



**ILGSPD Publication Series
No 6/25: Working Paper**

*The Legal Issues Surrounding
Freely Given Consent
Raised by Pay-or-Okay
Models under the General
Data Protection Regulation*

Chloe Young
June 2025



ERASMUS MUNDUS JOINT MASTER

**International Law
of Global Security,
Peace and Development**



Erasmus Mundus Joint Master in International Law of Global Security, Peace and Development

International Law of Global Security, Peace and Development (ILGSPD) is a multidisciplinary Master's degree delivered collaboratively by an international consortium composed of six Higher Education institutions: University of Glasgow, Institut Barcelona d'Estudis Internacionals, University of Tartu, Leuphana University of Luneburg, Radboud University, and Université libre de Bruxelles. It is recognised and funded by the European Commission as an Erasmus Mundus Joint Master Degree (EMJMD). The programme provides the next generation of lawyers and policy makers with expert knowledge required to respond to pressing challenges of global security, peace and development and trains tomorrow's leaders to navigate the political context of international law.

ILGSPD Publication Series

ILGSPD Publication Series aims to showcase the work developed by the programme's postgraduate students, in the form of a dissertation, working paper, or policy brief. Publications address themes of global security, peace and development, broadly understood, through the lens of international law, international relations, and/or sustainability.

Coordinating Institution:
University of Glasgow
University Avenue
Glasgow G12 8QQ
Scotland, United Kingdom
E-mail: ilgspd@glasgow.ac.uk
www.globalsecuritylaw-erasmusmundus.eu

The views, information and opinions expressed in this publication are the author's own. The ILGSPD Consortium, or the University of Glasgow, is not responsible for the accuracy of the information.



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of Contents

Introduction	1
1. Legal Background	5
1.1. The EU Data Protection Legal Framework	5
1.1.1. EU Primary Law	5
1.1.2. EU Secondary Law	6
1.1.3. The 1995 Directive versus the GDPR	7
1.2. Pre-GDPR Case Law and Opinions on Consent	11
1.2.1. ECJ Case Law	11
1.2.2. Action Against Google	13
1.2.3. Action Against Meta	14
1.3. European Data Protection Supervisor Opinions	16
1.4. Meta's Previous Legal Bases for Personal Data Processing	16
1.4.1. Inapplicable Legal Bases	16
1.4.2. The Consent Model (2004-2018) and Contract Model (2018-2023)	17
1.4.3. The Legitimate Interests Model (July-December 2023)	19
2. Legal Analysis of Pay-or-Okay Models Under the GDPR	21
2.1. The Board's Decision on Meta's Pay-or-Okay Model	21
2.2. Valid Consent under the GDPR	23
2.3. The Four Considerations for Freely Given Consent	25
2.3.1. Imbalance of Power	25
2.3.2. Conditionality	28
2.3.3. Detriment	34
2.3.4. Granularity	38
2.4. Recommendations on Alternatives to Behavioural Advertising	41
Conclusion	41
Annex	47

THE LEGAL ISSUES SURROUNDING FREELY GIVEN CONSENT RAISED BY PAY-OR-OKAY MODELS UNDER THE GENERAL DATA PROTECTION REGULATION

*Chloe Young**

Introduction

In November 2023, Meta (formerly known as Facebook) implemented a subscription model in the European Union (EU), Switzerland, Iceland, Norway, and Liechtenstein for Facebook and Instagram users over the age of eighteen in an attempt to comply with the General Data Protection Regulation (GDPR).¹ As the “toughest privacy and security law in the world,”² the GDPR entered into force in 2016 and became enforceable in 2018. Meta’s pay-or-okay model asks users to pay a monthly fee³ or consent to behavioural targeted advertising to access Facebook and Instagram services. Behavioural targeted advertising involves monitoring a user’s browsing habits and processing personal data to customize and distribute advertisements.⁴ Personal data is defined as “information relating to an identified or identifiable natural person.”⁵ This includes information on someone’s identity or characteristics including age, location, gender, buying patterns, and language preferences. Additionally, personal data processing is defined as “any operation...such as collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination restriction, and erasure or destruction”⁶ of personal data. Companies like Meta are increasingly collecting and processing personal data for behavioural advertising to boost click-through rates and revenue, finding it more effective than non-targeted

* Chloe Young is a graduate of the Erasmus Mundus Joint Master’s Degree in International Law of Global Security, Peace and Development, specialising in international law and cyberspace. Chloe holds a Bachelor of Arts in Politics and Chinese from Whitman College in Washington. This working paper is based on her Master’s dissertation. Contact email: youngchloemarie@gmail.com.

¹ EU General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) OJ 2016 L 119/1.

² GDPR.EU, ‘Complete Guide to GDPR Compliance’ (*Proton Technologies AG*, 2020) < <https://gdpr.eu> > accessed 10 March 2024.

³ Meta initially charged €9.99 for web users and €12.99 for app users but offered to reduce the price to €5.99 in March 2024.

⁴ Meta Business Help Center, “About Reaching New Audiences’ (*Meta*, 2024) < https://www.facebook.com/business/help/717368264947302?id=176276233019487&helpref=page_content > accessed 10 March 2024.

⁵ GDPR, art. 4(1).

⁶ *ibid* art. 4(2).

advertisements.⁷ As personal data becomes the new currency of the digital age, advertisers are increasingly using online platforms like Facebook and Instagram to reach potential customers.

In response to Meta's pay-or-okay model, 28 non-governmental organisations (NGOs) across Europe filed complaints to Data Protection Agencies (DPAs) urging the European Data Protection Board (hereinafter the Board) to condemn the company for violating the GDPR.⁸ DPAs are responsible for enforcing data protection laws and the GDPR at the national level whereas the Board ensures the GDPR is applied consistently throughout Europe.⁹ These NGOs argue paying a privacy fee violates the GDPR's requirement for freely given consent and makes the right to privacy a luxury accessible only to the wealthy.¹⁰ Conversely, some European companies¹¹ argue pay-or-okay models uphold privacy rights and exemplify the freedom to conduct business outlined in Article 16 of the Charter of Fundamental Rights of the European Union (hereinafter the Charter).¹² As online platforms of all sizes across Europe embrace pay-or-okay models, it is essential to analyse Meta's model as an example given the company's influence on industry standards. If Meta's pay-or-okay model is permitted under EU law, these models will likely continue to proliferate across "any industry sector with an ability to monetize personal data via consent."¹³

This working paper's objective is to address the legal uncertainties surrounding pay-or-okay models in the EU. More specifically, this paper asks: What legal issues surrounding freely given consent do pay-or-okay models raise under the GDPR? This paper focuses on the GDPR's conception of freely given consent because pay-or-okay models employ the legal basis for personal data processing found in Article 6(1)(a) GDPR which concerns data subject

⁷ Frederik Zuiderveen Borgesius and others, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' (15 March 2018) <<https://papers.ssrn.com/abstract=3141290>> accessed 7 May 2024, p. 4.

⁸ NOYB- European Center for Digital Rights, '28 NGOs Urge EU DPAs to Reject "Pay or Okay" on Meta' (*Forced Consent & Consent Bypass*, 16 February 2024) <<https://noyb.eu/en/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta>> accessed 7 May 2024.

⁹ European Data Protection Board, 'About the European Data Protection Board' (*EDPB*, 2024) <https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en> accessed 10 March 2024.

¹⁰ NOYB- European Center for Digital Rights, 'Complaint Under Article 77(1) GDPR' (*NOYB*, 28 November 2023) <<https://noyb.eu/sites/default/files/2023-11/Complaint%20-%20Meta%20Pay%20or%20Okay%20-%20REDACTED.pdf>> accessed 10 March 2024.

¹¹ Interactive Advertising Bureau (IAB) Europe, IAB Italia, IAB Spain, and Alliance Digitale, 'Opinion on 'Pay or Okay' Models Requested from the EDPB by the Norway Protection Authority, Hamburg Supervisory Authority, and the Netherlands Supervisory Authority' (19 March 2024) <<https://iabeurope.eu/wp-content/uploads/20240319-Letter-to-EDPB-upcoming-opinion-and-guidelines-on-the-consent-or-pay-model.pdf>> accessed 11 March 2024.

¹² The Charter of Fundamental Rights of the European Union (Charter) OJ 2010 C 83/389 art 16.

¹³ NOYB- European Center for Digital Rights, Letter to the EDPB: 'Pay or Okay' and the end of 'genuine and free' choice' (*NOYB*, 16 February 2024) https://noyb.eu/sites/default/files/2024-02/Pay-or-okay_edpb-letter_v2.pdf accessed 10 March 2024, p. 1.

consent. This research question is legally relevant because the GDPR outlines consent requirements but does not explain whether freely given consent can be obtained via a pay-or-okay model. Thus, analysing Meta's model as an example is important because it remains questionable whether user consent is freely given in such circumstances.¹⁴ For years, Meta has engaged in trial and error to find a suitable legal basis for personal data processing in the EU. If this process fails, European users could lose access to Meta services and the ability to connect with friends and family, engage in business, or receive news. Given these dire consequences, it is important to analyse the legal developments surrounding Meta's pay-or-okay model. Notably, in April 2024 the Board published a binding opinion addressing Meta's model. This opinion concluded that "in most cases it will not be possible for large online platforms to comply with the requirements for valid consent," but assessments needed to be made on a case-by-case basis.¹⁵ Given the Board's cautious approach and limited focus on large online platforms, this working paper examines the legality of pay-or-okay models more generally to address smaller online platforms falling outside the opinion's scope. This legal analysis is topical because Meta is expected to appeal the Board's decision,¹⁶ and the Board will issue a ruling on pay-or-okay models for smaller online platforms in the future.¹⁷

To answer the main research question, the following sub-questions will be addressed: What is the EU's legal framework for data protection and how have previous case law and decisions from the Article 29 Working Party (WP29),¹⁸ Board, and European Data Protection Supervisor interpreted freely given consent? What legal bases under Article 6 GDPR did Meta previously rely upon for personal data processing before implementing its pay-or-okay model? How can the four considerations for freely given consent be interpreted when analysing pay-or-okay models under the GDPR? Do legal possibilities exist for Meta to better meet the GDPR's consent requirements moving forward by replacing behavioural advertising with alternative advertising methods? Each sub-question will be addressed in a relevant section in the working paper.

In addition to these sub-questions, it is important to acknowledge research limitations and what will not be addressed. One research limitation is that some DPA verdicts, evaluations, and press releases required translation into English via online translation tools. For example, the German DPA's (DSK) evaluation of pay-or-okay models required translation from

¹⁴ GDPR, art. 4(1).

¹⁵ European Data Protection Board, 'Opinion 08/2028 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms' (17 April 2024) p. 3.

¹⁶ Meta Newsroom, 'How Meta Uses Legal Bases for Processing Ads in the EU' (*Meta*, 2023) <<https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/>> accessed 10 March 2024.

¹⁷ NOYB- European Center for Digital Rights, 'EDPB Opinion: Meta cannot rely on "Pay or Okay"' (*NOYB*, 17 April 2024) <<https://noyb.eu/en/statement-edpb-pay-or-okay-opinion>> accessed 17 May 2024.

¹⁸ The WP29 was an advisory body established by the Data Protection Directive which was later replaced by the European Data Protection Board in 2018 when the GDPR entered into force.

German,¹⁹ the Norwegian Privacy Appeals Board's (Personvernemnda) decision required translation from Norwegian,²⁰ and the Agencia Española de Protección de Datos' (AEPD) verdict required translation from Spanish.²¹ Considering a linguistic nuance in one language may not have an equivalent in another language, translated works may have slightly different meanings. This working paper will not address data transfers between the EU and the United States, or legal issues raised by pay-or-okay models under EU consumer law and competition law.

This working paper conducts qualitative research methodology by analysing EU primary law, EU secondary law, and non-binding legal sources and opinions. Online resources (including but not limited to scholarly articles, DPA decisions, and Board opinions) are referenced more often than books given the quickly evolving nature of the subject matter. This working paper also cites examples of national interpretations and implementations of freely given consent by DPAs but does not conduct a systematic comparative analysis of them across the EU. Section one employs legal dogmatics by analysing the current law in force (the GDPR) and its predecessor, the Data Protection Directive,²² to understand differences between both pieces of EU legislation. After all, the Court of Justice of the EU (hereinafter the CJEU) has found "the origins of a provision of EU law may provide information relevant to its interpretation."²³ Additionally, section one outlines EU primary law on data protection because the CJEU has found that "an EU act [like the GDPR] must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter."²⁴

Section two employs a grammatical-teleological interpretation of the four considerations for freely given consent under the GDPR. Given the CJEU's power to interpret EU law, the Court concluded this interpretation must be based on upholding the rule of law²⁵ and the spirit of EU treaties.²⁶ Following the Court's lead, this working paper considers "the interpretation of a provision of EU law [like the GDPR] requires that account be taken not only of its *wording*

¹⁹ The Committee of Independent German Federal and State Data Protection Supervisory Authorities (DSK), 'Bewertung von Pay-Abomodellen auf Websites' (DSK Privacy Conference, 22 March 2023).

²⁰ The Norwegian Privacy Appeals Board (Personvernemnda), 'Decision on Grindr's Disclosure of Personal Data Without Consent 20/02136-18' (27 September 2023).

²¹ Agencia Española de Protección de Datos (AEPD), 'Resolución de Procedimiento Sancionador (Numero Expediente: PS/00226/2020)' (2020).

²² *EU Directive 95/46*: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (The 1995 Directive) OJ 1995 L 281/31.

²³ *Bundesverband der Verbraucherzentralen Und Verbraucherbande-Verbraucherzentrale Bundesverbände eV v. Planet 49* (Case C-4673/17) [2019] ECLI:EU:C:2019:801 [48].

²⁴ *DB v. Commissione Nazionale per le Società e la Borsa (Consob)* (Case C-481/19) [2021] ECLI:EU:C:2021:84 [50]; *Ligue des droits humains ASBL v. Conseil des Ministres* (Case C-817/19) [2022] ECLI:EU:C:2022:491 [86].

²⁵ *Criminal Proceedings against E. and F.* (Case C-550/09) [2010] ECLI:EU:C:2010:382 [44].

²⁶ *Parti écologiste 'Les Verts' v. European Parliament* (Case 294/83) [1986] ECLI:EU:C:1986:166 [25].

and the objectives it pursues, but also of its context and the provisions of EU law as a whole.”²⁷ Grammatical interpretation analyses a legal provision based on its syntax and word choice to gauge its literal meaning.²⁸ Teleological interpretation focuses on understanding a legal provision “in view of the legislator’s original objectives.”²⁹ The Court refers to established case law and recitals of EU acts but does not consider the minutes or preparatory works of other EU institutions when interpreting a provision.³⁰ Therefore, Recital 10 of the GDPR proves helpful because it outlines the its objective to “ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union.”³¹

This working paper proceeds in two sections. Section one outlines the EU’s legal framework for data protection, examines the main differences between the Data Protection Directive (hereinafter the 1995 Directive) and the GDPR, analyses relevant pre-GDPR case law and opinions on freely given consent, and outlines Meta’s previous legal bases for personal data processing under Article 6 of the GDPR. Section two interprets the four considerations for freely given consent under the GDPR in the context of pay-or-okay models.³² These considerations include the imbalance of power between the controller and the data subject, conditionality, detriment, and granularity.³³ Additionally, section two recommends potential alternatives to behavioural advertising for online platforms to better meet the GDPR’s requirements for freely given consent. The summary reviews the research findings and suggests areas for future research.

1. Legal Background

1.1. The EU Data Protection Legal Framework

1.1.1. EU Primary Law

The EU’s legal framework for data protection stems from two sources of primary law: the Charter³⁴ and the Treaty on the Functioning of the EU (hereinafter the TFEU).³⁵ The Lisbon

²⁷ *Andy Wightman and Others v. Secretary of State for Exiting the European Union* (Case C-621/18) [2018] ECLI:EU:C:2018:999 [47]; *Bank Melli Iran v. Telekom Deutschland GmbH* (Case C-124/20) [2021] ECLI:EU:C:2021:1035 [43]; *WS v. Bundesrepublik Deutschland* (Case C-505/19) [2021] ECLI:EU:C:2021:376 [77] [emphasis added].

²⁸ Lina Kestemont, *Handbook on Legal Methodology: From Objective to Method* (Intersentia 2018) 22.

²⁹ *ibid* p. 28.

³⁰ *Quelle AG v. Bundesverband der Verbraucherzentralen und Verbraucherverbände* (Case C-404/06) [2018] ECLI:EU:C:2008:231 [32].

³¹ GDPR, recital 10.

³² *ibid* art. 4, 6 and 7.

³³ European Data Protection Board, ‘Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1’ (4 May 2020) p. 3.

³⁴ The Charter (n 12).

³⁵ Treaty on the Functioning of the European Union (TFEU) [2012] OJ C326.

Treaty³⁶ entered into force in 2009 and gave the Charter the same legal value as EU treaties, thus providing a stronger basis for data protection. Article 7 of the Charter codifies the right to privacy, family life, home, and communications to shield individuals from state interference.³⁷ While Article 7 of the Charter imposes a negative state obligation (i.e., the duty to not interfere), Article 8 recognises the protection of personal data as a distinct positive state obligation (i.e., the duty to act). More specifically, Article 8 of the Charter is a “proactive right”³⁸ that reassures individuals their personal data will only be processed if criteria in Articles 8(2) and 8(3) are met. These criteria include processing personal data fairly, specifically, and on a legally legitimate basis while allowing users to access and rectify their data.³⁹ In 2010, the European Court of Justice (hereinafter the ECJ) found that Articles 7 and 8 of the Charter could be limited based on Article 8(2) of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter the European Convention).⁴⁰ The Court explained the right to respect for private and family life could be lawfully limited in the interests of national security and public safety.⁴¹ In addition to the Charter, Article 16(1) of the TFEU (formerly Article 286 of the Treaty on the European Union)⁴² codifies the right to personal data protection.⁴³ In Article 16(2) of the TFEU, the EU Parliament and Council have the power to pass rules on personal data protection relating to the free movement of data in the internal market.⁴⁴ Together, the Charter and the TFEU constitute primary EU law and form the legal foundation for the Union’s data protection framework.⁴⁵

1.1.2. EU Secondary Law

In addition to primary law, the EU Parliament and Council have passed secondary law such as directives, regulations, decisions, opinions, and recommendations on data protection. Both the 1995 Directive and the GDPR came into force to further protect the processing of personal data as a fundamental right. Notably, the GDPR replaced the 1995 Directive and is

³⁶ Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 306.

³⁷ The Charter (n 12) art. 7.

³⁸ The European Data Protection Supervisor, ‘Preliminary Opinion- Privacy and competitiveness in the age of big data: The interplay between data protection, competition law, and consumer protection in the Digital Economy’ (March 2014) para 6.

³⁹ The Charter (n 12) art. 8.

⁴⁰ Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8(2).

⁴¹ *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* (Joined Cases C-92/09 and C-93/09) [2010] ECLI:EU:C:2010:662 [52].

⁴² Treaty on European Union (The Maastricht Treaty) [1992] OJ C 191/35 art 286.

⁴³ TFEU (n 35) art 16(1).

⁴⁴ *ibid* art 16(2).

