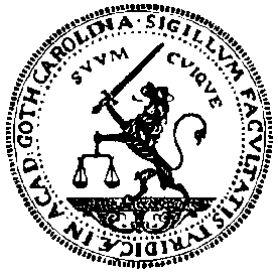

FACULTY OF LAW
Lund University

Gabbi Meskenaite

An examination of the criteria for valid consent under the GDPR in the light of the rationale and technological neutrality

LAGM01 Graduate Thesis

Graduate Thesis, Master of Laws program
30 higher education credits

Supervisor: Ulrika Wennersten

Semester of graduation: Period 2 Spring semester 2022

Contents

Summary

As a means to safeguard the fundamental right to data protection in light of the rapid advancement of use of technology and to address the fragmented implementation of data protection, the GDPR was introduced. For processing of personal data to be lawful under the GDPR, processing must have a legal basis, such as consent. The ePrivacy Directive establishes that consent is the only valid legal basis for certain processing purposes within the electronic communications sector, thus making the lawfulness of many processing activities dependent on consent. As consent is considered as the cornerstone of data protection, it is vital that the notion of valid consent is consistent with GDPR's dual rationale; the rationale encompasses the protection of fundamental rights, where data protection is central but not absolute, and the protection of the free movement of data within the European Union. Additionally, technological neutrality is a prerequisite for achieving modern legislation that can meet current needs. Without understanding the criteria for valid consent, compliance is challenging. By researching the requirements for valid consent as defined by the GDPR as well as how the criteria have been interpreted by both the CJEU and at national level, this thesis provides a teleological examination of the criteria in the light of the rationale and technological neutrality.

The GDPR establishes four cumulative criteria for valid consent: 'freely given', 'specific', 'informed' and 'unambiguous'. Freely given consent aims at rejecting consent that has been given under coercive circumstances that do not represent the data subject's own free will. Specific consent entails that consent has been given to a well-defined and granular purpose. The data subject must be provided with information that enables them to make an informed decision. Finally, there must not be any doubt as to whether the data subject intended to consent or not, thus requiring unambiguity in respect to the data subjects' intentions. The CJEU has provided some guidance on the criteria, especially on what is required for the criteria to be met when requesting consent using cookie banners. However, there is ambiguity in relation to the distinction of, and attribution to, the criteria. As the criteria leave room for interpretation, there is a level of discrepancy in interpretation and enforcement amongst Member States that gives rise to fragmentation, thus contravening harmonisation and free flow of data within the Union. As shown by several DPA decisions, notably the decision against IAB Europe's Transparency & Consent Framework in the European AdTech industry, entire technological solutions have been declared as unlawful; the ability to obtain consent has been virtually precluded despite consent being required as a legal basis. Such interpretation is thus not technologically neutral.

As the provisions are not practically possible to comply with, the legislation essentially fails with protecting the right to data protection. While further research is needed in order to assess the consequences on specific fundamental rights and freedoms, it can be noted that the current consent criteria might be problematic in relation to the various interests under the rationale.

While beyond the scope of the paper, it is suggested that the issues attributed to the interpretation of the criteria, in regard to the rationale, might be an issue of when consent is required rather than the essence of consent. Perhaps, in the light of the rationale and technological neutrality, the criteria for valid consent under the GDPR are neither good or bad, but rather dependant on the context and whether the limits of consent as the appropriate legal basis have been adequately considered.

Sammanfattning

I syfte att säkerställa den grundläggande rätten till skydd av data samt att motverka fragmenteringen av dataskyddsrätten inom EU infördes den allmänna dataskyddsförordningen, ’GDPR’. För att personuppgiftsbehandling ska vara tillåtet under GDPR, krävs det rättslig grund, exempelvis samtycke. För särskilda behandlingsändamål inom elektronisk kommunikation fastställer ePrivacy-direktivet att enbart samtycke utgör giltig rättslig grund, vilket innebär att samtycke är avgörande för lagligheten av särskilda behandlingsaktiviteter. Då samtycke anses vara en grundpelare i skyddet av data är det viktigt att samtycke är förenligt med GDPRs syfte att å ena sidan säkerställa fundamentala fri- och rättigheter, varav skydd av data är centralt, och att å andra sidan skydda den fria rörligheten av data inom EU. Vidare ställs det upp ett krav på teknologisk neutralitet för att säkerställa en modern lagstiftning som kan möta nutida behov. Utan förståelse för de krav som ställs för giltigt samtycke blir rättelse i enlighet med bestämmelsen utmanande. Genom att utreda samtyckeskraven som uttryckt av GDPR samt tolkningen av samtycke av dels EU-domstolen och dels av nationella myndigheter, möjliggörs en teleologisk undersökning av samtyckeskraven i ljuset av GDPRs syfte och teknologisk neutralitet.

GDPR ställer upp fyra kumulativa kriterier för giltigt samtycke innebärandes att samtycke måste vara frivilligt, specifikt, informerat och en otvetydig viljeyttring. Frivilligt samtycke åsyftar till att ge uttryck för en persons egen fria vilja genom att utesluta samtycke som givits under yttre påtryckning. Specifikt samtycke ställer upp ett krav på att syftet för behandlingen för vilken samtycke begärs är väldefinierat och avgränsat. Ett informerat beslut kräver att tillräcklig samt tydlig information presenteras före samtyckandet. Slutligen får det inte föreligga tvivel kring huruvida intentionen varit att samtycka. Medan EU-domstolen gett vägledning i vad som krävs för att uppfylla kriterierna, råder det fortsatt tvetydighet gällande avgränsningen och identifiering av kriterierna. Då det finns tolkningsutrymme föreligger det en diskrepans medlemsstater emellan. Detta ger upphov till fragmentering, vilket således motverkar harmonisering och fritt flöde av data inom unionen. Av nationella dataskyddsmyndigheters beslut, särskilt beslutet mot IAB Europes ramverk som reglerar stora delar av den digitala marknadsföringsindustrin inom EU, framgår det att hela metoder och tekniska lösningar omöjliggörs då kraven för giltigt samtycke har ansetts omöjliga att uppnå samtidigt som samtycke krävs enligt ePrivacy-direktivet. En sådan tolkning av samtycke kan inte anses teknologiskt neutral. Då tillämpningen av GDPR omöjliggörs, misslyckas en sådan tolkning av

samtycke dessutom med att säkerställa grundläggande fri- och rättigheter. Fastän vidare forskning krävs för att bedöma samtyckeskravens konsekvenser för specifika fri- och rättigheter, kan det noteras att samtyckeskraven i deras nuvarande bemärkelse kan vara problematiska i förhållande till GDPRs syften.

