1], 65% of companies see the

Continued on p.7

Issue 190 **AUGUST 2024**

COMMENT

2 - Enforcement phase begins for EU digital laws

NEWS

10- Training of AI models
13 - GDPR: Much Ado About Nothing
18 - AI and privacy
22 - Online tracking: A post-cookie future?
30 - Will the EU streamline its data laws?

ANALYSIS

1 - EU AI Act: New Brussels effects?
15 - How decentralized social networks affect privacy
20 - Ambiguity 'fairness' in EU GDPR
24 - Personal data on the balance sheet

LEGISLATION

1 - Germany debates changes to its federal data protection law

MANAGEMENT

26 - Events Diary
27 - Certifications: A win-win-win?

NEWS IN BRIEF

12 - European DPAs act on Meta's AI training model
12 - Nordic DPAs stress children's privacy and AI
14 - OECD report on AI and privacy
14 - EDPS AI and personal data guidelines
14 - Latin American SCCs guide
17 - New AI research centre begins work
17 - EDPS celebrates 20 years
19 - EU AI Board meets for first time
26 - EDPB website auditing tool
29 - Pay or consent: Meta challenged
29 LinkedIn limits ad targeting

INTERNATIONAL report

ISSUE NO 190 AUGUST 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
Julia Garbaciok and Katharina Weimer
Fieldfisher, Germany

Paul Maynard and Madelaine Harrington
Covington, UK

Dr John Selby
Privcore, Australia

Asher Dresner
PL&B Correspondent

Poojan Bulani
University College London, UK

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

comment

Enforcement phase begins for EU digital laws

For some years, we have seen much GDPR enforcement both at the national and EU level, although some countries are more active than others. The EU's new digital package means that there are now a multitude of digital laws to enforce, and ensure that they operate in the intended way with the GDPR which is the underlying regulation.

Recently, there have been interesting developments in this field. The ever-so-active noyb made complaints about Meta's AI training practices to 11 DPAs whose intervention put a stop to Meta's plans for now (p.12), and the EU Commission is looking into applying the Digital Markets Act in the area of pay or consent (p.22).

Civil society is playing an increasingly important role – consumer organisations have also challenged Meta over Pay or Consent (p.29). EDRi's action on LinkedIn's targeting of adverts based on sensitive personal data has already been successful (p.29).

In May, the European Commission decided to open infringement procedures by sending a letter of formal notice to 18 Member States that did not designate the responsible authorities to implement the Data Governance Act which facilitates data sharing across sectors and EU countries. Authorities also need to be appointed in Member States, in quite a short timescale, to become responsible for AI as per the EU AI Act. In some countries, the existing data protection supervisors may become AI authorities but this is not necessarily the case everywhere (p.18).

The EU AI Act was published in the EU Official Journal on 12 July 2024 and will be in force from 1 August. Most of its provisions will become applicable from 2 August 2026. This world-first Act may influence AI governance globally in many different ways – read analysis by Graham Greenleaf on p.1.

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 at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> *PL&B* reports are an invaluable resource to anyone working in the data privacy, e-commerce or digital marketing fields. Unlike many news feeds or updater services, each report provides rare depth of commentary and insight into the latest developments.
>
> **Rafi Azim-Khan, Partner – Head of Digital Law, Crowell & Moring**

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.