⁴⁵ GDPR, recitals 1 and 2.

now the central piece of secondary legislation on data protection in the EU.⁴⁶ Another piece of secondary law under Article 16 of the TFEU includes Directive 2002/28/EC (the ePrivacy Directive) which particularises and complements the GDPR but does not discuss data subject consent.⁴⁷ The ePrivacy Directive initially entered into force in 2002 and was amended in 2009.⁴⁸ This Directive covers cookie usage, email marketing, and data minimisation (which entails only collecting, processing, and storing personal data that is necessary for specific and limited purposes).⁴⁹ Following the *lex specialis* principle, ePrivacy Directive provisions that are more specific than those in the GDPR take priority. However, the GDPR continues to govern any personal data processing not covered by the ePrivacy Directive. Although the ePrivacy Directive currently cites the 1995 Directive's definition of consent, this will soon be replaced by the new ePrivacy Regulation aligned with the GDPR.⁵⁰ In addition to the ePrivacy Directive, a third piece of relevant secondary law under Article 16 of the TFEU is Regulation (EC) No. 45/2001 which provides the legal framework for personal data protection by EU institutions and bodies.⁵¹ Overall, this working paper focuses on the GDPR when analysing Meta's pay-or-okay model as the Regulation constitutes the core instrument of secondary law on data protection in the EU.⁵²

1.1.3. The 1995 Directive versus the GDPR

Before comparing the 1995 Directive and the GDPR, it is worth discussing Europe's impetus for the 1995 Directive. After enduring both World Wars and extensive government surveillance, Europe prioritised developing information privacy rights for individuals.⁵³ Both the Universal Declaration of Human Rights (1948)⁵⁴ and the European Convention on

⁴⁶ European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (2018 edn, Imprimerie Centrale Luxembourg 2018) 31.

⁴⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) [2002] OJ L 201 art 1(1); GDPR, art 94(2).

⁴⁸ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (ePrivacy Directive) [2009] OJ L 337.

⁴⁹ European Data Protection Board 'Opinion 08/2028 on Valid Consent' (n 15) para 58.

⁵⁰ European Commission, 'Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (ePrivacy Regulation)' COM(2017) 10 final.

⁵¹ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L 008.

⁵² European Union Agency for Fundamental Rights and Council of Europe (n 46).

⁵³ Ruben De Bruin, 'A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence' [2022] SSRN Electronic Journal 128, 138.

⁵⁴ Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12.

Human Rights (1950)⁵⁵ included a right to privacy and respect for private life. Subsequently, the Swedish Data Protection Act⁵⁶ (1973) was the first data protection law to be introduced in Europe followed by the German Data Protection Act (1977)⁵⁷ and the French Data Protection Act (1978).⁵⁸ Notably, all three laws mentioned data subject consent for personal data processing. In 1980, the Organization for Economic Cooperation and Development (OECD) published the first internationally agreed upon guidelines declaring that personal data should be processed “with the knowledge or consent of the data subject.”⁵⁹ One year later, the Council of Europe published the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.⁶⁰ Three years after the Maastricht Treaty formally established the EU in 1992,⁶¹ the European Parliament and European Council passed the 1995 Directive to protect the free movement of data and data processing for European users.

The 1995 Directive drew inspiration from the 1980 OECD guidelines and was likely implemented given Member State reluctance to ratify the Council of Europe Convention.⁶² Given the World Wide Web’s infancy in the early 1990s, the 1995 Directive was ahead of its time for requiring all Member States to address data protection and protect individuals who capitalised on the increasing affordability and accessibility of online services. This foresight is exemplified by the subsequent founding of Google in 1998 and Facebook in 2004. Although the 1995 Directive was a legislative act outlining goals for Member States to achieve individually, the GDPR is a binding legislative regulation transposed in all Member States. As an EU regulation, the GDPR is directly applicable across the EU and requires Member States to align existing national laws with its provisions. However, Recital 10 of the GDPR allows Member States a margin of manoeuvre in specifying certain rules (such as the rules for processing special categories of personal data), while also reinforcing that the “consistent

⁵⁵ ECHR (n 40).

⁵⁶ Datalagen [The Swedish Data Act] SFS 1973:289.

⁵⁷ Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei Datenverarbeitung (Bundesdatenschutzgesetz- BDSG) [Act to protect against misuse of personal data in data processing (Federal Data Protection Act-BDSG) 1 January 1977 BGBl.

⁵⁸ Loi 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés [Law 78-17 of 6 January 1978 relating to data processing, files and freedoms] Légifrance [Official Gazette of France]

⁵⁹ The Organization for Economic Cooperation and Development (OECD), ‘Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data’ (OECD, 23 September 1980) para 7.

⁶⁰ Council of Europe, ‘Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data’ (28 January 1981) European Treaty Series No. 108.

⁶¹ The Maastricht Treaty (n 42).

⁶² Andrew Folks, ‘Meta’s new digs: A deep dive into practical considerations of consent’ (IAPP, 9 January 2024) < <https://iapp.org/news/a/metass-new-digs-a-deep-dive-into-practical-considerations-of-consent> > accessed 8 May 2024.

and homogenous application of the rules...with regard to the processing of personal data should be ensured throughout the Union.”⁶³

Beyond the transposition distinction between the 1995 Directive and the GDPR, it is important to highlight substantive differences between both pieces of legislation. According to the Board, the GDPR “represents a significant evolution of the EU data protection law”⁶⁴ compared to the 1995 Directive. Firstly, the GDPR imposes a stronger extraterritorial scope than the 1995 Directive and clearly states “this regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union.”⁶⁵ Conversely, the 1995 Directive’s extraterritoriality principle was more ambiguous and implicitly derived from Article 4(1)(a) which stated that “each member state shall apply the national provisions it adopts pursuant to this directive to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State.”⁶⁶ Recital 19 of the 1995 Directive broadly defined establishment as “the effective and real exercise of activity through stable arrangements”⁶⁷ including branches or subsidiaries of a main establishment. Although some scholars argue recitals have no legal value and only provide legitimate expectations,⁶⁸ the ECJ has referred to recitals to clarify the 1995 Directive’s territorial scope.⁶⁹ To clarify the definition of an establishment under Article 4(1)(a) of the 1995 Directive, the ECJ considered Google Spain to be a subsidiary establishment of Google Incorporated (headquartered in the US) and thus subject to Spain’s national data protection legislation.⁷⁰ This finding reinforced the 1995 Directive’s implied extraterritorial scope, which the GDPR later solidified.

Secondly, the GDPR defines personal data breach and increases fines for controllers who violate its provisions. Although the 1995 Directive did not provide a definition for personal data breach in Article 2, the GDPR defines it in Article 4(12) as a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”⁷¹ Additionally, the GDPR includes a provision on data breach notifications unlike the 1995 Directive.⁷² To

⁶³ GDPR, recital 10.

⁶⁴ European Data Protection Board, ‘Guidelines 03/2018 on the territorial scope of the GDPR (Article 3)- Version for public consultation’ (16 November 2018) p. 3.

⁶⁵ GDPR, art 3(2).

⁶⁶ The 1995 Directive, art 4(1)(a).

⁶⁷ *ibid* recital 19.

⁶⁸ Tadas Klimas and Jurate Vaiciukaite, ‘The Law of Recitals in European Community Legislation’ [2008] *ILSA Journal of International & Comparative Law* 1, 2.

⁶⁹ *Google LLC v. Commission nationale de l’informatique et des libertés (CNIL)* (Case 24/62) [1963] ECLI:EU:C:2019:772 [54], [55].

⁷⁰ *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C-131/12) [2014] ECLI:EU:C:2014:317.

⁷¹ GDPR, art 4(12).

⁷² *ibid* art 33.

determine fines against controllers, Article 83(5) of the GDPR stipulates that infringements of the principles of data processing and consent are subject to “administrative fines up to 20,000,000 euros...or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.”⁷³ This change is noteworthy as demonstrated by the French Data Protection Authority (CNIL) levying a 150,000 euro fine against Facebook in 2017⁷⁴ and then a 40 million euro fine against a technology company called Criteo in 2023.⁷⁵ Another example includes the DPC fining Meta 1.2 billion euros in 2023 following the Board’s binding decision on the illegality of Meta’s data transfers from the EU to the US.⁷⁶ Overall, technology companies now face greater financial consequences for violating the GDPR.

Thirdly, the GDPR implements stricter consent requirements than the 1995 Directive. According to the Board, the GDPR “raises the bar” by mandating additional consent requirements.⁷⁷ For example, the 1995 Directive explained that the data subject’s consent “shall mean any freely given, specific, and informed indication of his wishes.”⁷⁸ Going one step further, the GDPR mandates the “unambiguous indication of the data subject’s wishes by a statement or by a clear affirmative action.”⁷⁹ This suggests that presumed consent containing no references, silence, inactivity, or implied consent based on the data subjects’ actions (e.g., pre-ticked boxes) do not meet the GDPR’s consent standards.⁸⁰ These heightened standards help explain Meta’s switch from an implied consent model to a contract model in early 2018 in an attempt to obtain consent in a GDPR-compliant way. Additionally, unlike the 1995 Directive, the GDPR explicitly codifies the right to easily withdraw consent in Article 7(3).⁸¹ According to the WP29, the 1995 Directive implied a right to withdraw consent due to its overarching purpose to protect the data subject’s informational self-determination.⁸² However, the GDPR solidifies the right to withdrawal and provides stronger protections for data subjects by avoiding excessive ambiguity in interpretation by national courts.

⁷³ *ibid* art 83(5).

⁷⁴ Samuel Gibbs, ‘Facebook Facing Privacy Actions across Europe as France Fines Firm €150k’ *The Guardian* (16 May 2017) <<https://www.theguardian.com/technology/2017/may/16/facebook-facing-privacy-actions-across-europe-as-france-fines-firm-150k>> accessed 9 May 2024.

⁷⁵ Niall McCarthy, ‘The Biggest GDPR Fines of 2023: The Financial Penalties for Breaching the GDPR Can Be Staggering, Running into Hundreds of Millions of Euros’ (*EQS Group*, 16 January 2024) <<https://www.eqs.com/compliance-blog/biggest-gdpr-fines/>> accessed 9 May 2024.

⁷⁶ European Data Protection Board ‘Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65)’ (13 April 2023).

⁷⁷ European Data Protection Board ‘Guidelines 05/2020 on consent’ (n 33) para 167.

⁷⁸ The 1995 Directive, art 2(h).

⁷⁹ GDPR, art 4(11).

⁸⁰ European Data Protection Board ‘Guidelines 05/2020 on consent’ (n 33) para 79.

⁸¹ GDPR, art 7(3).

⁸² Article 29 Working Party (WP29), ‘Opinion 15/2011 on the definition of consent’ 01197/II/EN WP187 (13 July 2011) p. 9.

Finally, the GDPR requires more streamlined communication between controllers, processors, and data subjects in several ways compared to the 1995 Directive. For example, the GDPR requires the controller to inform the relevant supervisory authority of a personal data breach with undue delay.⁸³ This provision enhances communication between processors and controllers by requiring the former to describe the nature of the breach, outline possible consequences of the breach, and explain the corrective measures taken to address the situation.⁸⁴ Another difference is that the GDPR introduces required compliance mechanisms including record-keeping,⁸⁵ training for employees,⁸⁶ and data protection impact assessments.⁸⁷ These mechanisms reinforce the great value of personal data by ensuring controllers maintain accurate registries of all data processing responsibilities, instruct personnel on how to properly handle personal data, and understand the risks that new technologies pose to personal data processing. As technology advances and personal data becomes increasingly valuable, it is important to recognise how the GDPR clarifies and strengthens personal data protection.

1.2. Pre-GDPR Case Law and Opinions on Consent

1.2.1. ECJ Case Law

The ECJ has addressed consent requirements for personal data processing on several occasions. It is worth noting the CJEU is comprised of the ECJ and the General Court. The former addresses preliminary rulings for national courts and certain annulment and appeal processes, whereas the latter addresses actions for annulment for individuals, companies, and sometimes EU governments.⁸⁸ This working paper cites ECJ cases providing preliminary rulings for national courts on the GDPR's consent and data processing requirements. In 2011 and 2017, the ECJ concluded controllers must obtain the renewed consent of data subjects if they wish to use their personal data for an additional purpose not previously disclosed.⁸⁹ This decision underscored the importance of avoiding bundling, which is when controllers gain consent for one purpose but then misuse personal data for other purposes unrelated to the consent obtained. Additionally, the Court has concluded that the consent of data subjects cannot be coerced. For example, in 2013 the Court found that people applying for a passport cannot be deemed to have freely consented to having their fingerprints taken because "it is

⁸³ GDPR, art 33.

⁸⁴ *ibid* art 33(3).

⁸⁵ GDPR, art 30.

⁸⁶ *ibid* art 47(2)(n).

⁸⁷ *ibid* art 35.

⁸⁸ Directorate-General for Communication, 'Court of Justice of the European Union' (*Official Website of the European Union*) <https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en> accessed 11 May 2024.

⁸⁹ *Deutsche Telekom AG v Bundesrepublik Deutschland* (Case C-543/09) [2011] ECLI:EU:C:2011:279 [15]; *Tele2 (Netherlands) BV and Others v Autoriteit Consument en Markt (ACM)* (Case C-536/15) [2017] ECLI:EU:2017:214 [41].

essential for citizens of the Union to own a passport.”⁹⁰ The Court argued freely given consent cannot be forced and people wishing to travel outside the Union were “not free to object to the processing of their fingerprints.”⁹¹ Applying this finding to pay-or-okay models, one could argue this business model creates a forced situation whereby users cannot freely give consent if they cannot afford the subscription rate or would risk being disconnected from friends and family on the platform. Overall, the Court has found that consent must be acquired separately for different personal data processing usages and cannot be obtained via a forced situation.

Additionally, the Court clarified that DPAs across Europe can investigate Meta’s compliance with consent requirements under Article 28(3) of the 1995 Directive. In response to previous cases brought against it by Belgian and French authorities,⁹² Meta argued only the Irish DPC could investigate the company because its headquarters are based in Ireland.⁹³ It is important to acknowledge Ireland’s lenient approach to enforcing the GDPR likely influenced Meta’s decision to establish its European headquarters in Ireland in 2008.⁹⁴ This leniency is exemplified by the European Parliament calling upon the European Commission in 2021 to initiate infringement proceedings against Ireland due to the country’s lack of proper GDPR enforcement.⁹⁵ Meta’s argument was noteworthy because if the CJEU ruled that only the Irish DPC could investigate the company, it would undermine the enforceability of the 1995 Directive and result in lawsuits from European Member States being dismissed. However, the Court found the company’s subsidiary establishments in other Member States granted those Member States investigative powers to safeguard the fundamental privacy rights and freedoms of EU users.⁹⁶ More specifically, the Court interpreted Article 28(3) of the 1995 Directive to allow DPAs across the Union to investigate Meta’s actions and the actions of other online platforms with multiple establishments. The GDPR later codified this power by stating DPAs are competent when personal data processing affects “data subjects on its territory or [when] processing [is] carried out by a controller or processor not established in the Union [but targets] data subjects residing on its territory.”⁹⁷ This provision

⁹⁰ *Michael Schwarz v Stadt Bochum* (Case C-291/12) [2013] ECLI:EU:C:2013:670 [32].

⁹¹ *ibid.*

⁹² Samuel Gibbs, ‘Facebook “Tracks All Visitors, Breaching EU Law”’ *The Guardian* (31 March 2015) <<https://www.theguardian.com/technology/2015/mar/31/facebook-tracks-all-visitors-breaching-eu-law-report>> accessed 10 May 2024; Gibbs, ‘Facebook Facing Privacy Actions across Europe as France Fines Firm €150k’ (n 74).

⁹³ Gibbs, ‘Facebook Facing Privacy Actions across Europe as France Fines Firm €150k’ (n 74).

⁹⁴ Meta Newsroom, ‘Facebook to Establish International Headquarters in Dublin, Ireland’ (*Meta*, 2 October 2008) <<https://about.fb.com/news/2008/10/facebook-to-establish-international-headquarters-in-dublin-ireland/>> accessed 10 May 2024.

⁹⁵ European Parliament Resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020- Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (‘Schrems II’) Case C-311/18 (2020/2789(RSP)) [2021].

⁹⁶ *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (Case C-210/16) [2018] ECLI:EU:C:2018:388 para 64.

⁹⁷ GDPR, recital 122 and art 62.

gives DPAs similar investigative powers to the lead investigatory authority (in this case, the Irish DPC). In early 2024, the Court's finding allowed the Norwegian, Dutch, and German DPAs to ask the Board for a binding opinion on Meta's pay-or-okay model.⁹⁸

1.2.2. Action Against Google

Before analysing Meta's approach to data processing and consent, it is worth examining the conduct of other technology companies like Google for reference. After all, analysing European action against other large online platforms like Google can help better understand the legal context for Meta's pay-or-okay model. In 2010, a class-action suit filed in the US against Google's street view program prompted investigations in the EU on whether Google's program in Europe violated the 1995 Directive.⁹⁹ For context, Google sought to improve digital mapping on the Google Maps app by equipping cars with cameras to capture images of houses and roads.¹⁰⁰ After German authorities launched an investigation over Google's practices in 2010, the company agreed to blur images upon request.¹⁰¹ However, this opt-out option for refusing consent was unsatisfactory and the Hamburg Commissioner for Data Protection fined Google 145,000 euros for illegally collecting and storing people's personal data including images, Wi-Fi information, and more.¹⁰² Although Google admitted it was not its intention to store personal data,¹⁰³ the German authorities disregarded the company's intent and focused on the company's actions. Similar fines were levied by Belgian, French, Dutch, and Italian authorities against Google.¹⁰⁴ This strong reaction from European authorities revealed opt-out procedures for consent were inadequate under the 1995 Directive.

In 2012, Google changed its privacy policy and prompted the WP29 to send Google a letter regarding the company's continued lack of compliance with the 1995 Directive.¹⁰⁵ This document revealed Google both provided insufficient information to users on the "purpose and categories of data being processed" ¹⁰⁶ and combined data across services without an

⁹⁸ NOYB- European Center for Digital Rights, '28 NGOs Urge EU DPAs to Reject "Pay or Okay" on Meta' (n 8).

⁹⁹ *Google Inc. Street View Electronic Communications Litigation* [2011] (United States District Court, N.D. California, San Francisco Division) 794 F. Supp. 2d 1067.

¹⁰⁰ Tom Simonite, 'Google's New Street View Cameras Will Help Algorithms Index The Real World' *Wired* <<https://www.wired.com/story/googles-new-street-view-cameras-will-help-algorithms-index-the-real-world/>> accessed 10 May 2024.

¹⁰¹ Kimberly Houser and Gregory Voss, 'GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?' (2018) 25 *RICH. J.L. & Tech* 5, 26.

¹⁰² Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (The Hamburg Commissioner for Data Protection and Freedom of Information), 'Fine imposed upon Google: Ruling in the proceeding pursuant to Wifi scanning is legally binding' (22 April 2023).

¹⁰³ Brad Stone, 'Google Says It Inadvertently Collected Personal Data' (*Bits Blog*, 1273869892) <<https://archive.nytimes.com/bits.blogs.nytimes.com/2010/05/14/google-admits-to-snooping-on-personal-data/>> accessed 10 May 2024.

¹⁰⁴ Houser and Voss (n 101) para 34.

¹⁰⁵ Article 29 Working Party (WP29), 'Letter to Google' (16 October 2012).

¹⁰⁶ *ibid* p. 2.

appropriate legal ground for consent. The WP29 explained Google did not obtain unambiguous consent as defined in Article 7(a) of the 1995 Directive and the company's legitimate interests could not override fundamental privacy rights.¹⁰⁷ More specifically, the WP29 noted that "no contract justifies this large combination of data,"¹⁰⁸ and the company should have established limits to combining data.¹⁰⁹ To improve compliance, the WP29 suggested Google establish layered privacy notices and develop interactive presentations to ensure data subjects were properly informed before giving consent.¹¹⁰ It is worth noting the 1995 Directive and the GDPR outline the same legal grounds for data processing including obtaining user consent or demonstrating that data processing is necessary for fulfilling a contract, meeting legal obligations, safeguarding vital interests, executing tasks in the public interest, or pursuing the legitimate interests of the controller.¹¹¹

1.2.3. Action Against Meta

To contextualise personal data processing and consent disputes involving Meta, it is worth reviewing the company's privacy policies. In 2010, Meta published a privacy policy over 5,000 words long allowing people's personal data to be shared with third parties.¹¹² Although this policy offered an opt-out option to keep personal data private, selecting this option required users to select more than 50 privacy buttons and choose among 170 options.¹¹³ This complex process sparked criticism and prompted Meta to update its policy two years later. At this point, the Irish DPC released an audit report explaining Meta's business model of offering free services in exchange for collecting and processing personal data was legitimate under the 1995 Directive.¹¹⁴ However, this report acknowledged that the Irish DPC's conclusion remained a matter of judgment by the Irish Courts and the CJEU.¹¹⁵ Additionally, the report listed improvements for gathering consent to ensure users are fully aware that their personal data is used for targeted advertising.¹¹⁶ In 2014, Meta revised its data policy and introduced interactive guides to inform users about how their personal data is collected.¹¹⁷ Despite this promising development, Meta expressed its intention to "enhance

¹⁰⁷ *ibid.*

¹⁰⁸ *ibid.*

¹⁰⁹ *ibid.*

¹¹⁰ *ibid.*

¹¹¹ The 1995 Directive, art 7; GDPR, art 6.