Även om det ligger bortom ramen för detta arbete, noteras att de problem som hänförs till tolkningen av samtyckeskraven avseende GDPRs syften, kan vara en fråga om när samtycke krävs. Det är möjligt att kriterierna för giltigt samtycke varken är bra eller dåliga i ljuset av GDPRs syften och teknologisk neutralitet, utan snarare beror på sammanhanget samt huruvida samtyckets lämplighet som rättslig grund har beaktats.

Abbreviations

Adtech	Advertising technologies
BEUC	The European Consumer Organisation
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CMPs	Consent Managing Platforms
CNIL	French data protection authority
Council	European Council
DMPs	Data Management Platforms
DPA	Data Protection Authority / Supervisory authority
DPD	Data Protection Directive (95/46/EC)
DSP	Demand Side Platform
EC	European Commission
EDPB	European Data Protection Board
EDPB Consent Guidelines	EDPB Guidelines 05/2020 on consent under the GDPR
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ePrivacy Directive	Directive 2002/58/EC
EU	European Union
GDPR	General Data Protection Regulation (2016/679)
GDPR Proposal	Proposal for the General Data Protection Regulation
IAB Europe	Interactive Advertising Bureau Europe
Parliament	European Parliament
RTB	Real-time bidding
SSP	Supply Side Platform
TCF	IAB Europe's Transparency & Consent Framework
TC String	Transparency & Consent String
TFEU	Treaty on the Functioning of the European Union
WP29	Article 29 Working Party

1 Introduction

1.1 Background

Information technologies[1] have an integral part of everyday life with everything from private communications to health care visits taking place in cyberspace. While the vast majority of Europeans access the internet on a daily basis, the inevitable trade-off of personal data is often overlooked.[2] Many businesses, most noticeably large companies such as Meta (Facebook), Alphabet (Google), Amazon, Apple and Microsoft, have built entire business models around consumer data, making it clear that personal data is a currency with indisputably significant value.[3] In the face of such amassing of remunerative assets, the need for protection of one's personal data has never been more evident. Under European Union ('EU') law, i.e., the Charter of Fundamental Rights of the European Union ('CFR') [4], protection of personal data is a fundamental right and freedom.[5] As a means to safeguard the right to data protection, the European Union's General Data Protection Regulation ('GDPR') [6] entered into force, setting up extensive requirements for the processing of personal data.

The GDPR lays down that processing of personal data must have a lawful basis, such as consent by the data subject. For consent to be valid, the GDPR lists several cumulative criteria that must be shown by the data controller prior to processing of personal data; consent must be freely given, specific, informed and unambiguous. Yet, data subjects' personal data is constantly processed without valid consent and perhaps without the knowledge of the data subject, despite such consent being required by law. During 2021, non-profit organisation 'noyb', led by lawyer and privacy activist Max Schrems, launched an action against website operators whose cookie[7] banners did not comply with the requirements for valid consent under the GDPR. Noyb filed

[1] The use of computers, or other similar devices, to create, process, store and exchange data.
[2] Eurostat, 'Internet use and activities', 2021.
[3] Napier et al., 'Modern Business Models Will Drive the Post-Pandemic World', MIT Sloan Management Review, 2020; R. Varadarajan, 'Customer information resources advantage, marketing strategy and business performance: A market resources based view', Industrial Marketing Management, 2020, pp. 89-97.
[4] Charter of Fundamental Rights of the European Union, 2000/C, 364/01.
[5] Article 8(1) CFR.
[6] General Data Protection Regulation 2016: 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.
[7] Cookies, as defined by C-673/17, are 'text files which the provider of a website stores on the website user's computer which that website provider can access again when the user visits the website on a further occasion, in order to facilitate navigation on the internet or transactions, or to access information about user behaviour'.

456 complaints with 20 different Data Protection Authorities ('DPAs') across the EU, with further rounds of compliance reviews coming up. The majority of the cookie banners that noyb picked up on did not offer an adequate 'reject' option, an easy way to withdraw consent and the banners were often designed in a deceptive manner.[8] In the beginning of 2022, the internet ecosystems reliance on consent as a valid legal basis was struck with another swing of reprimands; the Belgian Data Protection Authority ruled that the Transparency and Consent Framework used by the online advertising industry in the EU, does not comply with the provisions on consent under the GDPR, thus making most of the consent that users give on a daily basis invalid.[9]

With the ever-growing importance of online presence for EU citizens, an adequate protection of fundamental rights and freedoms in the realm of cyberspace is essential. While the GDPR establishes a high threshold for data processing, the provisions are often vague and difficult to interpret. The uncertainties and lack of guidance leaves businesses with large fines as their interpretations of e.g. valid consent turns out to be inaccurate.[10] Moreover, despite the GDPR intending to be modern, issues with assessing valid consent arise with new technologies as businesses struggle to properly apply the provisions into new and often complex data processing strategies.[11] Considering the daily processing, and the glaring value, of personal data, it is evident that a proper understanding of what valid consent truly connotes is essential for adequate protection of individuals' fundamental rights and freedoms; without understanding the requirements for valid consent, compliance might be challenging. After all, most people don't even notice that their personal data is being processed in an unlawful manner and their rights being abused on a daily basis. Securing the protection of rights as provided under the GDPR ultimately requires an understanding of what constitutes freely given, specific, informed and unambiguous consent, especially as consent is considered as the cornerstone of EU data protection law.[12]

[8] Noyb, 'More Cookie Banners to go: Second wave of complaints underway', 2022.
[9] DOS-2019-01377, Autorité de protection des données Gegevensbeschermingsautoriteit, Litigation Chamber, Concerning: Complaint relating to Transparency & Consent Framework, Decision on the merits 21/2022 of 2 February 2022.
[10] Brinnen & Westman, 'What's wrong with the GDPR? Description of the challenges for business and some proposals for improvement', 2019.
[11] FRA, 'Technological advances and data protection should go hand-in-hand', 2021.
[12] Kuner et al., 'The EU General Data Protection Regulation: A Commentary', 2020, p. 18, with reference to the Albrecht Report.