¹¹² Meta Newsroom, 'Facebook Redesigns Privacy' (*Meta*, 26 May 2010) < <https://about.fb.com/news/2010/05/facebook-redesigns-privacy/> > accessed 9 May 2024.

¹¹³ Nick Bilton, 'Price of Facebook Privacy? Start Clicking' *The New York Times* (12 May 2010) < <https://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html> > accessed 10 May 2024.

¹¹⁴ The Office of the Data Protection Commissioner of Ireland, 'Report of Audit: Facebook Ireland Ltd' (21 December 2011) p. 4.

¹¹⁵ *ibid.*

¹¹⁶ *ibid.*

¹¹⁷ Erin Egan, 'Updating our Terms and Policies: Helping You Understand How Facebook Works and How to Control Your Information' (*Meta*, 13 November 2014) < <https://about.fb.com/news/2014/11/updating-our->

advertisements based on the sites users visit”¹¹⁸ and offered little information on how users could control their personal data. In 2016, Meta attempted to simplify the opt-out process by allowing users to control the extent of online tracking.¹¹⁹ Although some users refused online tracking for certain advertisements, Meta still collected and repurposed these people’s personal data for other uses without adequate consent.¹²⁰ This behaviour revealed Meta’s prioritisation of personal data collection over protecting online users.

Meta’s compliance with the 1995 Directive’s consent requirements was scrutinised on several occasions by DPAs and national courts. For example, in 2014, data protection authorities in several European countries – including France, Belgium, the Netherlands, Germany, and Spain – conducted a joint investigation into Meta’s personal data processing scheme. One year later, Belgium sued Meta for tracking and collecting personal data without explicit consent from users and non-users for advertising purposes.¹²¹ Similarly in 2017, France fined Meta 150,000 euros for collecting personal data for targeted advertising without the knowledge of users and non-users.¹²² As for national courts, in February 2018, the German regional court in Berlin concluded Facebook’s pre-checked consent boxes violated German competition and data protection law.¹²³ In its decision, the Court explained necessary and freely given consent requires the user to be “fully informed about the context, background, and the scope of his declaration.”¹²⁴ In response, Meta argued the user already gave implicit consent to the use of data during the registration process and this consent later applied to data processing.¹²⁵ However, the Court argued “implied consent through continued use”¹²⁶ was legally insufficient and Meta should have provided the user with knowledge of the default settings at the time of registration and clarified what the phrase “use for commercial, sponsored or related content”¹²⁷ covered. Overall, this German case clarified that, for consent to be considered freely given, users must be adequately informed, and the use of pre-checked boxes is not permissible.

[terms-and-policies-helping-you-understand-how-facebook-works-and-how-to-control-your-information/](#)> accessed 9 May 2024.

¹¹⁸ *ibid.*

¹¹⁹ Samuel Gibbs, ‘Facebook’s New Opt-out for Tracking Ads Is Not Enough, Says Privacy Expert’ *The Guardian* (18 September 2015) <<https://www.theguardian.com/technology/2015/sep/18/facebooks-opt-out-tracking-ads-not-enough-privacy-expert>> accessed 10 May 2024.

¹²⁰ *ibid.*

¹²¹ Gibbs, ‘Facebook “Tracks All Visitors, Breaching EU Law”’ (n 92).

¹²² Gibbs, ‘Facebook Facing Privacy Actions across Europe as France Fines Firm €150k’ (n 74).

¹²³ Landgericht Berlin [Berlin Regional Court] *The Federal Association of Consumer Centers and Consumer Associations- Federal Association of Consumer Organizations v Facebook Ireland Ltd.* (16 Jan 2018) No. 16 O 341/15.

¹²⁴ *ibid* p. 25.

¹²⁵ *ibid* p. 20.

¹²⁶ *ibid* p. 26.

¹²⁷ *ibid* p. 32.

1.3. European Data Protection Supervisor Opinions

Finally, European Data Protection Supervisor opinions can help clarify the requirements for freely given consent. The European Data Protection Supervisor (hereinafter the EDPS) was established in 2004 as an independent authority to ensure EU institutions respect privacy rights. In 2014, the EDPS published a preliminary opinion explaining many online platforms like Meta are perceived as free of charge but require payment in the form of personal data from users.¹²⁸ Given this reality, the EDPS reiterated that online platforms must obtain freely given, unambiguous, and informed consent before processing personal data under a specific, explicit, and legitimate legal basis.¹²⁹ In 2016, the EDPS published another opinion explaining “privacy is not a luxury, but a universal right and it should not only be available to those with the means to pay.”¹³⁰ This statement emerged from a discussion on establishing an EU values-based common area on the web to ensure freedom from tracking or interference. This guidance was also issued for EU institutions and bodies rather than technology companies like Meta. Nevertheless, this guidance reveals the EDPS’s high standards for personal data processing and the prioritisation of privacy rights over business schemes like pay-or-okay models.

1.4. Meta’s Previous Legal Bases for Personal Data Processing

1.4.1. Inapplicable Legal Bases

Before outlining the previous legal bases for personal data processing that Meta has unsuccessfully relied upon under Article 6 of the GDPR, it is worth addressing the three legal bases that Meta has not used and cannot reasonably use for behavioural advertising. Article 6 GDPR provides six legal bases for personal data processing: consent, contractual fulfilment, legal obligation, vital interest, public interest, and legitimate interest.¹³¹ However, Meta has not employed the legal obligation, public interest, or vital interest legal bases. For legal obligation, Article 6(1)(c) of the GDPR stipulates that personal data processing “shall be lawful only if and to the extent that the processing is necessary for compliance with a legal obligation to which the controller is subject.”¹³² To rely on this legal basis, Meta would need to prove that it processes personal data for behavioural advertising to comply with an EU law, Irish law, or law of another Member State. However, if Meta can “reasonably comply

¹²⁸ The European Data Protection Supervisor, ‘The European Data Protection Supervisor, ‘Preliminary Opinion- Privacy and competitiveness in the age of big data’ (n 38) p. 3.

¹²⁹ *ibid* para 14 and 74.

¹³⁰ The European Data Protection Supervisor, ‘Opinion 8/2016 EDPS Opinion on Coherent enforcement of fundamental rights in the age of big data’ (23 September 2016) p. 16.

¹³¹ GDPR, art 6(1).

¹³² *ibid* art 6(1)(c).

[with the law] without processing personal data,”¹³³ then this legal basis becomes inapplicable. Given the absence of laws compelling or requiring Meta to process personal data for behavioural advertising, it is prudent to consider the alternative legal basis grounded in public interest.

For public interest, Article 6(1)(e) of the GDPR allows personal data processing that “is necessary for the performance of a task carried out in the public interest of or in the exercise of official authority vested in the controller.”¹³⁴ Tasks that are carried out in the public interest generally include humanitarian, healthcare, religious, or electoral activities.¹³⁵ Behavioural advertising is not a task that is carried out in the public interest and Meta is not an official authority with public functions and powers,¹³⁶ so the public interest legal basis is inapplicable. Finally, the vital interest legal basis under Article 6(1)(d) of the GDPR allows “processing [that] is necessary in order to protect the vital interests of the data subject.”¹³⁷ Recital 46 GDPR defines vital interests as being “essential for the life of the data subject.”¹³⁸ Since personal data processing for behavioural advertising does not involve emergencies or life-and-death situations,¹³⁹ the vital interests legal basis is inapplicable.

1.4.2. The Consent Model (2004-2018) and Contract Model (2018-2023)

Meta’s pay-or-okay model marks the company’s fourth attempt in seven years to comply with the GDPR. Prior to 2018, Meta relied on implied consent to process personal data for behavioural advertising purposes. Under this first model, Meta argued individuals consented to targeted advertising when signing up for Meta services.¹⁴⁰ Meta continues employing this model in the US because the right to privacy follows a sectoral approach and is implied from the Fourth Amendment of the US Constitution,¹⁴¹ rather than explicitly codified like in EU treaties. However, anticipating the GDPR’s stricter consent requirements than those in the 1995 Directive, Meta pre-emptively switched to a contractual legal basis in early 2018 for personal data processing in Europe.¹⁴² Under this contractual model, European users were required either to accept the new Terms of Reference or to delete Instagram and Facebook

¹³³ The Data Protection Commission (DPC), ‘Guidance Note: Legal Bases for Processing Personal Data’ (DPC, December 2019) <<https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf>> accessed 23 May 2024 p. 14.

¹³⁴ GDPR, art 6(1)(e).

¹³⁵ DPC, ‘Guidance Note: Legal Bases for Processing Personal Data’ (n 133) p. 19.

¹³⁶ *ibid* p. 18.

¹³⁷ GDPR, art 6(1)(d).

¹³⁸ *ibid* recital 46.

¹³⁹ DPC, ‘Guidance Note: Legal Bases for Processing Personal Data’ (n 133) p. 17.

¹⁴⁰ Landgericht Berlin (n 123) p. 20.

¹⁴¹ U.S. Constitution [1787] amend. IV.

¹⁴² NOYB -European Center for Digital Rights, ‘Meta (Facebook, Instagram) Switching to ‘Legitimate Interest’ for Ads’ (NOYB, 30 March 2023) <<https://noyb.eu/en/meta-facebook-instagram-switching-legitimate-interest-ads>> accessed 10 March 2024.

accounts. Under this second model, Meta argued personal data processing was a contractual necessity for the delivery of social media services under Article 6(1)(b) of the GDPR.¹⁴³

Despite Meta's change, NOYB-European Center for Digital Rights filed a complaint against the company to the Belgian DPA on the first day of the GDPR's applicability on 25 May 2018.¹⁴⁴ This complaint argued Meta breached the GDPR's requirements for freely given consent because Article 6(1)(b) can only be relied upon "in respect of processing that is 'strictly necessary' to perform the contract."¹⁴⁵ More specifically, NOYB argued data processing must "be linked to the 'core' functions of the contract"¹⁴⁶ and behavioural advertising was outside the contract's scope. However, the Irish DPC disagreed with NOYB and concluded Facebook did not seek to rely on consent to process personal data and was not obliged to do so.¹⁴⁷ Therefore, the DPC rejected NOYB's argument that clicking on the accept button for the Terms and Conditions constituted consent and was subject to the GDPR's consent requirements.¹⁴⁸ In accordance with Article 60(3) of the GDPR, the Irish DPC submitted its draft decision to its peer regulators called Concerned Supervisory Authorities (CSA) for feedback. However, the DPC later rejected the CSA's feedback and triggered the Board's binding dispute resolution mechanism under Article 65(a) of the GDPR.

In its binding decision, the Board disagreed with the DPC's finding that Meta was not obliged to rely on consent to process personal data for behavioural advertising.¹⁴⁹ The Board also concluded the DPC's investigation into Meta lacked due diligence and did not address how special categories of personal data were obtained and processed for online advertising.¹⁵⁰ Given Meta's sole reliance on Article 6(1)(b) of the GDPR for personal data processing, the Board argued data subjects would be deprived of the protections derived from using consent as a legal basis, including the possibility to consent to different data processing operations,¹⁵¹ the right to be forgotten,¹⁵² and the right to withdraw consent.¹⁵³ The Board's decision was significant because even though Meta's legal basis for processing personal data was not Article 6(1)(a) of the GDPR, the requirements for freely given consent remained applicable.

¹⁴³ James Grieco, 'Data Privacy Hits Back Against Meta in 2023' (14 November 2023) <<https://www.mineos.ai/articles/data-privacy-hits-back-against-meta-in-2023>> accessed 8 March 2024.

¹⁴⁴ NOYB- European Center for Digital Rights, 'Breaking: Meta Prohibited from Use of Personal Data for Advertising' (NOYB, 4 January 2023) <<https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising>> accessed 10 March 2024.

¹⁴⁵ Helen Dixon, 'Draft Decision for the purposes Article 60 of the GDPR of the Data Protection Commission made pursuant to Section 113(2)(a) of the Data Protection Act 2018' (DPC, 6 October 2021) para 4.10.

¹⁴⁶ *ibid.*

¹⁴⁷ *ibid* para 3.25.

¹⁴⁸ *ibid.*

¹⁴⁹ European Data Protection Board, 'Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65)' (5 December 2022) para 202.

¹⁵⁰ *ibid* para 199.

¹⁵¹ GDPR, recital 43.

¹⁵² *ibid* art. 17.

¹⁵³ *ibid* art. 7(3).

Additionally, the Board concluded the GDPR “treats personal data as a fundamental right inherent to a data subject and his/her dignity, and not as a commodity data subjects can trade away through a contract.”¹⁵⁴ This finding is pertinent for both contractual necessity and pay-or-okay models because it acknowledges that fundamental privacy rights can override the economic interests of online platforms. However, the Board still recognised the validity of economic interests by explaining data protection rights should be balanced “against other fundamental rights and freedoms such as the freedom to conduct a business.”¹⁵⁵ By acknowledging the importance of balancing opposing interests, the Board gave European businesses a stepping stone to argue that contracts and pay-or-okay models are business practices protected under Article 16 of the EU Charter. For example, the Interactive Advertising Bureau of Europe (IAB) and Alliance Digitale have implored the Board to uphold pay-or-okay models as standard business practices.¹⁵⁶ After the Board struck down Meta’s contract model under Article 6(1)(b) of the GDPR, the Irish DPC fined Meta €390 million for GDPR breaches and ordered the company to establish a new legal basis for personal data processing by April 2023.¹⁵⁷

1.4.3. The Legitimate Interests Model (July-December 2023)

In late March 2023, Meta switched from a contract model to a legitimate interest model under Article 6(1)(f) of the GDPR, arguing that personal data processing was essential for the company’s functioning.¹⁵⁸ This change prompted the DPC and other DPAs to start assessing Meta’s compliance with the GDPR. Before issuing its assessment, the DPC explained it would wait for the ECJ’s judgment in the *Bundeskartellamt* case.¹⁵⁹ This case stemmed from the German national competition authority’s (BKartA) decision in February 2019 to impose restrictions on Meta for breaching German competition law because “there [was] no effective consent to the users’ information being collected if their consent [was] a prerequisite for using Facebook in the first place.”¹⁶⁰ After Meta appealed this decision, the Düsseldorf Higher Regional Court requested a preliminary ruling from the ECJ. On 4 July 2023, the ECJ concluded data subjects could not reasonably expect Meta to process their personal data for behavioural advertising solely based on legitimate interest without

¹⁵⁴ European Data Protection Board, ‘Binding Decision 4/2022 on the dispute submitted by the Irish SA’ (n 149) para 104.

¹⁵⁵ *ibid.*

¹⁵⁶ Interactive Advertising Bureau (IAB) Europe, IAB Italia, IAB Spain, and Alliance Digitale (n 11).

¹⁵⁷ The Data Protection Commission (DPC), ‘Data Protection Commission announces conclusion of two inquiries into Meta Ireland’ (DPC, 4 January 2023) <<https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland>> accessed 10 March 2024.

¹⁵⁸ Meta Newsroom, ‘How Meta Uses Legal Bases for Processing Ads in the EU’ (n 16).

¹⁵⁹ *Facebook Inc. and Others v. Bundeskartellamt* (Case C-252/21) [2023] ECLI:EU:C:2023:537.

¹⁶⁰ Bundeskartellamt (BKartA) [Independent Competition Authority – Federal Cartel Office] ‘Case Summary: Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing (6 February 2019), p. 1.

consent.¹⁶¹ The Court also argued that the rights of data subjects override the financial interests of operators, so Meta could not rely on Article 6(1)(f) of the GDPR for data processing for behavioural advertising.¹⁶² This finding is significant for both legitimate interest and pay-or-okay models because it prioritised privacy rights over Meta's interest in using behavioural advertising to finance its operations.

In addition to rejecting Meta's reliance on Article 6(1)(f) of the GDPR for behavioural advertising, the ECJ made two noteworthy comments on the considerations for freely given consent. Firstly, the Court acknowledged that the dominant position of an online platform like Meta did not prevent them from validly obtaining consent.¹⁶³ However, this dominant position could create an imbalance of power between the controller and the data subject, leading to "conditions that are not strictly necessary for the performance of a contract."¹⁶⁴ The Court did not elaborate on whether other online platforms in less dominant positions created similar imbalances of power that contravened the GDPR's conception of freely given consent. Secondly, the Court suggested "users [could] be offered, *if necessary for an appropriate fee*, an equivalent alternative not accompanied by such data processing operations [emphasis added]."¹⁶⁵ This caveat has sparked extensive debate on the meaning of appropriate fee. For example, CNIL explained determining an appropriate fee should be made on a case-by-case basis.¹⁶⁶ However, the authority acknowledged that establishing this standard was outside its jurisdiction and was up to the ECJ.¹⁶⁷ The Norwegian, German, and Austrian DPAs have also emphasised the importance of avoiding unreasonably high prices for payment alternatives but provided no specifics.¹⁶⁸ Despite this uncertainty, the possibility of imposing an appropriate fee prompted Meta to implement its pay-or-okay

¹⁶¹ *Facebook Inc.* (n 159) [117].

¹⁶² *ibid.*

¹⁶³ *ibid* [147], [149].

¹⁶⁴ *ibid.*

¹⁶⁵ *ibid* [150].

¹⁶⁶ Commission nationale de l'informatique et des libertés [CNIL] 'Cookie walls: la CNIL publie des premiers critères d'évaluation (Cookie walls: the CNIL publishes first evaluation criteria)' (16 May 2022) <<https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation>> accessed 10 May 2024.

¹⁶⁷ *ibid.*

¹⁶⁸ The Norwegian Data Protection Authority (Datatilsynet), 'Hvad siger reglerne? Cookie Walls (What do the rules say? Cookie Walls)' <<https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/cookies/cookie-walls>> accessed 11 May 2024; The Committee of Independent German Federal and State Data Protection Supervisory Authorities (DSK), 'Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) (Guidance from the supervisory authorities on the processing of personal data for direct advertising purposes under the General Data Protection Regulation (GDPR))' (February 2022); The Data Protection Authority for Austria (Datenschutzbehörde), 'FAQ zum Thema Cookies und Datenschutz (FAQ on Cookies and Data Protection)' (20 December 2023).

model under the legal basis of consent found in Article 6(a) of the GDPR in August 2023.¹⁶⁹ After all, Meta was required to change its legitimate interest legal basis for data processing after the DPC issued a provisional paper on the matter on 11 July 2023. Three days later, the Norwegian DPA also implored Meta to change its legal basis by prohibiting the company from processing personal data for behavioural advertising in Norway under the contract and legitimate interest models.¹⁷⁰

2. Legal Analysis of Pay-or-Okay Models Under the GDPR

2.1. The Board's Decision on Meta's Pay-or-Okay Model

To guide this working paper's interpretation of freely given consent for pay-or-okay models, it is important to discuss the Board's binding decision on Meta's pay-or-okay model from 17 April 2024. The impetus behind this decision stemmed from disagreements among DPAs on the legality of pay-or-okay models. For example, the German DPA (DSK) determined these models were legally justified if both the tracking and tracking-free options were equivalent and fulfilled the GDPR's consent requirements.¹⁷¹ The Austrian DPA made a more specific finding that pay-or-okay models presented as banners breached the granularity condition for freely given consent under the GDPR, but did not explicitly rule on the legality of such models.¹⁷² Both the British DPA (ICO) and the Norwegian DPA (Datatilsynet) expressed concerns over Meta's pay-or-okay model and are currently contributing to legal assessments at the national and European levels.¹⁷³ These inconclusive assessments among DPAs revealed continent-wide confusion on the legality of pay-or-okay models and the need for Board intervention.