1.2 Purpose and research questions

The purpose of this thesis is to, in the light of the rationale and technological neutrality, examine the requirements for valid consent under the GDPR, specifically the four cumulative key criteria for consent to be: freely given, specific, informed and unambiguous.

In order to fulfil the purpose, the following sub-questions will be answered:

1. What constitutes valid consent as defined by the GDPR?
2. How has valid consent under the GDPR been interpreted by the CJEU?
3. How has valid consent under the GDPR been interpreted at Member State level?

1.3 Existing research and contribution

At the time of publishing (Summer of 2022), the GDPR has been in effect for approximately four years. As the regulation is relatively new there is little doctrinal research on the GDPR, especially on consent under the GDPR that provides authoritative interpretations. Most existing research on the GDPR has a rather general approach where not much room is given for specific provisions and concepts.[13] Albeit, there is some research on specific provisions such as the right to be forgotten, that briefly consider the requirements for consent under the GDPR.[14] While there is literature that focuses specifically on the requirements for consent under EU data protection laws, such material predates the GDPR.[15]

Withal, it is due to the lack of updated research focused on the requirements for valid consent under the GDPR, that this thesis takes form. By systematically assessing the criteria and presenting the findings, this thesis adds to the understanding of the GDPR, especially in the light of the rationale and notion of technological neutrality.

[13] E.g., IT Governance Privacy Team, 'EU General Data Protection Regulation (GDPR) - An implementation and compliance guide', 2020; Bieker, 'The Right to Data Protection - Individual and Structural Dimensions of Data Protection in EU Law', 2022; Sharma, 'Data Privacy And GDPR Handbook', 2020; Kuner et al. 2020.
[14] See Politou et al., 'Privacy and Data Protection Challenges in the Distributed Era', 2022.
[15] See Kosta, 'Consent in European Data Protection Law', 2013.

1.4 Methodology and Materials

When examining EU law, the European legal methodology is appropriate as it encompasses the singularity of the EU legal system that in contrast to most domestic legal systems is new and has a modest repertoire of legal doctrines. EU law tends to be reactive and context dependent, rather than anchored in a solid theoretical foundation.[16] Accordingly, particular for the European legal methodology is the significance of EU case law. The Court of Justice of the European Union ('CJEU') has long had a prominent role in the forming of EU law, making case law imperative for the understanding of the legislation. In their judicial practice, the CJEU gravitates towards a teleological approach of the law, giving the union's objectives, and present-time practical relevance, a navigating role.[17]

The greenness of EU law, in combination with its intergovernmental nature, has given significance to 'soft law' as a legal source in EU law. As EU law is based on a synergy of several legal systems, many independent EU bodies have emerged in order to ensure a consistent application of union law. While the recommendations of various EU bodies are not necessarily binding, such guidance is given great authority as it provides a representative stance on specific topics. Similarly, private actors frequently publish policies on EU law, in an attempt to interpret the legislations and make the provisions intelligible for businesses and other actors subject to the legal obligations. While the CJEU refrains from giving legal authority to non-binding law, the court still acknowledges that soft law has a considerable effect on a national level. National courts and authorities tend to fill in legal gaps with soft law as a basis for interpretation of the binding acts. By recognizing how EU law is interpreted, and consequently implemented, in practice, it is possible to assess the law in the light of the purposes guiding the EU legal system.[18]

Accordingly, the European legal methodology will be applied to this thesis as the aim requires an assessment of the current, contextual, legal discourse on EU law. The research questions are attuned with the European methodology, thus CJEU case law is given interpretational value while national interpretations are acknowledged as a means to teleologically assess the implementation of the GDPR.

[16] Walker, 'Legal Theory and the European Union: a 25th Anniversary Essay', 2005, pp. 581–601.
[17] Nääv & Zamboni, 'Juridisk metodlära', 2018, p.122.
[18] Nääv & Zamboni, p.128.

As the GDPR is subject of examination, the regulation and its provisions will make the foundation for the choice of materials. The primary EU rules referred to are the CFR and the Treaty on the Functioning of the European Union ('TFEU') [19] as they dictate the underlying rationale of the GDPR.

As EU case law bears great importance, CJEU judgements on consent under GDPR will be examined. However, the main source of interpretation on valid legal consent are the guidelines adopted by the European Data Protection Board ('EDPB') in 2020.[20] The guidelines on valid consent under GDPR published by the EDPB ('EDPB Consent Guidelines')[21] offer a comprehensive outline for the notion of valid consent, wherefore they comprise a basis for the examination of the respective requirements. The EDPB Consent Guidelines are an extension of the guidelines on consent issued by the Article 29 Working party[22] ('WP29').[23] The EDPB has endorsed several other WP29 documents on data protection.[24] Apart from the officially endorsed documents, when interpreting consent, the EDPB frequently refers to the WP29 opinion on the definition of consent.[25] As such, the different WP29 documents will constitute a part of the material used in this thesis.

In respect to the above presented method, some notable decisions by national authorities will be examined. The choice of decisions issued by national authorities will be made based on the impact within the Union and the relevance in regard to the purpose of this thesis.