DPAs and Member States have discretion to interpret and restrict certain GDPR articles. Article 23 and Recital 10 of the GDPR give Member States the power to restrict the scope of Articles 5, 12 to 22, and 34 if restrictions are necessary, proportionate, and safeguard an enumerated purpose.¹⁷⁴ This flexibility prompted some Member States to pass national data protection laws adding lawful bases for the processing of sensitive personal data, changing

¹⁶⁹ Meta Newsroom, 'Facebook and Instagram to Offer Subscription for No Ads in Europe' (*Meta*, 30 October 2023) < <https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/> > accessed 10 March 2024.

¹⁷⁰ The Norwegian Data Protection Authority (Datatilsynet), 'Urgent and Provisional Measures- Meta' (14 July 2023) <https://www.datatilsynet.no/contentassets/36ad4a92100943439df9a8a3a7015c19/urgent-and-provisional-measures--meta_redacted.pdf> accessed 11 May 2024.

¹⁷¹ DSK, 'Bewertung von Pur-Abo-Modellen auf Websites' (n 19).

¹⁷² The Data Protection Authority for Austria (Datenschutzbehörde), 'Decision on Cookie Banners' (29 March 2023).

¹⁷³ The Information Commissioner's Office (ICO), 'Call for Views on 'consent or pay' business models' (2024) < <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-views-on-consent-or-pay-business-models/> > accessed 5 May 2024; The Norwegian Data Protection Authority (Datatilsynet), 'Datatilsynet følger med på nye løsninger' (8 November 2023).

¹⁷⁴ GDPR, art. 23.

the age of consent for children, and more.¹⁷⁵ Article 23 of the GDPR does not discuss restricting the scope of the definition and conditions for consent – which lay the foundation for pay-or-okay models – found in Articles 4, 6, and 7 of the GDPR. Therefore, to ensure a harmonised interpretation and application of consent, the Board has published guidelines and decisions on the matter for national DPAs. Reinforcing the Board’s important role, the EU Parliament acknowledged the group “harmonized rules on what constitutes valid consent, replacing different interpretations by many national DPAs and avoiding fragmentation.”¹⁷⁶ Overall, the GDPR aims to safeguard the free movement and protection of personal data which requires a harmonized interpretation and enforcement of consent across the EU.

Considering DPAs across Europe have not agreed on the legality of Meta’s pay-or-okay model, the Norwegian, Dutch, and German DPAs requested the Board’s opinion under Article 64(b) GDPR in January 2024.¹⁷⁷ In its opinion, the Board concluded that “in most cases, it will not be possible for large online platforms to comply with the requirements for valid consent”¹⁷⁸ if people are given a binary option between agreeing to behavioural advertising or paying a fee. This opinion will inform subsequent national investigations on Meta by DPAs and require the DPC to re-issue a decision on Meta’s compliance with the GDPR.¹⁷⁹ The Board’s opinion was requested under Article 64(2) rather than Article 66(2) of the GDPR because the latter concerns the urgency procedure. Meta has previously argued the Board is not competent to order measures under the urgency procedure on an EU-wide basis, so the Board requested that EU legislators clarify this matter.¹⁸⁰ However, the Board’s opinion under Article 64(2) of the GDPR is binding when DPAs – in this case, those in Norway, the Netherlands, and Germany – allege another authority (i.e., the DPC) does not comply with mutual assistance obligations under Article 61 of the Regulation.¹⁸¹ Although the Board’s decision is binding on DPAs, Meta can still appeal the decision and bring an action for annulment before the ECJ for review.

Despite the Board’s decision, this working paper’s legal analysis of pay-or-okay models under the GDPR remains relevant for three reasons. Firstly, the Board only addressed pay-or-okay models for large online platforms and explained each situation needed to be

¹⁷⁵ GDPR Resource Center, ‘Derogations Tracker’ (Latham & Watkins, 2024) < <https://gdpr.lw.com/Home/Derogations>> accessed 6 May 2024.

¹⁷⁶ European Parliament Resolution 2020/2717(RSP) of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application [2021].

¹⁷⁷ NOYB- European Center for Digital Rights ‘28 NGOs Urge EU DPAs to Reject “Pay or Okay” on Meta’ (n 8).

¹⁷⁸ European Data Protection Board, ‘Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms’ (17 April 2024) p. 3.

¹⁷⁹ Meta’s European headquarters are based in Ireland, making the DPC the company’s primary DPA.

¹⁸⁰ European Data Protection Board, ‘Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR’ (27 October 2023) para 267.

¹⁸¹ GDPR, art 61.

assessed on a case-by-case basis.¹⁸² This narrow scope reveals the need to examine freely given consent under the GDPR for other types of online platforms. Secondly, this working paper can help inform the Board's future guidelines on pay-or-okay models for all types of online platforms.¹⁸³ These guidelines will likely be published after the Board engages in discussions with relevant stakeholders including DPAs, businesses, NGOs, and other stakeholders. Thirdly, Meta is expected to appeal both the Board's decision and the DPC's subsequent decision on the matter, which will prolong legal discussions on personal data processing for behavioural advertising under the GDPR.¹⁸⁴ The DPC also has a history of challenging the Board's decisions. For example, in March 2023 legal experts reported the DPC would challenge the Board's jurisdiction to require a new investigation into Meta because Article 263 of the TFEU grants a power of review to the CJEU when it comes to EU legislative acts.¹⁸⁵ Ultimately, there is a long road of legal argument ahead in the CJEU and Irish Courts regarding Meta's pay-or-okay model and pay-or-okay models more generally.

2.2. Valid Consent under the GDPR

Before discussing the four considerations for freely given consent, it is worth outlining the GDPR's conception of valid consent. This discussion is important because online platforms like Meta have based the lawfulness of personal data processing for behavioural advertising on Article 6(1)(a) of the GDPR for pay-or-okay models. This article stipulates that "the data subject has *given consent* to the processing of his or her personal data for one or more specific purposes [emphasis added]."¹⁸⁶ Article 4(11) of the Regulation defines valid consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement."¹⁸⁷ This definition reveals freely given consent is the first of four cumulative requirements for valid consent. The second requirement for valid consent is specificity, meaning online platforms need to define "a specific, explicit, and legitimate purpose"¹⁸⁸ for personal data processing. To maintain specificity, online platforms cannot bundle data processing activities together and must request consent for each separate and different activity. The third requirement for valid consent is that the controller informs the data subject before asking for consent. More specifically, Article 7(2) of the GDPR stipulates that the controller asks for consent in a

¹⁸² European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) p. 3.

¹⁸³ Laura Cabrera and Nathalie Maréchal, 'The European Data Protection Board's Opinion on "Pay or Okay" Models – Surveillance-Based Advertising Is on Borrowed Time' (*Center for Democracy and Technology*, 10 May 2024) <<https://cdt.org/insights/the-european-data-protection-boards-opinion-on-pay-or-okay-models-surveillance-based-advertising-is-on-borrowed-time/>> accessed 11 May 2024.

¹⁸⁴ Meta Newsroom, 'How Meta Uses Legal Bases for Processing Ads in the EU' (n 16).

¹⁸⁵ Luke Irwin, 'Irish DPC Challenges EDPB Jurisdiction in Meta Investigation' (*IT Governance Blog*, 23 March 2023) <<https://www.itgovernance.eu/blog/en/irish-dpc-challenges-edpb-jurisdiction-in-meta-investigation>> accessed 11 May 2024.

¹⁸⁶ GDPR, art 6(1)(a).

¹⁸⁷ *ibid* art 4(11).

¹⁸⁸ European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) para 161.

clearly distinguishable, easily accessible, clear, and plain way.¹⁸⁹ This requirement is linked to Article 5 which requires personal data to be processed “lawfully, fairly, and in a transparent manner.”¹⁹⁰ To achieve informed consent, the Board concluded that data subjects must be informed of the controller’s identity, the purpose for data processing, the type of data collected, and the risks of providing consent.¹⁹¹ Informed consent also depends on the data subject’s knowledge of their right to withdraw consent at any time.¹⁹²

The fourth requirement for valid consent is that the data subject provides an unambiguous and affirmative indication of their wishes. Affirmative action is not fulfilled by “silence or inactivity on the part of the data subject.”¹⁹³ Additionally, the controller cannot pre-tick consent boxes in its favour.¹⁹⁴ To provide unambiguous and affirmative consent, the data subject must take deliberate action when agreeing to data processing. A final requirement for valid consent which is not outlined in the GDPR includes the renewal process. The GDPR does not specify an expiration date for valid consent, but the Board suggested the timeframe depends on the context and scope of the data processing activities.¹⁹⁵ Although the Board previously recommended consent “be refreshed at appropriate intervals,”¹⁹⁶ it later specified that controllers should renew consent in the context of behavioural advertising on an annual basis.¹⁹⁷

In the context of pay-or-okay models, this working paper will analyse the four considerations for freely given consent and examine ECJ cases, Board opinions, DPA sources, and NOYB complaints in the process. Freely given consent implies the data subject has a real choice and can exercise free will without coercion, intimidation, or deception by the controller.¹⁹⁸ The ECJ has outlined four considerations for freely given consent: imbalance of power between the controller and the data subject, conditionality, detriment to the data subject, and granularity.¹⁹⁹ Although these considerations are interrelated, each must be followed when the data subject initially provides consent to the processing of personal data. Under Article 7(1) and Recital 42 of the GDPR, it is the controller’s responsibility to demonstrate that consent has been obtained in a valid and freely given way.²⁰⁰ Overall, this working paper argues the GDPR does not prohibit pay-or-okay models in principle, but these models must meet all requirements for valid and freely given consent to be legally permissible.

¹⁸⁹ GDPR, art 7(2).

¹⁹⁰ *ibid* art 5.

¹⁹¹ European Data Protection Board, ‘Guidelines 05/2020 on consent’ (n 33) para 64.

¹⁹² GDPR, art 7(3), 13(2)(c), 14(2)(d), and 17(1)(b).

¹⁹³ European Data Protection Board, ‘Guidelines 05/2020 on consent’ (n 33) para 79.

¹⁹⁴ *ibid*.

¹⁹⁵ *ibid* p. 23.

¹⁹⁶ *ibid*.

¹⁹⁷ European Data Protection Board, ‘Opinion 08/2024 on Valid Consent’ (n 178) para 178.

¹⁹⁸ GDPR, recital 42; European Data Protection Board, ‘Opinion 08/2024 on Valid Consent’ (n 178) para 69.

¹⁹⁹ *Facebook Inc.* (n 159) [143]-[154].

²⁰⁰ GDPR, recital 42 and art 7(1).

2.3. The Four Considerations for Freely Given Consent

2.3.1. Imbalance of Power

The first consideration for freely given consent is the imbalance of power between the controller and the data subject. The GDPR defines controller as “the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.”²⁰¹ The imbalance of power consideration stems from Recital 43 which stipulates that “to ensure consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority”.²⁰² These situations typically occur within the context of an employment relationship. For example, the WP29 explained “employees are almost never in a position to freely give consent,”²⁰³ and this consent can only be obtained in “exceptional circumstances.”²⁰⁴ In other words, an employee’s reliance on the employer for money often invalidates the data subject’s consent. In the context of pay-or-okay models, assessing imbalances of power raises concern for content creators because their livelihoods depend on social media activity and followings. This illustrates how content creators are disproportionately exposed to consequences when refusing consent for personal data processing. However, the employer-employee relationship for content creators remains ambiguous because some online platforms like Meta do not directly compensate individuals.²⁰⁵ Rather, revenue for content creators comes from third-party brand partnerships and affiliate programs.²⁰⁶ Despite this ambiguity, the Board confirmed that imbalances of power can occur outside the formal employer-employee relationship and must be assessed on a case-by-case basis.²⁰⁷

For pay-or-okay models operated by large online platforms like Meta, the Board outlined key factors when determining imbalances of power. For example, the Board argued the relationship between the controller and data subject should be assessed based on “the position of the large online platform in the market, the existence of lock-in or network effects, the extent to which the data subject relies on the service, and the main audience of the service.”²⁰⁸ As for the online platform’s position in the market, the GDPR lacks explicit guidance on how this affects the controller’s relationship with the data subject. Adding to

²⁰¹ GDPR, art 4(7).

²⁰² *ibid* recital 43.

²⁰³ Article 29 Working Party (WP29), ‘Opinion 2/2017 on data processing at work’ WP 249 (8 June 2017) p. 4.

²⁰⁴ *ibid*.

²⁰⁵ Jean Folger, ‘How to Make Money on Instagram 2024’ (*Time*, 2024) <<https://time.com/personal-finance/article/how-to-make-money-on-instagram/>> accessed 11 May 2024.

²⁰⁶ *ibid*.

²⁰⁷ European Data Protection Board, ‘Guidelines 05/2020 on consent’ (n 33) para 22; European Data Protection Board, ‘Opinion 08/2024 on Valid Consent’ (n 178) para 99.

²⁰⁸ European Data Protection Board, ‘Opinion 08/2024 on Valid Consent’ (n 178) p. 3.

this uncertainty, the ECJ explained the controller’s dominant position “may create an imbalance”²⁰⁹ but should be considered on an individual basis when determining freely given consent. Considering the Court has provided no specific guidelines for conducting this assessment, it is helpful to review previous Board opinions. The Board has explained that a dominant market position is not necessary for an imbalance of power to exist between the controller and data subject.²¹⁰ This finding suggests online platforms with a non-dominant market position can still create imbalances of power contrary to freely given consent. However, determining whether non-dominant online platforms generate imbalances of power is challenging because their smaller user base would likely result in less noticeable network and lock-in effects. Network and lock-in effects arise when users depend on an online platform for social connections and cannot easily switch platforms without isolating themselves from friends, family, acquaintances, and online resources. Ultimately, assessing the market positions of online platforms should be done individually and be reviewed periodically to account for changing market dynamics.

2.3.1.1. Network and Lock-In Effects

In addition to an online platform’s market position, potential network and lock-in effects must be carefully considered to determine whether an imbalance of power exists between the controller and the data subject. The Board argues that network and lock-in effects become exacerbated “when the user has significantly invested in [and relied upon] the platform”²¹¹ and cannot realistically choose an alternative. However, the Board has not clarified how someone’s investment in an online platform can be quantified. Should this depend on the number of Facebook friends, online posts, or hours the individual spends on social media? The Board opined that content creators may endure an irreparable loss in the context of pay-or-okay models if they lose their portfolio and their following.²¹² If imbalance of power assessments are made on a case-by-case basis, the Board’s reasoning may provide individuals who are more active on social media with greater protections than less active individuals. When determining network and lock-in effects, the Board should also consider that individuals in some Member States, such as Denmark, Cyprus, and Hungary, to participate in social networks more than individuals in other Member States like France, Germany, and Italy.²¹³ This raises questions on the extent to which network and lock-in effects depend on the individual’s country of residence. Overall, evaluations of network and lock-in effects should minimise discussions on the data subject’s reliance on the online platform to avoid measurability challenges.

²⁰⁹ *Facebook Inc.* (n 159) [149].

²¹⁰ European Data Protection Board, ‘Opinion 08/2024 on Valid Consent’ (n 178) para 103.

²¹¹ *ibid* para 108.

²¹² *ibid* p. 23.

²¹³ ‘59% of EU Individuals Using Social Networks in 2023 - Eurostat’ (*Eurostat*)

<<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240319-1>> accessed 11 May 2024.

Given the ambiguity surrounding someone's reliance on an online platform, emphasis should instead be placed on the online platform's economic dominance in a specific region. In Meta's case, the European Commission designated the online platform a gatekeeper under the Digital Markets Act (DMA) due to its strong economic position in multiple Member States.²¹⁴ The DMA is a piece of EU legislation that places obligations on gatekeepers to maintain a fair and open digital market across Europe.²¹⁵ Although Meta is appealing its designation as a gatekeeper for certain services, this identification is important because it underscores the company's dominance within the internal market.²¹⁶ In a previous opinion regarding online profiling, the Board recommended examining whether gatekeepers offered consumers a non-profiling version of the online service and whether individuals had to endure access conditions for such a service.²¹⁷ In another opinion regarding WhatsApp, the Board found that the online platform's "take-it or leave-it situation" for personal data processing was impermissible due to the lack of alternative services available in the market for users.²¹⁸ Given these findings, it is unsurprising that the Board's opinion on Meta's pay-or-okay model concluded that "the offering of (only) a paid alternative to the service...should not be the default way forward for controllers."²¹⁹ Nevertheless, the Board should have highlighted Meta's market power with roughly 9.4 billion in revenue across the EU rather than people's reliance on Facebook for social connections.²²⁰ This market power approach was adopted by the AEPD when it assessed the economic power and annual revenue of a bank to determine whether freely given consent was obtained under Article 7(4) of the GDPR.²²¹ Overall, framing imbalance of power discussions on market dominance and economics is more easily quantifiable than measuring someone's reliance on an online platform.

2.3.1.2. The Main Audience of the Service

Finally, the main audience of the service must be examined when determining whether an imbalance of power exists between the controller and the data subject. More specifically, the

²¹⁴ European Commission, 'Digital Markets Act: Commission designates six gatekeepers' (Press release, 6 September 2022).

²¹⁵ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directive (EU) 2-19/1937 and (EU) 2020/1828 (Digital Markets Act) L 265/1.

²¹⁶ Supantha Mukherjee and Foo Yun Chee, 'Meta Appeals against EU Gatekeeper Status for Messenger, Marketplace' *Reuters* (15 November 2023) <<https://www.reuters.com/technology/meta-appeals-against-eu-gatekeeper-status-messenger-marketplace-2023-11-15/>> accessed 11 May 2024.

²¹⁷ European Data Protection Board and European Data Protection Supervisor, 'Joint EDPB-EDPS contribution to the public consultation on the draft template relating to the description of consumer profiling techniques (Art. 15 DMA)' (20 September 2023) p. 13.

²¹⁸ European Data Protection Board, 'Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR)' (5 December 2022) para 156.

²¹⁹ European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) p. 3.

²²⁰ Stacy Jo Dixon, 'Meta: Quarterly Revenue in Europe 2024' (*Statista*, 26 April 2024) <<https://www.statista.com/statistics/745351/facebook-s-quarterly-revenue-in-europe/>> accessed 11 May 2024.

²²¹ Agencia Española de Protección de Datos (n 21) p. 13.

Board explained online platforms must examine their “target or predominant audience” to ensure their privacy policies are formulated in an easily understandable way so users are informed before providing consent.²²² For example, an online platform targeting children or other vulnerable individuals may lead to a clearer imbalance of power.²²³ Meta requires online users to be at least thirteen years old (with varying age requirements across different countries), indicating the platform’s primary audience is not small children.²²⁴ However, Meta may attract users beyond their target audience. This illustrates how relying solely on age verification during the sign-up process may not reflect reality. While the Board has not defined Meta’s target or main audience, NOYB contended that Meta’s extensive user base sets it apart from other platforms like LinkedIn and TikTok. Citing LinkedIn’s professional focus and TikTok’s appeal to younger demographics, NOYB argued users cannot freely consent to Meta’s personal data processing scheme due to the lack of similar alternatives.²²⁵ To determine imbalances of power more adequately, both NOYB and the Board should focus on the online platform’s functionalities rather than its target audience. While LinkedIn caters to career networking and TikTok features continuous loop videos, Meta offers more services like chatting, joining groups, and reading news articles. Given Meta’s broader range of services, it becomes more challenging to find a suitable alternative. Therefore, framing imbalance of power discussions on an online platform’s functionalities is more reliable than gauging its main audience.

2.3.2. Conditionality

The second consideration for freely given consent is conditionality. Conditionality stems from Article 7(4) of the GDPR which stipulates that “when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.”²²⁶ This article aims to guarantee transparency and ensure controllers do not mislead users into providing consent for personal data processing that is not required for the contract. The term “utmost account” suggests controllers should carefully ask users for consent. Additionally, a grammatical interpretation of the term “inter alia” implies that the necessity of personal data processing for contract performance is one of numerous factors that should be considered when determining freely given consent. According to the WP29, the phrase “necessary for the performance of a contract” should be interpreted strictly so that personal data

²²² European Data Protection Board, ‘Opinion 08/2024 on Valid Consent’ (n 178) para 111.

²²³ *ibid* p. 26.

²²⁴ Facebook Help Center, ‘Confirming Your Age on Facebook’ (*Meta*, 2024) <<https://www.facebook.com/help/adsmanagerbuiltin/157793540954833>> accessed 11 May 2024.

²²⁵ NOYB-European Center for Digital Rights, ‘Complaint pursuant to Article 80(1) GDPR against Meta Platforms Ireland Limited’ (*NOYB*, 28 November 2023) para 37.

²²⁶ GDPR, art 7(4).

processing is directly linked to the contract's purpose.²²⁷ For example, if an online platform requests consent from customers to share their address details with a third-party courier for delivery purposes, this aligns with necessary contractual obligations. However, requesting consent from customers to share their preferences with third parties for marketing purposes would be contrary to freely given consent.

In the context of Meta's pay-or-okay model, users can only access Facebook and Instagram services if they consent to behavioural advertising or pay a monthly fee. The ECJ concluded behavioural advertising is not strictly necessary for contract performance, making it important to analyse whether imposing a fee is a legally justified and equivalent alternative.²²⁸ Determining whether pay-or-okay models are equivalent alternatives is important because the wording of Article 7(4) is "not construed in an absolute manner" in the GDPR.²²⁹ This interpretation is supported by the Board's suggestion that there might be "limited space"²³⁰ for cases where conditionality does not render consent invalid. However, the Board also provided an example of invalid consent where a bank requests the consent of customers to process personal data for marketing purposes. If customers refusing to consent suffer an increase in fees or the closure of bank accounts, then consent cannot be freely given.²³¹ Considering pay-or-okay models include fees by design, it is important to determine whether these models are equivalent alternatives to those with behavioural advertising and whether the fees imposed are appropriate under the GDPR.

2.3.2.1. Defining 'Equivalent Alternative'

To determine whether imposing a fee is legally justified, it is important to first define 'equivalent alternative' in the context of conditionality. In 2017, the WP29 published draft guidelines on consent explaining that a second online service option needed to include "no further costs" to be genuinely equivalent with the first online service option. Interestingly, this requirement was omitted from the WP29's final guidelines published in 2018, indicating potential disagreement on the matter.²³² In 2023, the ECJ addressed the concept of freely given consent and explained users must be free to refuse a particular data processing operation without being blocked from the online platform.²³³ Additionally the Court explained that users "are to be offered, *if necessary for an appropriate fee*, an equivalent alternative not accompanied by such data processing operations."²³⁴ This suggests online services can be considered genuinely equivalent if the only differences between them

²²⁷ European Data Protection Board, 'Guidelines 05/2020 on consent' (n 33) para 30.

²²⁸ *Facebook Inc.* (n 159) [149].

²²⁹ European Data Protection Board, 'Guidelines 05/2020 on consent' (n 33) para 35.

²³⁰ *ibid.*

²³¹ *ibid* para 33.

²³² Article 29 Working Party (WP29), 'Guidelines on Consent under Regulation 2016/679' (28 November 2017) p. 10.

²³³ *Facebook Inc.* (n 159) [150].

²³⁴ *ibid* (emphasis added).

include behavioural advertising and cost. The Board also clarified that conditionality assessments must be conducted on a case-by-case basis.²³⁵ However, the Board noted that the greater the disparity between the online versions, the less likely they are to be genuinely equivalent.²³⁶ Considering the main disparities between Meta's two service options involve behavioural advertising and costs, defining 'appropriate fee' is essential.

2.3.2.2. Interpreting 'Appropriate Fee'

Interpretations of the term 'appropriate fee' vary among authorities. Unfortunately, the ECJ briefly mentioned the possibility of an appropriate fee without providing clarification on its meaning or specifying which factors to consider when assessing appropriateness.²³⁷ Given this lack of guidance, the Board's opinion on Meta's pay-or-okay model employs cautious language to avoid contradicting the Court. The Board explained personal data "cannot be considered a tradeable commodity"²³⁸ and controllers should individually assess "both whether a fee is appropriate *at all* and what amount is appropriate [emphasis added]."²³⁹ At first glance, the Board's suggestion that fees may be unsuitable challenges the Court's explicit allowance for alternative versions of an online platform to impose fees. However, it is important to consider the German language version of the ECJ's judgment because the case was dealt with in German under Article 41 of the Court's Rules of Procedure.²⁴⁰ From a legal perspective under Article 55 of the TEU, all language versions of Community provisions and CJEU judgments are authentic and not considered translations.²⁴¹ Although the obligation to compare different language versions of CJEU judgments is debated,²⁴² the ECJ has concluded that "interpretation of a provision of Community law involves a comparison of the language versions."²⁴³ Additionally, the Court has affirmed that "Community provisions must be interpreted and applied uniformly in the light of the versions existing in the other Community languages."²⁴⁴ Given the ambiguity surrounding the term "appropriate fee", it is worth comparing the English and German versions of the Court's judgment for clarification.

The German version of the Court's judgment provides greater flexibility than the English version by suggesting certain circumstances must be present for the controller to impose a

²³⁵ European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) para 124.

²³⁶ *ibid.*

²³⁷ *Facebook Inc.* (n 159) [150].

²³⁸ European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) p. 4.

²³⁹ *ibid.*

²⁴⁰ *Facebook Inc.* (n 159); The Rules of Procedure of the Court of Justice (29 September 2012) L 265/1 art 41.

²⁴¹ Lucie Pacho Aljanati, 'Multilingual interpretation by the CJEU in the Area of Freedom, Security, and Justice' in Anne Lise Kjaer and Joanna Lam (eds), *Language and Legal Interpretation in International Law* (OUP 2022) 166.

²⁴² *ibid.*

²⁴³ *Aannemersbedrijf P.K. Kraaijeveld BV e.a. v. Gedeputeerde Staten van Zuid-Holland* (Case 72/ 95) [1996] EU:C:1996:404 [28].

²⁴⁴ *Ferriere Nord SpA v Commission of the European Communities* (Case C-219/95) [1997] ECLI:EU:C:1997:375 [15].

fee. The English version states an appropriate fee may be imposed if necessary. The Board clarified that this phrasing in the English version does not implicate Article 52(1) of the Charter which states limitations to rights can “only be made if they are necessary.”²⁴⁵ However, the German version uses the term “gegebenenfalls”. This phrasing translates to “if applicable” or “under certain circumstances” in English, suggesting controllers can only impose a fee on a case-by-case basis.²⁴⁶ In other words, this German phrasing is more tentative than the English version and implores controllers to first determine whether a fee is appropriate and then decide upon the amount. When determining the fee amount, the Board explained controllers must ensure fees do not inhibit users from making a genuine choice to consent.²⁴⁷ This guidance is legally accurate for obtaining freely given consent but remains ambiguous because a fee may be reasonable for one person but unreasonable for another. Overall, the diversity of people’s financial circumstances makes assessing fee appropriateness more challenging.

2.3.2.3. NOYB’s Conditions for an Appropriate Fee

Considering the uncertainties surrounding the term “appropriate fee”, NOYB outlined an approach to determining fee amounts in its complaint to the Board on Meta’s pay-or-okay model. Firstly, NOYB argued the ECJ’s mention of appropriate fee should be considered *obiter dictum* given its vagueness.²⁴⁸ *Obiter dictum* is something said or written by a judge that is not essential to the Court’s final decision.²⁴⁹ However, no formal doctrine of *stare decisis* exists in EU law, meaning there is no distinction between *ratio decidendi* and *obiter dictum*.²⁵⁰ *Ratio decidendi* is legal reasoning that underscores the Court’s final decision.²⁵¹ Although NOYB’s first argument is legally questionable, the organisation’s second approach to determining an appropriate fee is more reasonable. This approach includes four criteria for an appropriate fee: the fee does not significantly alter an individual’s will to provide consent, it remains affordable even if pay-or-okay models proliferate across the market, it considers the income of users, and it compensates users for the controller’s profit made by behavioural advertising. As for the first condition, NOYB argues Meta’s current fee is inappropriate

²⁴⁵ The Charter (n 12) art 52(1).

²⁴⁶ European Data Protection Board, ‘Opinion 08/2024 on Valid Consent’ (n 178) para 131.

²⁴⁷ *ibid* p. 4.

²⁴⁸ NOYB-European Center for Digital Rights, ‘Complaint pursuant to Article 80(1) GDPR against Meta Platforms Ireland Limited’ (n 225) p. 9.

²⁴⁹ ‘Obiter Dictum’ (*Oxford Reference*)

<<https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100243515>> accessed 11 May 2024.

²⁵⁰ Takis Tridimas, ‘Precedent and the Court of Justice: A Jurisprudence of Doubt?’ in Julie Dickson and Pavlos Eleftheriadis (eds), *Philosophical Foundations of European Union Law* (OUP 2012) 307, 313.

²⁵¹ ‘Ratio Decidendi’ (*Oxford Reference*)

<<https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100405351>> accessed 11 May 2024.

because it achieves “almost ‘North Korean’ consent rates of 99%.”²⁵² Citing survey results, NOYB argues roughly 3 to 10 percent of users want behavioural advertisements and this illustrates the discrepancy between people’s will and actions.²⁵³ Further assessment is necessary to verify the accuracy of these percentages because extraneous factors including the length and complexity of Meta’s Terms and Conditions could impact consent rates. Therefore, future research should perform systematic random sampling of online users to better understand the numerous variables affecting people’s decision to consent to pay-or-okay models.

The second condition outlined by NOYB is that an appropriate fee remains affordable if pay-or-okay models proliferate across the market. On average, individuals use 35 applications on their mobile device every month.²⁵⁴ If these applications all implemented pay-or-okay models, this cumulative fee would likely be unreasonable for most users. This is reinforced by NOYB’s calculation that a cumulative fee could reach 8,815 euros annually per user.²⁵⁵ Interestingly, Meta acknowledged this financial burden and offered to lower its subscription rate from 9.99 euros to 5.99 euros monthly in March 2024.²⁵⁶ In a statement to the European Commission, Meta lawyer Tim Lamb argued “[t]hat is by far the lowest end of the range that any reasonable person should be paying for services of this quality.”²⁵⁷ Meta’s decision prompts further discussion on whether reducing fees will alter consent rates. According to NOYB founder Max Schrems, “even a fee of 1.99 euros or less leads to a shift in consent,”²⁵⁸ prompting most users to agree to a company’s behavioural advertising scheme. Therefore, future research should investigate the threshold at which consent rates are affected to help determine how the term appropriate fee can be interpreted to safeguard the GDPR’s requirements for freely given consent.

The third condition outlined by NOYB is that an appropriate fee be based on the user’s income. This condition stems from the principle of fairness codified in Articles 5 and 6 of the GDPR for data processing.²⁵⁹ For Meta’s pay-or-okay model, it would be unfair if two individuals paid the same fee when one uses Instagram and Facebook every day whereas the other person uses it occasionally. The disparity in average incomes across EU Member States should also be assessed when determining an appropriate fee. After all, the average income

²⁵² NOYB-European Center for Digital Rights, ‘Complaint pursuant to Article 80(1) GDPR against Meta Platforms Ireland Limited’ (n 225) p. 6.

²⁵³ *ibid* p. 7.

²⁵⁴ NOYB- European Center for Digital Rights ‘28 NGOs Urge EU DPAs to Reject “Pay or Okay” on Meta’ (n 8).

²⁵⁵ NOYB-European Center for Digital Rights, ‘Complaint pursuant to Article 80(1) GDPR against Meta Platforms Ireland Limited’ (n 225) p. 9.

²⁵⁶ Foo Yun Chee, ‘Meta Offers to Almost Halve Facebook and Instagram Monthly Fees’ (*Reuters*, 19 March 2024) <<https://www.reuters.com/technology/meta-offers-cut-facebook-instagram-monthly-fees-599-euros-2024-03-19/>> accessed 11 May 2024.

²⁵⁷ *ibid*.

²⁵⁸ *ibid*.

²⁵⁹ GDPR, art 5(1)(a), 6(2) and 6(3).

in Luxembourg and Belgium is higher than in Romania, Croatia, and Hungary.²⁶⁰ On this point, the Board found that DPAs should be the ones to assess fee appropriateness. More specifically, the Board explained DPAs are tasked with enforcing the GDPR's application and this is related "to the impact of any fee on the data subject's freedom of choice."²⁶¹ The Board likely reached this conclusion by acknowledging the cost disparities among Member States, which is a positive development. However, giving DPAs a large margin of discretion raises concern regarding the potential lack of harmonisation across the EU if they come to different conclusions.

Additionally, determining fee appropriateness inherently monetises the right to privacy which may contradict the EU's goal to ensure every citizen enjoys the same fundamental rights based on equality, non-discrimination, and human dignity.²⁶² Supporting this idea, the Board advised large online platforms like Meta to offer an equivalent alternative "that does not entail the payment of a fee."²⁶³ If the ECJ rejects the Board's guidance and allows equivalent alternatives to impose a fee, then online platforms should offer a standard market fee.²⁶⁴ This position is supported by the DSK, albeit without a specific method for calculating a standard market fee. This fee should also consider both the users' income and the average income in their state of residence. As illustrated by Mastodon – an online platform headquartered in Germany – online platforms can operate free of charge by non-profit organisations.²⁶⁵ Given this possibility, NOYB's third condition for determining an appropriate fee must be broadened to consider the average income in specific Member States and the practice of other online platforms.

The fourth condition outlined by NOYB is that an appropriate fee should consider the controller's profits generated from behavioural advertising. From 2021 to 2023, between 18 to 26 percent of Meta's total revenue was spent on expenses associated with operating and maintaining Facebook and Instagram services.²⁶⁶ This statistic suggests a significant portion of Meta's revenue, between 74 to 82 percent, does not contribute to enhancing user benefits. On average, Meta also generates roughly US\$16 per fiscal quarter (i.e., a three-month period)

²⁶⁰ Indrabati Lahiri, 'Which European Countries Have the Highest and Lowest Salaries?' (*Euronews*, 24 November 2023) <<https://www.euronews.com/business/2023/11/24/switzerland-and-iceland-highest-payers-across-the-eu-and-eea>> accessed 11 May 2024.

²⁶¹ European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) p. 40.

²⁶² Directorate-General for Communication, 'Justice and Fundamental Rights – European Union' <https://european-union.europa.eu/priorities-and-actions/actions-topic/justice-and-fundamental-rights_en> accessed 11 May 2024.

²⁶³ European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) p. 3.

²⁶⁴ DSK 'Bewertung von Pur-Abo-Modellen auf Websites' (n 19) p. 1.

²⁶⁵ Eugen Rochko, 'Annual Report 2022' (*Mastodon Blog*, 2 October 2023) <<https://blog.joinmastodon.org/2023/10/annual-report-2022/>> accessed 11 May 2024.

²⁶⁶ 'Meta Earnings Presentation Q3 2023' (*Meta*, 2023) <https://s21.q4cdn.com/399680738/files/doc_earnings/2023/q3/presentation/Earnings-Presentation-Q3-2023.pdf> accessed 15 April 2024.

on every user in Europe.²⁶⁷ This breaks down to roughly US\$5.33 a month per user.²⁶⁸ Considering Meta's initial monthly subscription rate of 9.99 euros (≈US\$10.71) was overpriced, this likely prompted the company to lower the rate to 5.99 euros (≈US\$6.42).²⁶⁹ However, factoring in minor fluctuations in the US dollar-to-euro conversion rate, Meta still imposes an excessive surcharge on users who opt out of behavioural advertising. Meta makes roughly US\$1.09 more on users who reject behavioural advertising than those who provide consent, suggesting the two versions of the online platform are not equivalent alternatives. To avoid fees that are inappropriately high, Meta must consider its profits from behavioural advertising when setting fees to ensure they are either equal or less than the company's monthly revenue per user.²⁷⁰

2.3.3. Detriment

2.3.3.1. Refusing Consent

The third consideration for freely given consent is detriment. Recital 42 of the GDPR states that consent cannot be regarded as freely given if the data subject "is unable to refuse or withdraw consent without detriment."²⁷¹ This provision illustrates how detriment focuses on two potential phases of the consent process: refusal and withdrawal. When refusing consent, the Board argues users can only exercise freely given consent when "there is no risk of deception, intimidation, coercion, or significant negative consequences (e.g. substantial extra costs) if he/she does not consent."²⁷² The Board did not clarify the meaning of substantial extra costs, but inappropriately high subscription fees would likely qualify as detrimental because users who refuse behavioural advertising endure an economic disadvantage compared to those who provide consent. This disadvantage likely pressures users to avoid the fee and agree to data processing, which contradicts the essence of freely given consent. The AEPD supported this rationale in a case involving a bank customer seeking to withdraw consent for data processing related to promotions and personalised advertisements.²⁷³ More specifically, the AEPD concluded that requiring the individual to pay a higher maintenance fee after withdrawing consent was detrimental and violated the principle of freely given consent.²⁷⁴ This violation stemmed from fee exemptions being conditional on consent for data processing that was not necessary for contract performance.²⁷⁵ In the context of pay-or-okay models, the AEPD's finding suggests that

²⁶⁷ *ibid* p. 15.

²⁶⁸ *ibid*.

²⁶⁹ Chee, 'Meta Offers to Almost Halve Facebook and Instagram Monthly Fees' (n 256).

²⁷⁰ European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) para 85.

²⁷¹ GDPR, recital 42.

²⁷² European Data Protection Board, 'Guidelines 05/2020 on consent' (n 33) para 24.

²⁷³ AEPD (n 21).

²⁷⁴ *ibid* p. 101.

²⁷⁵ *ibid* p. 104.

requiring users to pay higher fees for refusing or withdrawing consent constitutes a detriment under Recital 42 of the GDPR.

To better understand the meaning of detriment, it is worth discussing whether freely given consent can be achieved when refusing consent leads to negative consequences. The Board has argued that “where a clear imbalance of power exists, consent can only be used in ‘exceptional circumstances’ and where the controller... can prove there are ‘no adverse consequences at all.’”²⁷⁶ This absolute wording suggests any negative impact on users for refusing consent contradicts the conception of freely given consent. Additionally, this statement places the burden of proof on the controller to illustrate that no adverse consequences exist. The statement’s conclusion that consent can only be used in exceptional circumstances depends on whether a clear imbalance of power exists. The Board has argued that large online platforms like Meta “may be uniquely situated in respect of... the existence of an imbalance of power.”²⁷⁷ While the Board’s language is cautious, it suggests that large online platforms like Meta typically create an imbalance of power inconsistent with freely given consent. However, this imbalance of power may be less evident for smaller online platforms, resulting in a broader use of consent beyond exceptional circumstances.