The role and authority of the actors mentioned in this section will be presented under sub-chapters 2.2 and 2.3 as their legal capacities determine the interpretational value of the different materials.

Other materials that will be cited consist of literature, journals and where necessary in terms of providing a contextual element; such material will be referred to correspondingly. Noteworthy is the GDPR Commentary edited by professors and leading authors on EU data protection law. The commentary takes into account legal processes up to 1st August 2019 and has been praised

[19] Treaty on the Functioning of the European Union, OJ C 202, 76.2016.
[20] For more about the EDPB see sub-chapter 2.2.
[21] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, Adopted on 04 May 2020.
[22] The Working Party on the Protection of Individuals with regard to the Processing of Personal Data.
[23] Article 29 Working Party Guidelines on consent under Regulation 2016/679, 17/EN, WP259 rev.01.
[24] The European Data Protection Board Endorsement 1/2018, Brussels, 25 May 2018.
[25] WP29, Opinion 15/2011 on the definition of consent, 01197/11/EN, WP187, Adopted on 13 July 2011, ('WP187').

as a valuable contribution to the understanding of the GDPR by the former European Data Protection Supervisor ('EDPS') Giovanni Buttarelli†.[26] The commentary will mainly be used for providing a general understanding of the GDPR and its rationale in chapter 2.

1.5 Delimitations

As the GDPR has a broad scope and valid consent is required in numerous data processing activities, an extensive delimitation is necessary in order to achieve the purpose of this thesis within its confines.

EU instruments on data protection law other than the GDPR will not be covered except when particularly relevant for understanding the GDPR. As this paper focuses on the GDPR on an EU level, Member States' laws and their legislative implementations will be excluded. However, in order to illustrate how the regulation has been interpreted, particularly selected decisions by national authorities will be subject for examination. Ultimately, this thesis does not intend to provide a comparative examination and relies on national authorities solely for guidance on the decipherment of the criteria for consent under the GDPR.

This thesis will be limited to an examination of the definitions, interpretations and implications of the requirements for valid consent to be freely given, specific, informed and unambiguous. An examination of when valid consent is required is excluded, with only a brief demonstration of consent as a legal basis. Other conditions for valid consent, such as age in relation to particular processing, will be excluded. Likewise, consent for the processing of special categories of personal data will be excluded. Thus, the following are the GDPR provisions governing consent that are excluded from the scope of this thesis: Article 8 on children's consent on the internet; Article 9 on consent for processing of special categories of personal data; Article 22 requiring consent regarding automated individual decision-making, including profiling, to be explicit and finally Article 49 that governs consent in relation to transfers of personal data to third countries and international organisations.

The analysis of the interpretations of the respective requirements will be made from a general perspective, leaving room for further elaboration on the implications on specific actors, e.g. the different actors in programmatic marketing. As this thesis aims at analysing valid consent in the light of the rationale, such an analysis is made on a general level and with focus on

[26] Kuner et al., Foreword by Giovanni Buttarelli.

technological neutrality, leaving room for further research on the GDPR and fundamental rights and freedoms.

While referencing information technologies and various implementations of such technologies, this thesis will provide information on the relevant technologies exclusively to an extent that is strictly necessary to understand the GDPR provisions and their implementations.

1.6 Disposition

The following chapter provides an elemental understanding of the GDPR. Sub-chapter 2.1 gives a brief overview of the background of the legislation and is closely connected to sub-chapter 2.2 on the role of the WP29 and the EDPB, as well as sub-chapter 2.3 on the role of the DPAs, national courts and the CJEU.

Sub-chapter 2.4 is further divided into five sections where the first section encompasses the rationale behind the GDPR, followed by the second section where the importance of technological neutrality is raised. Sections four and five delve into the scope and key terminology of the GDPR in order to provide a basic understanding of the regulation. The fifth and final section under sub-chapter 2.4 acknowledges the main principles of the GDPR and delves into the notion of lawful processing, thus providing a context for when consent is relevant.

Under chapter 3 the criteria for valid consent according to the GDPR are examined. Sub-chapter 3.1 provides a brief introduction to the notion of consent and presents Article 4(11) and Article 7 GDPR under which the definition and requirements for valid consent are established. The second sub-chapter is divided into four sections, each examining one of the four criteria (‘freely given’, ‘specific’, ‘informed’ and ‘unambiguous’) as defined by the GDPR with the guidance of the EDPB and WP29. Sub-chapter 3.3 examines how consent under the GDPR has been interpreted, and thus shaped, by the CJEU.

Chapter 4 examines how the criteria for valid consent have been interpreted at Member State level by national authorities. While attempting to untangle the prerequisites in order to provide a distinct understanding of each criteria, the criteria are typically bundled and discussed *en masse*. Moreover, the criteria are often interdependent and coinciding. Therefore, in order to

provide a clear and cohesive examination of the interpretation of the criteria, chapter 4 will be sectioned by cases and decisions, rather than the criteria for consent.

As EU data protection law is fairly new and rapidly evolving, noteworthy developments will be examined under chapter 5, as a means to provide an up-to-date examination of the legal discourse.

Finally, chapter 6 consists of concluding remarks on the examined material in the light of the purpose of this paper. Customarily, the final chapter is followed by a bibliography of the material used in this paper.