When determining the legality of pay-or-okay models for smaller online platforms, it is important to challenge the Board’s determination that no adverse consequences at all can exist when users refuse consent.²⁷⁸ According to the European Union Agency for Fundamental Rights and Council of Europe, circumstances exist when refusing consent can be valid despite having some negative consequences.²⁷⁹ For example, the Agency clarified that customers who refuse to participate in a supermarket’s loyalty program would forgo the benefit of small price reductions in goods, but their consent to join the loyalty program would remain a valid legal basis for data processing. The Agency also argued that when “the consequences of not consenting are not serious enough to prevent the data subject’s free choice,”²⁸⁰ then consent remains a valid legal basis. The AEPD rejected the Agency’s argument when dealing with a case that did not concern a customer loyalty program,²⁸¹ suggesting the agency’s argument should be interpreted narrowly. However, in a similar customer loyalty program case, the German Federal Court of Justice argued situations with an excessive financial incentive render freely given consent impossible, but customer loyalty programs are “not subject to any such economic coercion.”²⁸² Therefore, in the context of pay-or-okay models, it is important to evaluate fee appropriateness for signs of excessive economic influence or coercion. As the ultimate authority on interpreting EU provisions and

²⁷⁶ European Data Protection Board, ‘Opinion 08/2024 on Valid Consent’ (n 178) para 79.

²⁷⁷ *ibid* p. 12.

²⁷⁸ *ibid* para 79.

²⁷⁹ European Union Agency for Fundamental Rights and Council of Europe (n 46) 45.

²⁸⁰ *ibid*.

²⁸¹ AEPD (n 21) p. 103.

²⁸² Bundesgerichtshof [The Federal Court of Justice of Germany], Urteil vom 16 July 2008, VIII ZR 348/06.

their legality, the CJEU should determine when subscription fees constitute a detriment under Recital 42 of the GDPR.

2.3.3.2. Withdrawing Consent

For withdrawing consent, both Recital 42 and Article 7(3) of the GDPR are applicable. Article 7(3) stipulates that “it shall be as easy to withdraw as to give consent.”²⁸³ Although consenting to Meta’s behavioural advertising scheme can be done with a single click, refusing consent requires a “longer and more cumbersome payment process.”²⁸⁴ Users wishing to withdraw consent also need to successfully navigate through several windows.²⁸⁵ The Board previously established that controllers cannot force users to read through additional pages to reach a decline button for cookie banners, and this reasoning should apply when users withdraw consent for pay-or-okay models.²⁸⁶ By mandating the input and removal of payment details, Meta imposes a disproportionate burden on users wishing to avoid personal data processing for behavioural advertising. Reinforcing this point, the Council of Europe’s explanatory report on Convention 108 concerning personal data processing explains “no undue influence or pressure (which can be of an economic or other nature) whether direct or indirect, may be exercised” for freely given consent to exist.²⁸⁷ Given both the economic disadvantage and disproportionate burden placed on users wishing to withdraw consent, Meta’s pay-or-okay model does not comply with the detriment consideration. Additionally, Meta initially did not adopt a pay-or-okay model but subsequently introduced one, potentially worsening the negative financial consequences on long-term users.²⁸⁸ To determine whether pay-or-okay models constitute a detriment under the GDPR, fee appropriateness and the clarity, ease, and speed of the withdrawal process must be evaluated for each online platform.

2.3.3.3. Freedom to Conduct a Business

When considering whether subscription fees constitute a detriment under the GDPR, it is worth analysing the counterargument that pay-or-okay models are legally justified under Article 16 of the Charter. Article 16 stipulates that “the freedom to conduct a business in accordance with Community law and national laws and practices is recognized.”²⁸⁹ Several business stakeholders including Interactive Advertising Bureau (IAB) Europe and Alliance

²⁸³ GDPR, art 7(3).

²⁸⁴ European Data Protection Board, ‘Opinion 08/2024 on Valid Consent’ (n 178) footnote 90.

²⁸⁵ Alessia Sophia D’Amico and others, ‘Meta’s Pay-or-Okay Model: An Analysis Under EU Data Protection, Consumer, and Competition Law’ (28 March 2024) Utrecht University School of Law Series 2, 8.

²⁸⁶ European Data Protection Board, ‘Report of the work undertaken by the Cookie Banner Taskforce’ (17 January 2023) para 8.

²⁸⁷ Council of Europe, ‘Convention 108+ Convention for the protection of individuals with regard to the processing of personal data’ (June 2018) p. 20.

²⁸⁸ European Data Protection Board, ‘Opinion 08/2024 on Valid Consent’ (n 178) para 90.

²⁸⁹ The Charter (n 12) art 16.

Digitale have made this argument and implored the Board to uphold pay-or-okay models as standard business practices.²⁹⁰ According to the Explanation to the Charter, Article 16 should be interpreted based on relevant CJEU case law recognising the freedom to exercise economic activity, amend contracts, and uphold free competition.²⁹¹ More specifically, four CJEU cases are listed that discuss “the carrying on of economic activities,”²⁹² how contractual freedom cannot be limited “in the absence of Community rules,”²⁹³ people’s right to freely choose and “practice their trade or profession,”²⁹⁴ and how “the common organization of the market does not preclude”²⁹⁵ state action. Although none of these cases discuss personal data processing, the ECJ more recently held that privacy and data protection rights “override, as a rule, a controller’s economic interests.”²⁹⁶ Privacy and data protection rights may need to be balanced against other EU values including freedom of press, human rights, and national security, but they will prevail over the economic interests of online platforms like Meta. Therefore, pay-or-okay models are not automatically admissible under Article 16 of the Charter and must be assessed on a case-by-case basis to ensure adherence to the GDPR’s requirements for freely given consent.

2.3.3.4. Limitations Under Article 52(1) of the Charter

If pay-or-okay models are construed as limitations on privacy and data protection rights, then it is important to examine them within the framework of Article 52(1) of the Charter. This Article outlines the scope of rights and allows for limitations that are both based in law and respect the nature of other rights and freedoms.²⁹⁷ NOYB has argued that monetising the right to data protection via a pay-or-okay model requires a legal basis under Article 52(1), but no legal basis exists because “the GDPR does not provide for a payment burden for the refusal of consent.”²⁹⁸ Even if such a legal basis existed, it would need to be examined for its necessity (i.e., whether the data processing is strictly necessary for the purpose of processing) and proportionality (i.e., striking a balance between the means used and the intended goal).²⁹⁹ Although the GDPR does not explicitly allow for pay-or-okay models, they are not

²⁹⁰ Interactive Advertising Bureau (IAB) Europe, IAB Italia, IAB Spain, and Alliance Digitale (n 11).

²⁹¹ Explanations relating to the Charter of Fundamental Rights [2007] OJ C 303 art 16.

²⁹² *S.p.A. Eridania-Zucherifici Zazionali and others v. Minister of Agriculture and Forestry and others* (Case C-219/95) [1979] ECLI:EU:C:1979:216 [20].

²⁹³ *Kingdom of Spain v Commission of the European Communities* (Case 240-/97) [1999] ECLI:EU:C:1999:479 [99].

²⁹⁴ *J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities* (Case 4-73) [1974] ECLI:EU:C:1974:51.

²⁹⁵ *Sukkerfabriken Nykøbing Limiteret v Ministry of Agriculture* (Case 151/78) [1979] ECLI:EU:C:1979:4 [19].

²⁹⁶ *Google Spain* (n 70) [97], [99].

²⁹⁷ The Charter (n 12) art 52(1).

²⁹⁸ NOYB- European Center for Digital Rights, ‘Complaint Under Article 77(1) GDPR’ (n 10) para 21.

²⁹⁹ The European Data Protection Supervisor, ‘Necessity & Proportionality’ (2020) <https://www.edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en#:~:text=Proportionality%20is%20a%20general%20principle,used%20and%20the%20intended%20aim> accessed 16 May 2024.

prohibited in principle unless they violate the requirements for valid and freely given consent. This rationale was upheld by Personvernemnda concerning Grindr's disclosure of personal data to advertising partners. In this case, Grindr, a social networking and dating application, provided a paid-subscription version and an advertisement-based free version to users. After finding that Grindr's paid-subscription version fulfilled freely given consent requirements, Personvernemnda reversed Datatilsynet's infringement fee and concluded "Grindr is under no obligation to provide its services free of charge."³⁰⁰ Unlike Meta, Grindr is not considered a gatekeeper under the DMA.³⁰¹ As a smaller online platform, Grindr is less likely to contradict the requirements for freely given consent (namely, imbalance of power). Overall, Personvernemnda's decision reinforced how companies can finance their operations via pay-or-okay models if they comply with the GDPR.

2.3.4. Granularity

The fourth consideration for freely given consent is granularity. Granularity stems from Recital 43 of the GDPR which stipulates that "consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations."³⁰² The phrase "presumed" suggests Recital 43 is not absolute and may be rebuttable. Supporting this point, the British DPA (ICO) suggested that "in some limited circumstances" consent can be validly obtained if granularity is not fulfilled.³⁰³ For example, ICO listed circumstances involving online services having a minimal privacy impact on data subjects and the controller having a reasonable argument for bundling data processing operations.³⁰⁴ However, this flexibility is restricted by Recital 32 of the GDPR which reinforces that "when processing has multiple purposes, consent should be given for all of them."³⁰⁵ The GDPR lacks guidelines for determining whether a processing purpose is specific, but mandates that personal data be collected for "specific, explicit, and legitimate purposes."³⁰⁶ Given this discretion, the DKS posits that data processing purposes differing significantly from one another should be obtained through granular consent whereas purposes that are very closely related can be bundled together.³⁰⁷ The ECJ has found that Meta's collection of off-Facebook data across several of the company's services and its personalisation of content is not necessary in order to offer users an online social network.³⁰⁸ Users must have the possibility of giving consent separately for off-Facebook data collection

³⁰⁰ The Norwegian Privacy Appeals Board (Personvernemnda) (n 20).

³⁰¹ European Commission, 'Digital Markets Act: Commission designates six gatekeepers' (n 214).

³⁰² GDPR, recital 43.

³⁰³ The Information Commissioner's Office (ICO), 'Consultation: GDPR consent guidance' (31 March 2017) <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed 5 May 2024 p. 20.

³⁰⁴ *ibid.*

³⁰⁵ GDPR, recital 32.

³⁰⁶ GDPR, art 5(b).

³⁰⁷ DSK, 'Bewertung von Pur-Abo-Modellen auf Websites' (n 19) p. 20.

³⁰⁸ *Facebook Inc.* (n 159) [102], [103].

and the personalisation of content given the scale and impact of this data processing on users.³⁰⁹ Ultimately, controllers like Meta are legally obligated to present personal data processing purposes clearly and specifically to obtain freely given consent from users.

2.3.4.1. Lack of Processing Information

Freely given consent cannot be obtained when online platforms provide a single consent request for numerous different data processing operations. For Meta's pay-or-okay model, these operations likely include storing personal data in terminal equipment and using cookies for frequency capping or analysing the effectiveness of advertisements.³¹⁰ Each of these operations is distinct and must be consented to separately to fulfil the granularity condition.³¹¹ In agreement, the Board argued users must be free to choose which data processing purposes they accept without being confronted with a single consent request.³¹² However, Meta currently presents the following two options to EU users:³¹³

Subscribe to use without ads

Subscribe to use your Facebook and Instagram accounts without ads, starting at €12,99/month (inclusive of applicable taxes). Your info won't be used for ads.

Use for free with ads

Discover products and brands through personalized ads, while using your Facebook and Instagram accounts for free. Your info will be used for ads.

[Your current experience]

These options combine all data processing operations for behavioural advertising into one consent request without considering the distinct technical dynamics involved – such as combining personal data from multiple sources, personalising content, developing services, and measuring audiences.³¹⁴ Additionally, it remains uncertain how Meta will use personal data for advertisements and whether they will continue employing native advertising.³¹⁵ Native advertising involves collecting personal data to present online users with

³⁰⁹ Ibid [151].

³¹⁰ European Data Protection Board, 'EDPB Reply to the Commission's Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalized advertising choices- DRAFT PRINCIPLES (Ref. Ares (2023)6863760)' (13 December 2023) <https://www.edpb.europa.eu/system/files/2023-12/edpb_letter_out20230098_feedback_on_cookie_pledge_draft_principles_en.pdf> accessed 10 May 2024, p. 7.

³¹¹ *Planet 49 GmbH v. Bundesverband der Verbraucherzentralen Und Verbraucherverbände-Verbraucherzentrale Bundesverband eV* (Case C-673/17) [2019] ECLI:EU:C:2019:246 [66].

³¹² European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) p. 4.

³¹³ Alessia Sophia D'Amico and others (n 285) p. 4.

³¹⁴ European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) para 140.

³¹⁵ NOYB- European Center for Digital Rights 'Complaint Under Article 77(1) GDPR' (n 10) p. 11.

personalised content via posts and videos by influencers. Overall, Meta’s pay-or-okay model does not fulfil the granularity consideration because it does not offer users clear, separate consent requests for the different personal data processing operations involved in behavioural advertising.

2.3.4.2. Incentivising

Besides Meta’s data processing options lacking information on how personal data is used for advertisements, it is important to assess whether Meta’s wording for option two (i.e., using Facebook and Instagram services for free) complies with the GDPR’s principles of transparency and fairness. These principles emanate from Articles 5, 12, and Recital 58 of the GDPR which stipulate that information from the controller must be clear, concise, plain, and easy to understand.³¹⁶ Considering the GDPR does not explicitly address incentives by controllers, the Board has argued the Regulation “does not preclude all incentives but the onus would be on the controller to demonstrate that consent was still freely given.”³¹⁷ In other words, user consent can be freely given if provided willingly, without negative pressure or coercion, but through persuasion. For instance, consent would be freely given when a user agrees to personal data processing to receive news updates on their local sports team, even if encouraged by a club official.³¹⁸ Additionally, the Board clarified that data processing options must be presented in an “objective and neutral way, avoiding any deceptive or manipulative language or design.”³¹⁹ The Board’s comments reveal the delicate balance between incentivising and coercing users in violation of the GDPR.

In Meta’s pay-or-okay model, option two employs language meant to persuade users to provide consent. For example, option two explains users can “discover products and brands” and remain with their “current experience”, which may discourage users from refusing consent and selecting an unfamiliar option. Acknowledging this reality, the European Parliament noted that large online platforms like Meta have been criticised for employing language and designs discouraging users from “choosing more privacy-friendly settings.”³²⁰ The Parliament also explained freely given consent can be compromised when financial pressure is placed on users to provide consent in return for discounts and commercial offers.³²¹ This financial pressure reignites debates on determining fee appropriateness and

³¹⁶ GDPR, recital 58.

³¹⁷ European Data Protection Board, ‘Guidelines 05/2020 on consent’ (n 33) para 48.

³¹⁸ Eleni Kosta, ‘Article 7. Conditions for Consent’ in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP: 2020) 351.

³¹⁹ European Data Protection Board, ‘Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognize and avoid them Version 2.0’ (14 February 2023) para 18.

³²⁰ Hendrik Mildebrath, ‘Briefing: The future of data protection and privacy: How the European Parliament is responding to citizens’ expectations’ (European Parliamentary Research Service, April 2022) <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729396/EPRS_BRI\(2022\)729396_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729396/EPRS_BRI(2022)729396_EN.pdf)> accessed 5 May 2024 p. 3.

³²¹ European Parliament Resolution 2020/2717(RSP) (n 176) para 6.

to what extent controllers can incentivise users to provide consent without it constituting deception, intimidation, or coercion. To ensure GDPR compliance, controllers like Meta should present data processing options neutrally and refrain from language encouraging behavioural advertising.

2.4. Recommendations on Alternatives to Behavioural Advertising

Given the legal issues surrounding freely given consent raised by pay-or-okay models, it is worth outlining potential advertising alternatives for Meta and other online platforms to improve GDPR compliance moving forward. Although the Board explained large online platforms can generally not obtain freely given consent for behavioural advertising, it mentioned the possibility of introducing a third option beyond the two binary options offered by pay-or-okay models (i.e., paying a fee or consenting to personal data processing for behavioural advertising).³²² This third option involves offering a free, equivalent alternative online service without behavioural advertising that processes less or no personal data.³²³ Some feasible advertising methods that process no personal data include contextual advertising, product placement, and freemium models. While behavioural advertising processes personal data based on users' previous actions (e.g., liking a post or clicking on an advertisement), contextual advertising provides advertisements that align with users' interests without processing personal data. These advertisements appear based on the content or page a user is currently viewing.³²⁴ For example, behavioural advertising may process personal data to identify a user's interest in perfume. The online platform could display a perfume advertisement on a page about cars whereas contextual advertising would show car-related advertisements on that same page. Another advertising alternative that processes no personal data includes product placement whereby content creators feature and endorse products in their photos or videos. A third alternative to behavioural advertising includes freemium models which offer basic services for free and additional services for a fee, similar to LinkedIn. Overall, these three advertising methods do not involve processing users' personal data, allowing online platforms like Meta to finance their services without implicating or violating the GDPR's requirements for freely given consent.

Conclusion

This working paper addressed the legal issues surrounding pay-or-okay models in the EU. More specifically, this study asked: what legal issues surrounding freely given consent do pay-or-okay models create under the GDPR? This question was worth asking given the disagreements between NGOs, companies, and DPAs on the legality of pay-or-okay models. Although the Board issued an opinion on Meta's pay-or-okay model in April 2024, it

³²² European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) p. 3.

³²³ *ibid* para 181.

³²⁴ Laura Kloot, 'The Beginner's Guide to Contextual Advertising' (*Outbrain*, 24 October 2023)

<<https://www.outbrain.com/blog/the-beginners-guide-to-contextual-advertising/>> accessed 12 May 2024.

employed cautious language and only addressed large online platforms. Reinforcing the opinion's shortcomings, NOYB explained the Board "decided largely in a vacuum without independence and comprehensive evidence of how pay-or-okay models interfere with users' genuine and free choice."³²⁵ Therefore, the question remains whether pay-or-okay models for online platforms of different sizes can meet the GDPR's legal requirement for freely given consent. This working paper argued that in principle the GDPR does not prohibit pay-or-okay models, but controllers must prove that freely given consent has been obtained for personal data processing for behavioural advertising.

Before analysing the four considerations for freely given consent for pay-or-okay models under the GDPR, this working paper outlined the EU's legal framework for data protection along with the legal bases under Article 6 of the GDPR which Meta previously relied upon for personal data processing. The EU's legal framework for data protection primarily stems from the Charter, TFEU, GDPR, ePrivacy Directive, and Regulation (EC) No. 45/2001. As the central piece of EU secondary law on data protection, the GDPR was compared to its predecessor, the 1995 Directive. Beyond the transposition distinction between both pieces of legislation, the GDPR imposes a stronger extraterritorial scope, defines personal data breach, increases fines for controllers, implements stricter consent requirements, and streamlines communication between controllers, processors, and data subjects compared to the 1995 Directive. As for pre-GDPR case law and opinions on consent, the ECJ and DPAs have emphasised that consent for personal data processing must be freely given, uncoerced, informed, obtained separately for different purposes, and feature adequate opt-out procedures. Additionally, the Court found that DPAs outside of Ireland can investigate Meta's compliance with national data protection laws given its subsidiary establishments across the EU. As for Meta's previous legal bases for personal data processing, the Board and ECJ struck down both Meta's contract model under Article 6(1)(b) and its legitimate interest model under Article 6(1)(f) of the GDPR. This outcome prompted Meta to implement its pay-or-okay model under Article 6(1)(a) of the GDPR in November 2023.

Next, this working paper interpreted and analysed the four considerations for freely given consent under the GDPR: imbalance of power, conditionality, detriment, and granularity. Following the CJEU's interpretation method, this working paper employed a grammatical-teleological interpretation of the considerations for freely given consent by considering their wording and the GDPR's overall objective to safeguard the free movement and protection of personal data. Additionally, this working paper referenced EU primary law, secondary law, and other legal sources, such as WP29 opinions, Board opinions and guidelines, and DPA cases, to better understand the legal context surrounding pay-or-okay models. As online

³²⁵ NOYB- European Center for Digital Rights, 'EDPB Opinion: Meta cannot rely on "Pay or Okay"' (n 17).

platforms across the EU increasingly adopt pay-or-okay models, this working paper offered legal insights into how these models fare under the GDPR.

The first consideration for freely given consent includes potential power imbalances between the controller and the data subject. The Board has argued that power imbalances should be assessed based on the online platform's market position, the existence of lock-in or network effects, the data subject's reliance on the service, and the service's main audience.³²⁶ Determining whether smaller online platforms create power imbalances will likely be more challenging given the subtler network and lock-in effects compared to larger online platforms. This reality reinforces the importance of analysing online platforms on a case-by-case basis. When gauging network and lock-in effects, it is important to consider variations in social network participation across different EU member states. Additionally, power imbalance discussions should prioritise an online platform's market dominance and revenue over individual reliance on the service because the former is more easily quantifiable. As for the service's main audience, power imbalance discussions should prioritise the functionalities of online platforms over their target audience, as tracking demographic usage can be unreliable. Overall, the ECJ has reinforced the controller's responsibility under the GDPR to evaluate on a case-by-case basis whether an imbalance of power exists with the data subject.³²⁷

The second consideration for freely given consent is conditionality. According to the Board, conditionality concerns "whether consent is required to access goods or services, even though the processing is not necessary for the fulfilment of the contract."³²⁸ This consideration stems from Article 7(4) of the GDPR and aims to maintain transparency between the controller and the data subject. A grammatical-teleological interpretation of Article 7(4) suggests controllers should carefully ask data subjects for consent. Additionally, this interpretation method suggests the necessity of personal data processing should be understood narrowly as one of numerous factors for determining freely given consent. For Meta's pay-or-okay model, users can only access Facebook and Instagram services if they consent to behavioural advertising or pay a monthly fee. However, the ECJ determined behavioural advertising is not strictly necessary for Meta's contract performance.³²⁹ Therefore, users should have the ability to refuse non-necessary data processing operations. To make this a possibility, the ECJ concluded users are to be offered "if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations".³³⁰ This working paper argued the ECJ's ambiguity surrounding fee appropriateness underscores the need to consider the diverse financial circumstances of

³²⁶ European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) p. 3.

³²⁷ *Facebook Inc.* (n 159) [102]-[104], [149].

³²⁸ European Data Protection Board, 'Opinion 08/2024 on Valid Consent' (n 178) p. 3.

³²⁹ *Facebook Inc.* (n 159) [149].

³³⁰ *ibid* [150].

users, impact of fees on consent rates, cumulative financial burdens on users if pay-or-okay models proliferate across the market, average income across EU Member States, and controller's profits from behavioural advertising.

The third consideration for freely given consent is detriment, meaning data subjects must be able to refuse or withdraw consent without excessive negative consequences. In the context of pay-or-okay models, this working paper argued inappropriately high subscription fees would qualify as detrimental because users who refuse behavioural advertising would endure a financial disadvantage compared to those providing consent. However, this working paper highlighted a discrepancy between the Board's conclusion that no adverse consequences can arise from refusing or withdrawing consent and the EU Agency for Fundamental Rights' argument that limited negative consequences do not invalidate freely given consent such as foregoing discounts in supermarket loyalty programs. Given this discrepancy, this working paper reinforced the importance of assessing fee appropriateness to detect signs of excessive economic influence or coercion, which violates the GDPR. When it comes to withdrawing consent, Article 7(3) of the GDPR stipulates that "it shall be as easy to withdraw as to give consent."³³¹ Meta's pay-or-okay model does not satisfy the detriment consideration because the withdrawal process involves navigating multiple pages and removing payment details. Online platforms must ensure users can refuse or withdraw consent from pay-or-okay models as easily as they can provide consent.

Additionally, this working paper refuted counterarguments that pay-or-okay models are justified under Articles 16 and 52(1) of the Charter. Article 16 of the Charter concerns the freedom to conduct a business, and several business stakeholders including IAB Europe and Alliance Digitale have argued pay-or-okay models should be allowed as standard business practices.³³² According to the Explanation to the Charter, Article 16 should be interpreted based on relevant CJEU case law recognising the freedom to exercise economic activity, amend contracts, and uphold free competition.³³³ However, no CJEU cases listed in the Explanation to the Charter concern personal data processing, and the Court more recently found that data protection rights "override, as a rule, a controller's economic interests."³³⁴ Secondly, Article 52(1) stipulates that any limitation on the exercise of rights and freedoms in the Charter must be based in law and respect the essence of those rights and freedoms.³³⁵ If pay-or-okay models are construed as limitations to the right to data protection in Article 8 of the Charter, then they must be based in law, respect the right's essence, and fulfil necessity and proportionality requirements. However, the GDPR does not justify financial burdens for the refusal of consenting to data processing operations. Linking the right to data protection

³³¹ GDPR, art 7(3).

³³² IAB Europe, IAB Italia, IAB Spain, and Alliance Digitale (n 11).

³³³ Explanations relating to the Charter of Fundamental Rights (n 291).

³³⁴ *Google Spain* (n 70) [97], [99].

³³⁵ The Charter (n 12) art 52(1).

to money also undermines its essence, turning data into a commodity accessible only to those who can afford subscription fees. Therefore, pay-or-okay models cannot reasonably be accommodated under Articles 16 or 52(1) of the Charter.

Finally, the fourth consideration for freely given consent is granularity, meaning data subjects must have the ability to consent to different data processing operations separately. This consideration is found in Recital 43 of the GDPR. A grammatical-teleological interpretation of Recital 43 suggests consent is presumed not to be freely given when separate consent is not offered, indicating a non-absolute condition that may be contested under specific circumstances. However, the ECJ has found that Meta's personalisation of content and collection of personal data across different company-owned service platforms, such as Facebook, Instagram, and WhatsApp, is not necessary for contract performance and requires separate consent.³³⁶ Granularity is closely linked to the requirement of informed consent, and Meta's pay-or-okay model presents two options for personal data processing that lack important information on how personal data is collected and used. Additionally, Meta's second option employs language that persuades users to provide consent given the alleged benefits of behavioural advertising. This practice falls between incentivising users and coercing users – the latter of which the GDPR prohibits under a grammatical-teleological interpretation of Article 4(11) GDPR which stipulates that consent must be “freely given, specific, informed, and unambiguous”.³³⁷ Overall, pay-or-okay models must provide sufficient, neutral information that allow data subjects to consent to different data processing operations.

In conclusion, this working paper found pay-or-okay models can be legally justified if they fulfil the four considerations for freely given consent under the GDPR. However, large online platforms like Meta will likely face greater challenges fulfilling these considerations than smaller online platforms. Differences between online platforms reinforce the importance of analysing GDPR compliance on a case-by-case basis. Given the legal issues surrounding freely given consent raised by pay-or-okay models under the GDPR, this working paper discussed how contextual advertising, product placement, and freemium models are potential advertising alternatives that process no personal data. In the future, the Board is expected to release another decision on pay-or-okay models for smaller online platforms.³³⁸ In preparation, the Board should consult the operators of online platforms, business stakeholders, NGOs, competition law authorities in Member States, DPAs, the EU Parliament, and the EU Commission to gather all the necessary facts to render an informed decision. As for future research, scholars should examine Meta and the Irish DPC's anticipated appeals against the Board's April 2024 decision regarding large online platforms. Additionally, future research should examine how the proliferation of pay-or-okay models across the EU is

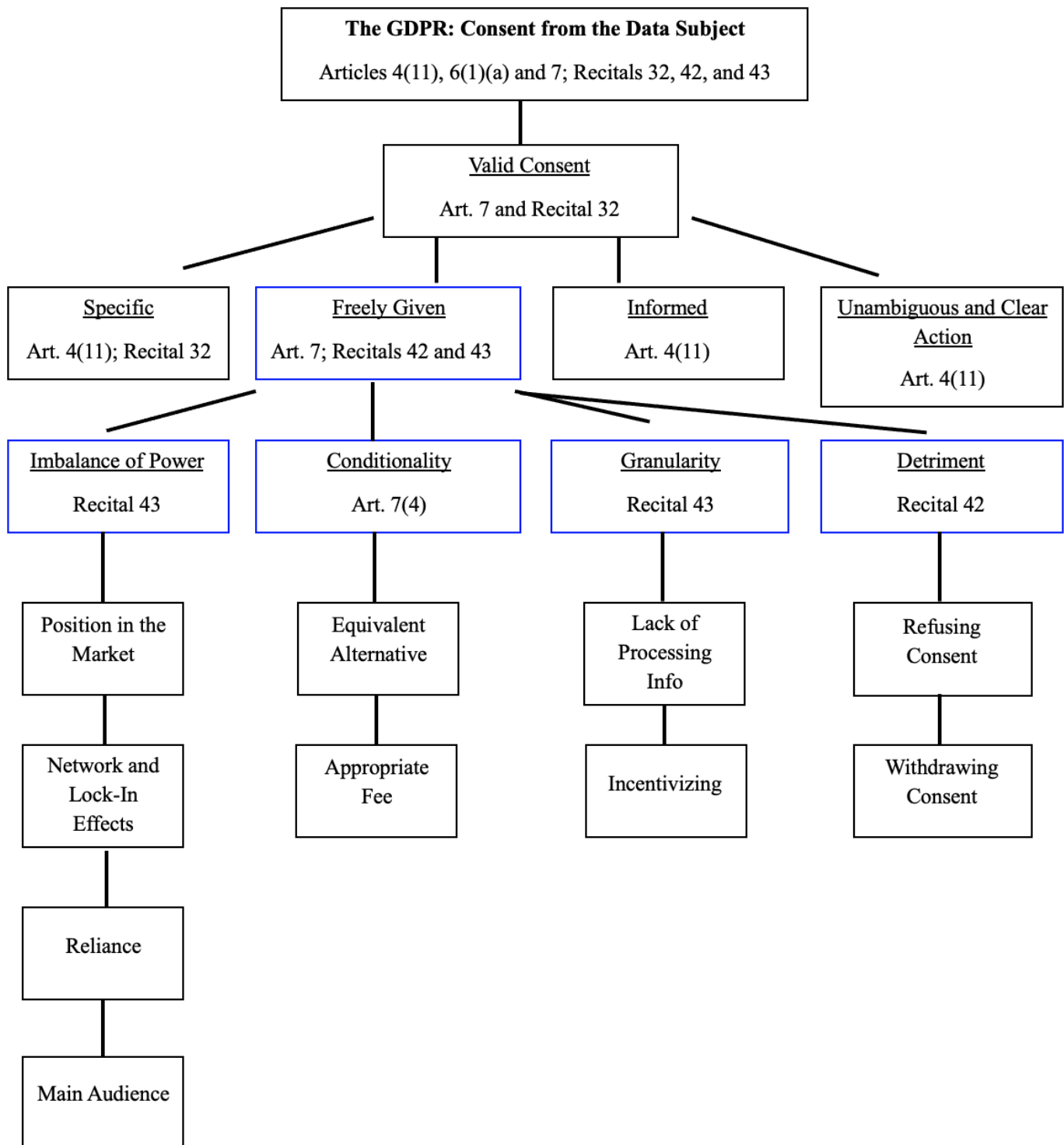
³³⁶ *Facebook Inc.* (n 159) [102]-[103], [151].

³³⁷ GDPR, art 4(11).

³³⁸ NOYB- European Center for Digital Rights, 'EDPB Opinion: Meta cannot rely on "Pay or Okay"' (n 17).

affected by the Boards' decisions. Overall, the GDPR's aim to safeguard and facilitate the free flow of personal data must be prioritised to prevent fundamental data protection rights from being commodified via pay-or-okay models contrary to freely given consent.

Annex



BIBLIOGRAPHY

Books

1. Aljanati L, 'Multilingual interpretation by the CJEU in the Area of Freedom, Security, and Justice' in Anne Lise Kjaer and Joanna Lam (eds), *Language and Legal Interpretation in International Law* (OUP 2022)
2. European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (2018 edn, Imprimerie Centrale Luxembourg 2018)
3. Kestemont L, *Handbook on Legal Methodology: From Objective to Method* (Intersentia 2018)
4. Kosta, E, 'Article 7. Conditions for Consent' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP: 2020)
5. Tridimas T, 'Precedent and the Court of Justice: A Jurisprudence of Doubt?' in Julie Dickson and Pavlos Eleftheriadis (eds), *Philosophical Foundations of European Union Law* (OUP 2012)

Journal Articles

1. Brunnermeier M and Landau JP, 'The digital euro: policy implications and perspectives' (European Parliament Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, January 2022) < [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703337/IPOL_STU\(2022\)703337_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703337/IPOL_STU(2022)703337_EN.pdf)> accessed 10 May 2024
2. D'Amico AS, Pelekis D, Santos C, and Duivenvoorde B, 'Meta's Pay-or-Okay Model: An Analysis Under EU Data Protection, Consumer, and Competition Law' (28 March 2024) Utrecht University School of Law Series <<https://papers.ssrn.com/abstract=4787609>> accessed 12 May 2024
3. De Bruin R, 'A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence' [2022] SSRN Electronic Journal <<https://www.ssrn.com/abstract=4251540>> accessed 20 April 2024
4. Houser K and Voss G, 'GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?' (2018) 25 RICH. J.L. & Tech < <https://jolt.richmond.edu/gdpr-the-end-of-google-and-facebook-or-a-new-paradigm-in-data-privacy/> > accessed 9 May 2024
5. Klimas T and Vaiciukaite J, 'The Law of Recitals in European Community Legislation' (14 July 2008) <<https://papers.ssrn.com/abstract=1159604>> accessed 9 May 2024

6. Zuiderveen Borgesius F, Kruikemeier S, Boerman S, and Helberger N, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' (15 March 2018) <<https://papers.ssrn.com/abstract=3141290>> accessed 7 May 2024

Online Websites and Articles

1. Bilton N, 'Price of Facebook Privacy? Start Clicking' *The New York Times* (12 May 2010) <<https://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html>> accessed 10 May 2024
2. Cabrera L and Maréchal N, 'The European Data Protection Board's Opinion on "Pay or Okay" Models – Surveillance-Based Advertising Is on Borrowed Time' (*Center for Democracy and Technology*, 10 May 2024) <<https://cdt.org/insights/the-european-data-protection-boards-opinion-on-pay-or-okay-models-surveillance-based-advertising-is-on-borrowed-time/>> accessed 11 May 2024
3. Chee FY, 'Meta Offers to Almost Halve Facebook and Instagram Monthly Fees' (*Reuters*, 19 March 2024) <<https://www.reuters.com/technology/meta-offers-cut-facebook-instagram-monthly-fees-599-euros-2024-03-19/>> accessed 11 May 2024
4. Directorate-General for Communication, 'Court of Justice of the European Union' (*Official Website of the European Union*) <https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en> accessed 11 May 2024
5. Directorate-General for Communication, 'Justice and Fundamental Rights –European Union' <https://european-union.europa.eu/priorities-and-actions/actions-topic/justice-and-fundamental-rights_en> accessed 11 May 2024
6. Dixon S, "Meta: Quarterly Revenue in Europe 2024" (*Statista*, 26 April 2024) <<https://www.statista.com/statistics/745351/facebooks-quarterly-revenue-in-europe/>> accessed 11 May 2024
7. European Commission Press Release, 'Data Protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases' (European Commission, 4 July 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609> accessed 10 March 2024
8. Folger J, 'How to Make Money on Instagram 2024' [2024] *Time* <<https://time.com/personal-finance/article/how-to-make-money-on-instagram/>> accessed 11 May 2024

9. Folks A, 'Meta's new digs: A deep dive into practical considerations of consent' (IAPP, 9 January 2024) < <https://iapp.org/news/a/metass-new-digs-a-deep-dive-into-practical-considerations-of-consent> > accessed 8 May 2024
10. Gibbs S, 'Facebook's New Opt-out for Tracking Ads Is Not Enough, Says Privacy Expert' *The Guardian* (18 September 2015) <<https://www.theguardian.com/technology/2015/sep/18/facebooks-opt-out-tracking-ads-not-enough-privacy-expert>> accessed 10 May 2024
11. Gibbs S, 'Facebook "Tracks All Visitors, Breaching EU Law"' *The Guardian* (31 March 2015) <<https://www.theguardian.com/technology/2015/mar/31/facebook-tracks-all-visitors-breaching-eu-law-report>> accessed 10 May 2024
12. Grieco J, 'Data Privacy Hits Back Against Meta in 2023' (*MineOS*, 14 November 2023) <<https://www.mineos.ai/articles/data-privacy-hits-back-against-meta-in-2023>> accessed 8 March 2024
13. GDPR Resource Center, 'Derogations Tracker' (Latham & Watkins, 2024) < <https://gdpr.lw.com/Home/Derogations> > accessed 6 May 2024
14. GDPR.EU, 'Complete Guide to GDPR Compliance' (*Proton Technologies AG*, 2020) < <https://gdpr.eu> > accessed 10 March 2024
15. Indrabati Lahiri, 'Which European Countries Have the Highest and Lowest Salaries?' (*Euronews*, 24 November 2023) <<https://www.euronews.com/business/2023/11/24/switzerland-and-iceland-highest-payers-across-the-eu-and-eea>> accessed 11 May 2024
16. Interactive Advertising Bureau (IAB) Europe, IAB Italia, IAB Spain, and Alliance Digitale, 'Opinion on 'Pay or Okay' Models Requested from the EDPB by the Norway Protection Authority, Hamburg Supervisory Authority, and the Netherlands Supervisory Authority' (19 March 2024) < <https://iabeurope.eu/wp-content/uploads/20240319-Letter-to-EDPB-upcoming-opinion-and-guidelines-on-the-consent-or-pay-model.pdf> > accessed 11 March 2024
17. Irwin L, 'Irish DPC Challenges EDPB Jurisdiction in Meta Investigation' (*IT Governance Blog*, 23 March 2023) <<https://www.itgovernance.eu/blog/en/irish-dpc-challenges-edpb-jurisdiction-in-meta-investigation>> accessed 11 May 2024
18. Kloot L, 'The Beginner's Guide to Contextual Advertising' (*Outbrain*, 24 October 2023) <<https://www.outbrain.com/blog/the-beginners-guide-to-contextual-advertising/>> accessed 12 May 2024
19. McCarthy N, 'The Biggest GDPR Fines of 2023: The Financial Penalties for Breaching the GDPR Can Be Staggering, Running into Hundreds of Millions of Euro' (*EQS Group*,

- 16 January 2024) <<https://www.eqs.com/compliance-blog/biggest-gdpr-fines/>> accessed 9 May 2024
20. Mildebrath H, 'Briefing: EU Policies- Understanding EU data protection policy' (European Parliamentary Research Service, January 2023) <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI\(2022\)698898_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf)> accessed 5 May 2024
 21. Mildebrath H, 'Briefing: The future of data protection and privacy: How the European Parliament is responding to citizens' expectations' (European Parliamentary Research Service, April 2022) <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729396/EPRS_BRI\(2022\)729396_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729396/EPRS_BRI(2022)729396_EN.pdf)> accessed 5 May 2024
 22. Mukherjee S and Chee F, 'Meta Appeals against EU Gatekeeper Status for Messenger, Marketplace' *Reuters* (15 November 2023) <<https://www.reuters.com/technology/meta-appeals-against-eu-gatekeeper-status-messenger-marketplace-2023-11-15/>> accessed 11 May 2024
 23. 'Obiter Dictum' (*Oxford Reference*) <<https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100243515>> accessed 11 May 2024
 24. 'Ratio Decidendi' (*Oxford Reference*) <<https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100405351>> accessed 11 May 2024
 25. Rochko E, 'Annual Report 2022' (*Mastodon Blog*, 2 October 2023) <<https://blog.joinmastodon.org/2023/10/annual-report-2022/>> accessed 11 May 2024
 26. Simonite T, 'Google's New Street View Cameras Will Help Algorithms Index The Real World' *Wired* <<https://www.wired.com/story/googles-new-street-view-cameras-will-help-algorithms-index-the-real-world/>> accessed 10 May 2024
 27. Stone B, 'Google Says It Inadvertently Collected Personal Data' (*Bits Blog*, 1273869892) <<https://archive.nytimes.com/bits.blogs.nytimes.com/2010/05/14/google-admits-to-snooping-on-personal-data/>> accessed 10 May 2024
 28. '59% of EU Individuals Using Social Networks in 2023 - Eurostat' (*Eurostat*) <<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240319-1>> accessed 11 May 2024