2 The GDPR – An overview

2.1 Background

In 2009, the Treaty of Lisbon[27] introduced the right to data protection along with a legal basis for data protection legislation in Article 16 TFEU. It also gave the CFR, along with its eighth article on right to data protection, a constitutional status. The following year the European Commission ('EC') decided that the at that time applicable Data Protection Directive ('DPD')[28] was no longer sufficient for ensuring data protection rights with regard to the rapid advancement of use of technology.[29] Following lengthy and at times controversial consultations and proposals amongst various EU institutions regarding the modernisation of the EU data protection framework, in January 2012 the EC released the final proposal for the General Data Protection Regulation ('GDPR Proposal').[30] Once the GDPR Proposal was adopted, the European Parliament (the 'Parliament') and the Council of the European Union (the 'Council') had to agree on the final text which proved challenging, as a record of 3,999 amendments were submitted by Members of the European Parliament.[31] Despite numerous disagreements amidst Parliament members and various committees, the legislative effort regarding the GDPR was encouraged and expedited by the scandalous news about widespread government intelligence surveillance, in particular the Snowden revelations regarding the United States Government.[32] In June 2015 the Council decided on a General Approach which was then subject for negotiation by the Council, the EC and the Parliament. In December of 2015 an agreement was reached and the GDPR was finally agreed on and in May 2016 the GDPR entered into force.[33] On 25 May 2018, the GDPR became applicable in all EU Member States and in June 2018 the GDPR became valid in the European Economic Area ('EEA').[34]

[27] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007); entry into force on 01 December 2009.
[28] 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.
[29] Kuner et al., p. 4.
[30] European Commission, Brussels, 25.1.2012 COM (2012), 11 final 2012/0011 (COD), Proposal for a Regulation Of The European Parlament and thee Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[31] Kuner et al., p. 5.
[32] Ibid.
[33] Ibid., p.7.
[34] EFTA, 'General Data Protection Regulation incorporated into the EEA Agreement', 2018.

2.2 The role of the WP29 and the EDPB

Article 29 of the DPD established the WP29 and gave it independent advisory status. The purpose of the WP29 was to advise the EC and contribute to a uniform application of the nationally devised laws integrating the rules pursuant to the DPD.[35] The WP29 was composed of representatives of the supervisory authorities from each Member State as well as representatives of the EDPS and the EC.[36]

The WP29 ceased to exist once the GDPR went into effect and was replaced by the EDPB.[37] The EDPB is composed of the EDPS and the heads of each Member States' respective supervisory authority.[38] Article 68 (1) GDPR establishes the EDPB and declares that the EDPB shall have legal personality, extending and enhancing the status of its predecessor. As an independent body of the EU, the EDPB has a dispute resolution function for disputes between national supervisory authorities and the EDPB can make legally binding decisions.[39] While the EDPB does not enforce laws, the EDPB provides general guidance on the interpretation of the GDPR, making their decisions, recommendations and other guiding acts of great importance in the interpretation and implementation of the GDPR.[40]

Prior to the implementation of the GDPR, the WP29 released several guiding documents on various GDPR aspects, one such document being the Guidelines on consent under the GDPR. The WP29 guidelines on consent were ultimately revised and adopted in April 2018. In connection to the implementation of the GDPR, the EDPB endorsed the WP29 Consent Guidelines, giving it significant interpretative status.[41] In May 2020 the EDPB published its own, updated, guidelines, referred to as the EDPB Consent Guidelines.

[35] Recital 65 DPD.
[36] Article 29 (2) DPD; Article 29 (2) DPD states that 'a representative of the authority established for the Community institutions and bodies' shall be part of the WP29. As established under Article 41.2 of Regulation 45/2001, such authority in regard to the processing of personal data shall be the EDPS.
[37] European Commission, Newsroom, 'The Article 29 Working Party ceased to exist as of 25 May 2018', 2018.
[38] See Article 68 (3) GDPR; EDPB,'Who we are'.
[39] Article 65 GDPR.
[40] EDPB, 'Who we are'.
[41] EDPB, Endorsement 1/2018, Brussels, 25 May 2018.

2.3 The role of DPAs, national courts and the CJEU

Each Member State is under Article 28 GDPR required to appoint at least one national supervisory authority, DPA, responsible for correct interpretation and enforcement of data protection laws on a national level, in order to protect the rights and freedoms under the rationale.[42] Article 58 GDPR awards the DPAs with investigative, corrective, authorisation and advisory powers. The DPAs are thus for instance authorised to, with respect to the controller or the processor, obtain access to all personal data and to all information necessary for the performance of its tasks, issue reprimands, order compliance with the GDPR and impose administrative fines.[43]

The DPAs are independent national authorities with the competence to enforce compliance with the GDPR by issuing legally binding decisions.[44] The DPAs primarily operate within the national legal systems and as the GDPR leaves a certain level of discretion to the Member States, there are some differences between Member States in terms of implementation and interpretation of the GDPR.[45] Nevertheless, as the DPAs have a key role in the implementation and interpretation of the GDPR, Article 63 GDPR obliges the DPAs to cooperate with each other and with the EC in order to contribute to a consistent application of the GDPR across the union. However, such cooperation is only required in cross-border instances. Hence, one DPAs interpretation of a provision in an exclusively domestic case does not have direct binding impact beyond the borders of the state the DPA operates in.[46]

In April 2022, the EDPB released a noteworthy statement; the EDPB members have agreed to expand cooperation between the DPAs in cases of strategic importance in order to ensure a consistent interpretation of the GDPR. This expands the notion of cross-border instances by including cases of strategic importance, defined by the EDPB as ‘cases which fulfil a number of quantitative and qualitative criteria (e.g., cases affecting a large number of data subjects in the EEA, cases dealing with a structural or recurring problem in several member states, cases related to the intersection of data protection with other fields,…)’. [47]

[42] Article 51 GDPR.
[43] Article 58 GDPR.
[44] See Article 78 GDPR.
[45] See Chapter IX GDPR; Recital 10 GDPR; Kuner et al., p. 870.
[46] Kuner et al., p. 1001.
[47] EDPB, Statement on enforcement cooperation, Adopted on 28 April 2022.

Article 78 GDPR asserts that legal or natural persons must have access to an effective judicial remedy before a competent court of the Member State against a legally binding decision issued by the DPA.[48] In order to secure a uniform application of EU law, the national courts may look at existing EU case law and if further guidance is needed, the courts can request a preliminary ruling by the CJEU.[49]

During main proceedings, national courts can refer questions concerning the interpretation or validity of EU law to the CJEU in order to get a preliminary ruling.[50] The national courts retain their judiciary competence and shall only draw conclusions from the CJEU's ruling. The CJEU has a key role in the interpretation, and hence shaping, of EU law as preliminary rulings are binding both on the referring court and to all courts in the Member States. Consequently, a reference for a preliminary ruling is particularly useful when questions are raised on new statutes that are yet to be interpreted for a uniform application of EU law. [51] As the CJEU has the power to determine the validity of EU law, the court can declare legal acts and decisions issued by EU bodies, e.g., decisions issued by the EDPB, invalid giving the CJEU supreme authority to interpret EU law and provide principal definition of EU law provisions. Additionally, in case a Member State fails to comply with EU law, including a court decision, or doesn't rectify a violation of EU law, the EC may refer the matter to the CJEU that in case of contravention can impose a fine on the Member State.[52]

2.4 General provisions and principles

2.4.1 Rationale

Article 1(2) of the GDPR establishes the dual rationale of the regulation: protection of the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and protection of the free movement of data within the union. The fundamental rights and freedoms of natural persons referred to are specified under Recital 1 of the GDPR: Article 8(1) CFR and Article 16 TFEU. While the former one guarantees right to protection of personal data and states that such data must be processed 'fairly for specified purposes and on

[48] Recital 129 GDPR; Article 47 CFR.
[49] Article 267 TFEU; Court of Justice of the European Union, Recommendations to National Courts and Tribunals in relation to the initiation of Preliminary Ruling Proceedings, 2019/C 380/01, 08 November 2019.
[50] Article 19 Treaty on European Union (Consolidated version 2016), OJ C 202, 7.6.2016; Article 267 TFEU.
[51] CJEU Recommendation C 380/01, 2019.
[52] Articles 258-260 TFEU; European Commission, 'Infringement Procedure'.

the basis of the consent of the person concerned or some other legitimate basis laid down by law', Article 16 of the TFEU specifies that such protection, must be laid down by the Parliament and the Council. While the objectives and principles of its predecessor, the DPD, remain, the GDPR has an additional goal of harmonisation within the union; Recital 9 of the GDPR addressed the fragmented implementation of data protection under the DPD and highlights the need of a uniform application of the rules in order to achieve the rationale. It is for this reason that the GDPR was adopted as a regulation instead of a directive.[53] While the regulation is set out on an EU level, Member States enjoy a margin of discretion; such discretion is limited to the maintenance of a balance between the different rationales of the GDPR.[54]

The right to protection of personal data is not absolute as it shall be designed to 'serve mankind' and hence considered in its context and balanced against other fundamental rights in accordance with the principle of proportionality.[55] The provisions under the GDPR must therefore be applied with regard to other fundamental rights and freedoms under the CFR, such as: the freedom of expression and information;[56] the freedom to conduct business;[57] and right to the principle of legality.[58] Moreover, while the right to data protection must be balanced against other fundamental freedoms, Article 1(2) of the GDPR sets out that data protection is a prerequisite for the effective exercise of other fundamental rights and therefore should be implemented in a way that reinforces other fundamental rights and freedoms.[59] Recital 2 GDPR further emphasises that the overall goal of the GDPR is to 'contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons'. The goal of data protection law is thus not to prohibit processing of data nor to prevent the use of technologies, but rather to prevent abuse of data in a way that violates our fundamental rights and freedoms.[60]

[53] Kuner et al., p. 604.
[54] Kuner et al., p. 53.
[55] Recital 4 GDPR.
[56] Article 11 CFR.
[57] Article 16 CFR.
[58] Article 49 CFR.
[59] Kuner et al., p. 57.
[60] See Bieker, p. 162.

2.4.2 Technological neutrality

The provisions under the GDPR must rest on the rationale rather than a specific means of data processing.[61] Thus, technological neutrality has been emphasised since the early stages of the preparations for the GDPR as the instrument aims at building a strong and modern data protection framework that is able to meet future needs.[62] As stipulated by the EC, technological neutrality means 'not to impose, nor discriminate in favour of, the use of a particular type of technology, but to ensure that the same service is regulated in an equivalent manner, irrespective of the means by which it is delivered'.[63]

Recital 6 GDPR recognizes the rapid technological developments and the significantly increased scale of the processing of personal data, as well as technology's role in the transformation of the economy and social life. Moreover, the recital underlines that technologies shall continue facilitating the free flow of personal data within the union while ensuring a high level of data protection. Recital 15 established that the GDPR should be technologically neutral in order to on the one hand ensure a high level of data protection and prevent circumvention, and on the other hand maintain the synergy with technological advancements.[64]

Consequently, technologically neutral legislation is fundamental in order to ensure protection of personal data without hindering technological advancement.

2.4.3 Material and territorial scope

As determined by Article 2(1), the material scope covered by the GDPR is the 'processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'. This is limited by the second paragraph which, for example, excludes processing by a natural person for purely personal or household activities, with no connection

[61] See argumentation by Reed, 'Taking Sides on Technology Neutrality', 2007, pp. 264-266.
[62] GDPR Proposal, p. 104.
[63] Commission of the European Communities, "Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Towards a new framework for Electronic Communications infrastructure and associated services – The 1999 Communications Review" COM(1999) 539 final, 10 November 1999, p. VI.
[64] Recital 15 GDPR.

to a professional or commercial activity.[65] See the next section for the definitions of 'processing' and 'personal data'.

As for the territorial scope, Article 3 established that the GDPR applies in three cases: whenever a data controller or data processor is established in the EU, regardless of whether the processing takes place in the EU or not; whenever a controller or processor, regardless of where they're established, offers goods or services in the EU or monitors the behaviour of individuals in the EU and finally, the GDPR applies to the processing of personal data by a controller established where Member State law applies by virtue of public international law. Thus, a company in the US offering services to data subjects located in the EU, must comply with the GDPR in regard to the processing of that personal data. Likewise, if a company in the EU processes personal data of persons located outside of the EU, they have to comply with the GDPR because they are established in the EU, regardless of data subjects' location.