Meta Sources

1. Egan E, 'Updating our Terms and Policies: Helping You Understand How Facebook Works and How to Control Your Information' (*Meta*, 13 November 2014) < <https://about.fb.com/news/2014/11/updating-our-terms-and-policies-helping-you-understand-how-facebook-works-and-how-to-control-your-information/>> accessed 9 May 2024
2. Facebook Help Center, 'Confirming Your Age on Facebook' (*Meta*, 2024) <<https://www.facebook.com/help/adsmanagerbuiltin/157793540954833>> accessed 11 May 2024
3. Meta Business Help Center, 'About Reaching New Audiences' (*Meta*, 2024) <https://www.facebook.com/business/help/717368264947302?id=176276233019487&helpref=page_content> accessed 10 March 2024
4. 'Meta Earnings Presentation Q3 2023' (*Meta*, 2023) < https://s21.q4cdn.com/399680738/files/doc_earnings/2023/q3/presentation/Earnings-Presentation-Q3-2023.pdf> accessed 15 April 2024
5. Meta Newsroom, 'Facebook to Establish International Headquarters in Dublin, Ireland' (*Meta*, 2 October 2008) < <https://about.fb.com/news/2008/10/facebook-to-establish-international-headquarters-in-dublin-ireland/>> accessed 10 May 2024
6. Meta Newsroom, 'Facebook and Instagram to Offer Subscription for No Ads in Europe' (*Meta*, 30 October 2023) < <https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>> accessed 10 March 2024
7. Meta Newsroom, 'Facebook Redesigns Privacy' (*Meta*, 26 May 2010) < <https://about.fb.com/news/2010/05/facebook-redesigns-privacy/>> accessed 9 May 2024
8. Meta Newsroom, 'How Meta Uses Legal Bases for Processing Ads in the EU' (*Meta*, 2023) <<https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/>> accessed 10 March 2024

NOYB- European Center for Digital Rights Sources

1. NOYB- European Center for Digital Rights, 'Breaking: Meta Prohibited from Use of Personal Data for Advertising' (*NOYB*, 4 January 2023) < <https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising>> accessed 10 March 2024
2. NOYB- European Center for Digital Rights, 'Complaint Under Article 77(1) GDPR' (*NOYB*, 28 November 2023) < <https://noyb.eu/sites/default/files/2023->

[11/Complaint%20-%20Meta%20Pay%20or%20Okay%20-%20REDACTED.pdf](#)> accessed 10 March 2024

3. NOYB-European Center for Digital Rights, 'Complaint pursuant to Article 80(1) GDPR against Meta Platforms Ireland Limited' (NOYB, 28 November 2023) < <https://noyb.eu/sites/default/files/2023-11/Complaint%20-%20Meta%20Pay%20or%20Okay%20-%20REDACTED.pdf>> accessed 10 May 2024
4. NOYB- European Center for Digital Rights, 'EDPB Opinion: Meta cannot rely on "Pay or Okay"' (NOYB, 17 April 2024) < <https://noyb.eu/en/statement-edpb-pay-or-okay-opinion>> accessed 17 May 2024
5. NOYB- European Center for Digital Rights, 'Instagram & Facebook: 28 Civil Rights Organizations Urge European DPAs to reject 'Pay or Okay' in Pending Case over €250 'privacy fee' (NOYB, 16 February 2024) <<https://noyb.eu/en/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta>> accessed 10 March 2024
6. NOYB- European Center for Digital Rights, 'Letter to the EDPB: 'Pay or Okay' and the end of 'genuine and free' choice' (NOYB, 16 February 2024) https://noyb.eu/sites/default/files/2024-02/Pay-or-okay_edpb-letter_v2.pdf accessed 10 March 2024
7. NOYB -European Center for Digital Rights, 'Meta (Facebook, Instagram) Switching to 'Legitimate Interest' for Ads' (NOYB, 30 March 2023) <<https://noyb.eu/en/meta-facebook-instagram-switching-legitimate-interest-ads>> accessed 10 March 2024
8. NOYB- European Center for Digital Rights, '28 NGOs Urge EU DPAs to Reject "Pay or Okay" on Meta' (*Forced Consent & Consent Bypass*, 16 February 2024) <<https://noyb.eu/en/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta>> accessed 7 May 2024

European Data Protection Board Sources

1. European Data Protection Board, 'About the European Data Protection Board' (2024) https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en accessed 10 March 2024
2. European Data Protection Board, 'Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR)' (5 December 2022) < https://www.edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202205_ie_sa_whatsapp_en.pdf> accessed 10 March 2024
3. European Data Protection Board, 'Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its

Facebook service (Art. 65)' (13 April 2023) < https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_en>

4. European Data Protection Board, 'Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65)' (5 December 2022) < https://www.edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf>
5. European Data Protection board, 'EDPB Reply to the Commission's Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalized advertising choices- DRAFT PRINCIPLES (Ref. Ares (2023)6863760)' (13 December 2023) https://www.edpb.europa.eu/system/files/2023-12/edpb_letter_out20230098_feedback_on_cookie_pledge_draft_principles_en.pdf accessed May 10 2024
6. European Data Protection Board, 'Guidelines 03/2018 on the territorial scope of the GDPR (Article 3)- Version for public consultation' (16 November 2018) < https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf> accessed 10 March 2024
7. European Data Protection Board, 'Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognize and avoid them Version 2.0' (14 February 2023) < https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf> accessed 15 March 2024
8. European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (4 May 2020) < https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>
9. European Data Protection Board and European Data Protection Supervisor, 'Joint EDPB-EDPS contribution to the public consultation on the draft template relating to the description of consumer profiling techniques (Art. 15 DMA)' (20 September 2023) <https://www.edpb.europa.eu/system/files/2023-09/edps-edpb_comments_on_article_15_dma_template_report_for_plen_formatted.pdf> accessed 10 May 2024
10. European Data Protection Board, 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms' (17 April 2024) <

https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf> accessed 17 April 2024

11. European Data Protection Board, 'Report of the work undertaken by the Cookie Banner Taskforce' (17 January 2023) <https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf> accessed 10 May 2024
12. European Data Protection Board, 'Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR' (27 October 2023) <https://www.edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf> accessed 5 March 2024

Article 29 Working Party (WP29) Sources

1. Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (28 November 2017) < https://www.privacyworld.blog/wp-content/uploads/sites/41/2017/12/wp259_enpdf-Consent-draft-guidance.pdf> accessed 10 May 2024
2. Article 29 Working Party, 'Letter to Google' (16 October 2012) < https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf> accessed 5 May 2024
3. Article 29 Working Party, 'Opinion 2/2017 on data processing at work' WP 249 (8 June 2017) < <https://ec.europa.eu/newsroom/article29/items/610169>> accessed 5 May 2024
4. Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' (13 July 2011) 01197/II/EN WP187 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> accessed 4 May 2024

European Data Protection Supervisor (EDPS) Sources

1. The European Data Protection Supervisor, 'Necessity & Proportionality' (2020) < https://www.edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en#:~:text=Proportionality%20is%20a%20general%20principle,used%20and%20the%20intended%20aim> accessed 16 May 2024
2. The European Data Protection Supervisor, 'Opinion 8/2016 EDPS Opinion on Coherent enforcement of fundamental rights in the age of big data' (23 September

2016) < https://www.edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf> accessed 10 March 2024

3. The European Data Protection Supervisor, 'Preliminary Opinion- Privacy and competitiveness in the age of big data: The interplay between data protection, competition law, and consumer protection in the Digital Economy' (March 2014) < https://www.edps.europa.eu/sites/default/files/publication/14-03-26_competition_law_big_data_en.pdf> accessed 10 March 2024

International Conventions

1. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)
2. Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)

European Union Legislation

a. Treaties

1. The Charter of Fundamental Rights of the European Union (Charter) OJ 2010 C 83/389
2. Treaty on European Union (Maastricht Treaty) [1992] OJ C 191/35
3. Treaty on the Functioning of the European Union (TFEU) [2012] OJ C326
4. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community (Lisbon Treaty) [2007] OJ C306

b. Explanations on the Treaties

1. Explanations relating to the Charter of Fundamental Rights [2007] OJ C 303

c. Directives

1. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) [2002] *OJ L 201*
2. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004

on cooperation between national authorities responsible for the enforcement of consumer protection laws (ePrivacy Directive) [2009] OJ L 337

3. *EU Directive 95/46*: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (The 1995 Directive) OJ 1995 L 281/31

d. Regulations

1. *EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1
2. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L 008
3. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directive (EU) 2-19/1937 and (EU) 2020/1828 (Digital Markets Act) L 265/1

European Union Institutional Sources

a. The European Union Parliament

1. European Parliament Resolution 2020/2717(RSP) of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application [2021] <
https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EN.html>
2. European Parliament Resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020- Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems ('Schrems II') Case C-311/18 (2020/2789(RSP)) [2021] <
https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.pdf>

b. The European Commission

1. European Commission, 'Digital Markets Act: Commission designates six gatekeepers' (Press release, 6 September 2022) <
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328> accessed 10 May 2024

2. European Commission, 'Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (ePrivacy Regulation)' COM (2017) 10 final

c. Court of Justice of the European Union (CJEU) Sources

1. The Rules of Procedure of the Court of Justice (29 September 2012) L 265/1

Case Law

a. European Court of Justice (ECJ)

1. Aannemersbedrijf P.K. Kraaijeveld BV e.a. v Gedeputeerde Staten van Zuid- Holland (Case 72/ 95) [1996] EU:C:1996:404
2. Andy Wightman and Others v. Secretary of State for Exiting the European Union (Case C-621/18) [2018] ECLI:EU:C:2018:999
3. Aannemersbedrijf P.K. Kraaijeveld BV e.a. v Gedeputeerde Staten van Zuid- Holland (Case 72/ 95) [1996] EU:C:1996:404
4. Bank Melli Iran v. Telekom Deutschland GmbH (Case C-124/20) [2021] ECLI:EU:C:2021:1035
5. Bundesverband der Verbraucherzentralen Und Verbraucherverbände- Verbraucherzentrale Bundesverband eV v. Planet 49 GmbH (Case C-673/17) [2019] ECLI:EU:C:2019:801
6. Criminal Proceedings Against E. and F. (Case C-550/09) [2010] ECLI:EU:C:2010:382
7. DB v. Commissione Nazionale per le Società e la Borsa (Consob) (Case C-481/19) [2021] ECLI:EU:C:2021:84
8. Deutsche Telekom AG v Bundesrepublik Deutschland (Case C-543/09) [2011] ECLI:EU:C:2011:279
9. Facebook Inc. and Others v. Bundeskartellamt (Case C-252/21) [2023] ECLI:EU:C:2023:537
10. Ferriere Nord SpA v Commission of the European Communities (Case C-219/95 P) [1997] ECLI:EU:C:1997:375
11. Google LLC v. Commission nationale de l'informatique et des libertés (CNIL) (Case 24/62) [1963] ECLI:EU:C:2019:772

12. Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (Case C-131/12) [2014] ECLI:EU:C:2014:317
13. J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities (Case 4-73) [1974] ECLI:EU:C:1974:51
14. Kingdom of Spain v Commission of the European Communities (Case 240-/97) [1999] ECLI:EU:C:1999:479
15. Ligue des droits humains ASBL v. Conseil des Ministres (Case C-817/19) [2022] ECLI:EU:C:2022:491
16. Michael Schwarz v Stadt Bochum (Case C-291/12) [2013] ECLI:EU:C:2013:670
17. Parti écologiste 'Les Verts' v. European Parliament (Case 294/83) [1986] ECLI:EU:C:1986:166
18. Quelle AG v. Bundesverband der Verbraucherzentralen und Verbraucherverbände (Case C-404/06) [2008] ECLI:EU:C:2008:231
19. S.p.A. ERIDANIA-ZUCCHERIFICI NAZIONALI and others v Minister of Agriculture and Forestry and others (Case 230/78) [1979] ECLI:EU:C:1979:216
20. Sukkerfabriken Nykøbing Limiteret v Ministry of Agriculture (Case 151/78) [1979] ECLI:EU:C:1979:4
21. Tele2 (Netherlands) BV and Others v Autoriteit Consument en Markt (ACM) (Case C-536/15) [2017] ECLI:EU:C:2017:214
22. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (Case C-210/16) [2018] ECLI:EU:C:2018:388
23. Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen (Joined Cases C-92/09 and C-93/09) [2010] ECLI: EU:C:2010:662
24. WS v. Bundesrepublik Deutschland (Case C-505/19) [2021] ECLI:EU:C:2021:376

b. Germany

1. Bundesgerichtshof [The Federal Court of Justice of Germany] 'Urteil VIII ZR 348/06' (Verdict VII ZR 348/06) (16 July 2008) < <https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=b4cd648537288a85606ef99d9fbc6697&nr=45162&pos=3&anz=5>>
2. Landgericht Berlin [Berlin Regional Court] *The Federal Association of Consumer Centers and Consumer Associations- Federal Association of Consumer Organizations v*

Facebook Ireland Ltd. (16 Jan 2018) No. 16 O 341/15 <
https://www.vzbv.de/sites/default/files/downloads/2018/02/12/facebook_lg_berlin.pdf>

c. The United States of America

1. *Google Inc. Street View Electronic Communications Litigation* [2011] (United States District Court, N.D. California, San Francisco Division) 794 F. Supp. 2d 1067

National Legislation

a. France

1. Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 relating to data processing, files and freedoms] Légifrance [Official Gazette of France] 6 January 1978

b. Germany

1. Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei Datenverarbeitung (Bundesdatenschutzgesetz- BDSG) [Act to protect against misuse of personal data in data processing (Federal Data Protection Act-BDSG) 1 January 1977 BGBl

c. Sweden

1. Datalagen [The Swedish Data Act] SFS 1973:289

d. United States of America

1. U.S. Constitution [1787] amend. IV.

Advocate General (AG) of the Court of Justice of the European Union Opinions

1. Planet 49 GmbH v. Bundesverband der Verbraucherzentralen Und Verbraucherverbände-Verbraucherzentrale Bundesverband eV (Case C-673/17) [2019] ECLI:EU:C:2019:246

The Organization for Economic Cooperation and Development (OECD) Sources

1. The Organization for Economic Cooperation and Development, 'Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (OECD, 23 September 1980) <<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>> accessed 9 May 2024

The Council of Europe Sources

1. Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (28 January 1981) European Treaty Series No. 108
2. Council of Europe, 'Convention 108+ Convention for the protection of individuals with regard to the processing of personal data' (June 2018) < https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIB E/DV/2018/09-10/Convention_108_EN.pdf> accessed 10 May 2024

Data Protection Authority (DPA) Sources

a. Austria

1. The Data Protection Authority for Austria (Datenschutzbehörde), 'Decision on Cookie Banners' (Decided 29 March 2023) <[https://gdprhub.eu/index.php?title=DSB_\(Austria\)_-2023-0.174.027](https://gdprhub.eu/index.php?title=DSB_(Austria)_-2023-0.174.027)> accessed 6 May 2024
2. The Data Protection Authority for Austria (Datenschutzbehörde), 'FAQ zum Thema Cookies und Datenschutz (FAQ on Cookies and Data Protection)' (20 December 2023) < https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.html#Frage_9> accessed 6 May 2024

b. France

1. Commission nationale de l'informatique et des libertés [CNIL] 'Cookie walls: la CNIL publie des premiers critères d'évaluation (Cookie walls: the CNIL publishes first evaluation criteria)' (16 May 2022) < <https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation>> accessed 10 May 2024

c. Germany

1. Bundeskartellamt (BKartA) [Independent Competition Authority – Federal Cartel Office] 'Case Summary: Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing (6 February 2019) < https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4>
2. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit [The Hamburg Commissioner for Data Protection and Freedom of Information], 'Fine imposed upon Google: Ruling in the proceeding pursuant to Wifi scanning is legally binding' (22 April 2023) < https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Pressemitteilungen/2013/2013-04-22_Google-Wifi-Scanning_PressRelease.pdf> accessed 6 May 2024

3. The Committee of Independent German Federal and State Data Protection Supervisory Authorities (DSK), 'Bewertung von Pur-Abo-Modellen auf Websites' (DSK Privacy Conference, 22 March 2023) < https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf?trk=article-ssr-frontend-pulse_little-text-block> accessed 6 May 2024
4. The Committee of Independent German Federal and State Data Protection Supervisory Authorities (DSK), 'Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) (Guidance from the supervisory authorities on the processing of personal data for direct advertising purposes under the General Data Protection Regulation (GDPR)) (February 2022) < https://www.datenschutzkonferenz-online.de/media/oh/OH-Werbung_Februar%202022_final.pdf> accessed 10 May 2024

d. Ireland

1. Dixon H, 'Draft Decision for the purposes Article 60 of the GDPR of the Data Protection Commission made pursuant to Section 113(2)(a) of the Data Protection Act 2018' (DPC, 6 October 2021) < <https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf>> accessed 10 May 2024
2. The Data Protection Commission (DPC), 'Data Protection Commission announces conclusion of two inquiries into Meta Ireland' (DPC, 4 January 2023) <<https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland>> accessed 10 March 2024
3. The Office of the Data Protection Commissioner of Ireland, 'Report of Audit: Facebook Ireland Ltd' (21 December 2011) < <https://www.pdpjournals.com/docs/87980.pdf>> accessed 5 May 2024
4. The Data Protection Commission (DPC), 'Guidance Note: Legal Bases for Processing Personal Data' (DPC, December 2019) <<https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf>> accessed 23 May 2024.

e. Norway

1. The Norwegian Data Protection Authority (Datatilsynet), 'Datatilsynet følger med på nye løsninger' (8 November 2023) <<https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/datatilsynet-folger-med-pa-metas-nye-losning/>> accessed 6 May 2024

2. The Norwegian Privacy Appeals Board (Personvernemnda), 'Decision on Grindr's Disclosure of Personal Data Without Consent 20/02136-18' (27 September 2023) <<https://www.personvernemnda.no/pvn-2022-22>> accessed 5 May 2024
3. The Norwegian Data Protection Authority (Datatilsynet), 'Hvad siger reglerne? Cookie Walls (What do the rules say? Cookie Walls)' <<https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/cookies/cookie-walls>> accessed 11 May 2024
4. The Norwegian Data Protection Authority (Datatilsynet), 'Urgent and Provisional Measures- Meta' (14 July 2023) <https://www.datatilsynet.no/contentassets/36ad4a92100943439df9a8a3a7015c19/urgent-and-provisional-measures--meta_redacted.pdf> accessed 11 May 2024

f. Spain

1. Agencia Española de Protección de Datos (AEPD), 'Resolución de Procedimiento Sancionador (Numero Expediente: PS/00226/2020)' (2020) <<https://www.aepd.es/documento/ps-00226-2020.pdf>> accessed 5 May 2024

g. The United Kingdom

1. The Information Commissioner's Office (ICO), 'Call for Views on 'consent or pay' business models' (2024) <<https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-views-on-consent-or-pay-business-models/>> accessed 5 May 2024
2. The Information Commissioner's Office (ICO), 'Consultation: GDPR consent guidance' (31 March 2017) <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed 5 May 2024



University
of Glasgow



LEUPHANA
UNIVERSITÄT LÜNEBURG



INSTITUT
BARCELONA
ESTUDIS
INTERNACIONALS



UNIVERSITÉ
LIBRE
DE BRUXELLES



UNIVERSITY
OF TARTU

Radboud Universiteit



Co-funded by
the European Union