2.4.4 Definitions of key terms

Article 4 of the GDPR provides definitions of the key terms used in the regulation: 'Personal data' is defined in broad terms and means any information relating to an identified or identifiable natural person ('data subject').[66] Hence, anonymous information is not covered by the GDPR, while pseudonymous and aggregated data, although depending on the level of aggregation, are in most cases considered as identifiable data as such data can together with additional information be attributed to a natural person.[67] Therefore, online identifiers such as cookie identifiers and internet protocol addresses are considered as personal data as such identifiers may be traced back to the data subject when combined with other information found on servers.[68]

Processing is defined as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[69] As the GDPR shall be technologically

[65] Recital 18 GDPR.
[66] Article 4(1) GDPR.
[67] Recital 26 GDPR.
[68] Recital 30 GDPR.
[69] Article 4(2) GDPR.

neutral, processing is a very broad term that encompasses every operation on personal data, from collection to deletion, regardless of technique.[70]

Article 4(7) defines controllers 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'. The controllers have a fundamental role in the operationalisation of the GDPR as they are the main bearers of the obligations set out by the regulation.[71] Controllership can be shared between multiple controllers and in order to achieve adequate protection of the data subject, the CJEU has emphasised that the interpretation of what constitutes a controller must be broad.[72] For example: a social media company collecting personal data is considered as the controller as it is they who determine the *how* and *why* of the processing. Meanwhile, a natural or legal person, public authority, agency or other body processing that same data, on behalf of the controller, is considered a processor.[73] In case the processor acts beyond the controller's instructions and starts to determine its own purposes and means of the processing, the processor assumes the role of controller in respect of that particular processing activity.[74]

2.4.5 Lawful processing

Article 5 GDPR establishes the key principles of data protection and outlines what constitutes GDPR compliant processing of personal data. The data must be: 'processed lawfully, fairly and in a transparent manner in relation to the data subject', 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes' and 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.[75] Furthermore, the data must be accurate, kept to date, stored identifiable to the data subject for no longer than necessary for the purpose and processed only if appropriate security measures are taken to ensure integrity and confidentiality.[76] Ultimately, the principle of accountability expressed in the second paragraph establishes that it is the

[70] Recital 15 GDPR.
[71] Kuner et al., p. 146.
[72] Kuner et al., p. 151; Ibid, p.148, as referring to Cases C-131/12, Google Spain, para. 34; Case C-210/16, Wirtschaftsakademie, para. 28; Case C-40/17, Fashion ID, paras. 65–66.
[73] Article 4(8) GDPR.
[74] Article 28(10) GDPR.
[75] Article 5(1)(a-c) GDPR.
[76] Article 5(1)(d-f) GDPR.

responsibility of the controller to account for and to demonstrate the compliance with these principles.[77]

For the processing to be lawful the processing must have a legal basis in accordance with Article 6(1) GDPR. Such a legal basis must be established in relation to each specific purpose by the controller prior to the processing and must be demonstrable unceasingly during the duration of the processing; this, in order to secure accountability and transparency in accordance with the principles laid down by Article 5 and the data subject rights under chapter 3 GDPR.[78] Article 6(1) provides an exhaustive list of legal bases:

1. When the data subject consents to the processing of their personal data for one or more specific purposes.[79] Such consent must satisfy the conditions for valid consent as stipulated under the GDPR. These requirements for valid consent under the GDPR are the subject of examination in this thesis and will therefore be elaborated on in the following chapter.
2. Processing is necessary for the performance of a contract to which the data subject is party or if such processing is necessary for entering into a contract on the request of the data subject.[80]
3. Processing is necessary for compliance with the controller's legal obligations.[81]
4. Processing is necessary in order to protect vital interests of a natural person, including the data subject.[82]
5. Processing is necessary for the performance of a task carried out in the public interest, including when the controller acts on behalf of an official authority.[83]
6. Processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party. Such interests must be balanced against, and shall not conflict with, the interests or fundamental rights and freedoms of the data subject, unless the controller is a public authority acting.[84]

[77] Article 5(2) GDPR.
[78] See IMY, 'Lawful grounds for personal data processing', 2022.
[79] Article 6(1)(a) GDPR.
[80] Article 6(1)(b) GDPR.
[81] Article 6(1)(c) GDPR.
[82] Article 6(1)(d) GDPR.
[83] Article 6(1)(e) GDPR.
[84] Article 6(1)(f) GDPR; Recital 47 GDPR.

While the controller is required to make an assessment on the appropriate legal basis for the processing of personal data, other legal obligations must be regarded for the processing to be lawful.[85] Directive 2002/58/EC,[86] amended by Directive 2009/136/EU,[87] outlines the legal framework for the processing of personal data and the protection of privacy in the electronic communications sector ('ePrivacy Directive'). The ePrivacy Directive is commonly known as the 'cookie law', as it introduced cookie consent pop-up banners that internet users often encounter while visiting a website.[88] Article 5(3) of the ePrivacy Directive lays down a user's prior consent as a condition for the use of cookies that are not strictly necessary for the essential functions of the service requested by the user.[89] Article 2(f) of the ePrivacy Directive establishes that the definition of consent shall correspond with consent under the GDPR, ergo harmonising consent and relying on the interpretations made in relation to the GDPR.

[85] Kuner et al., p. 314.
[86] 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 (Directive on privacy and electronic communications).
[87] Directive 2009/136/EC of the European Parliament and 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.
[88] GDPR.eu, 'Cookies are an important tool that can give businesses a great deal of insight into their users' online activity. Despite their importance, the regulations governing cookies are split between the GDPR and the ePrivacy Directive'.
[89] WP29, Opinion 2/2010 on online behavioural advertising, 00909/10/EN, WP 171, Adopted on 22 June 2010, p. 8; WP29, Opinion 04/2012 on Cookie Consent Exemption, 00879/12/EN, WP 194, Adopted on 07 June 2012, p. 2.

3 Valid consent under the GDPR

3.1 Overview

3.1.1 Introduction

Consent is fundamental under EU data protection law as Article 8(2) CFR explicitly recognizes consent and highlights it as a legitimate basis for processing of personal data. Fundamental data protection rights build on the idea that one should be in control of their own personal data, making consent essential as it leads to autonomy. At the same time, autonomy is a prerequisite for consent as consent itself must reflect one's genuine wish and consideration must be taken into whether an individual is in a position to take a decision.[90] For decades consent in law, both nationally and internationally, has been more than a simple 'yes'. While there are many discrepancies between the concept of consent between different areas of law and different legal systems, there has long been an understanding that consent must be free and informed, regardless of whether it has been within medical law or consumer contract law.[91] Consent does not have one universal definition and is instead dictated by law within respective field. Moreover, the notion of consent changes with time and with changing beliefs on rights and freedoms.

Important to note is that consent does not diminish the data controller's other obligations concerning the principles as established by Article 5 GDPR. As stated by the EDPB 'Even if the processing of personal data is based on consent of the data subject, this would not legitimise collection of data, which is not necessary in relation to a specified purpose of processing'.[92]

In order to gain a general understanding of what consent means under the GDPR, the articles governing consent will be cited and the provisions on consent will be delineated below.

[90] WP187, p. 8.
[91] Beyleveld & Brownsword, Consent in the Law, 2007, pp. 7-9.
[92] EDPB Consent Guidelines, p. 5.

3.1.2 Article 4(11) GDPR: Definition of consent

Article 4(11) GDPR defines consent as the following:

'consent' of the data subject means 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 to the processing of personal data relating to him or her.

The four criteria are closely linked and often dependent on each other; specific consent is closely linked to informed consent as both criteria safeguard transparency.[93] Similarly, for consent to be freely given there is a requirement of granularity, i.e., the purposes must be separated and specific.

3.1.3 Article 7 GDPR: Conditions for consent

The conditions for consent are further outlined under Article 7 GDPR that states:

- *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*[94]

The burden of proof is thus on the controller. It is up to the controller to decide on a fitting method of demonstration and the mere compliance with the obligation to demonstrate consent shall not necessitate further collection of data.[95] The controller must be able to demonstrate consent for as long as the processing activity lasts and not longer than strictly necessary for compliance with legal obligations after the processing activity ends.[96] As the GDPR does not set a time limit for how long consent lasts, the burden of proof remains with the controller in terms of whether consent is still valid in terms of context, supposed expectations of the data subject and changes in the scope of the processing.[97]

- *If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form,*

[93] EDPB Consent Guidelines, pp. 14-15.
[94] Article 7(1) GDPR.
[95] EDPB Consent Guidelines, p. 22.
[96] Ibid., pp. 22-23.
[97] Ibid., p. 23.

using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.[98]

- *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*[99]

- *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.*[100]

3.2 Criteria for valid consent

3.2.1 Freely given consent

3.2.1.1 Introduction

Freely given consent means an absence of coercion and aims at rejecting consent that has been given under coercive circumstances that do not represent the data subject's own free will.[101] 'Freely given' is closely linked to the notion of control that is derived from fundamental rights and freedoms, making freely given consent cardinal for exercising one's rights and freedoms.[102] While freely given consent is ultimately dependent on consent being specific, informed and unambiguous, the notion of 'freely given' consent can be divided into assessments of power imbalances, right to withdrawal and conditionality.

3.2.1.2 Imbalance of power

Recital 43 GDPR states that a clear imbalance between controller and data subject precludes freely given consent. Any element of pressure or influence must be considered and as emphasised by Recital 43, the asymmetry of power in the case where the data controller is a

[98] Article 7(2) GDPR.
[99] Article 7(3) GDPR.
[100] Article 7(4) GDPR.
[101] Recital 42 GDPR; EDPB Consent Guidelines, p. 9.
[102] WP187, p. 8.

public authority is undeniable.[103] In the case where a public authority wants to process personal data of the data subject, the EDPB advises to rely on another lawful basis. Although, valid consent in such a case is not completely unattainable; the EDPB Consent Guidelines provide examples of circumstances where consent to a public authority could be appropriate. A local municipality may offer citizens an email subscription with updates on the progress of major construction work, such as road works, as long as information about decisions and activities affecting citizens, is accessible for all in other means, e.g., on public websites. As refraining from consenting to the processing of one's personal data, i.e., email-address, the data subject suffers no negative consequences, thus enabling consent to be regarded as freely given. Another example is in the case where a public-school requests students' consent for the use of their photographs in a student catalogue. As long as the choice on whether to consent does not affect the students' education, such consent would be an expression of the students' genuine choice.[104]

A similar power asymmetry occurs when the data subject is an employee or prospecting employee of the data controller. As the data subject in such a context is dependent on the controller, assuring that consent has been given without pressure or fear of detriment is unlikely.[105] As specified by the WP29, coercion must be interpreted in a broad sense that encompasses e.g., social, financial and psychological detriment or intimidation.[106] Thus, if an employer would like to install cameras to monitor the workplace, consent could not be used as a legal basis for such processing of personal data of the employee. Nevertheless, there are exceptional circumstances where the employee could give free consent to their employer; the EDPB provides one such example: If the employer plans to have a film crew filming the office, the employer can ask for consent from the employees that would appear in the background in the specific filming location. However, the employees must be given a satisfactory alternative space to work elsewhere and a refusal to consent cannot have any negative consequences on the employment. As emphasised by the EDPB, the above-mentioned power asymmetries are not exhaustive and as established by the GDPR, any element of pressure or influence must be considered.[107]

[103] Ibid., p. 7.
[104] EDPB Consent Guidelines, p. 8.
[105] Ibid., p. 9.
[106] WP187, p. 13; See also EDPB Consent Guidelines, p. 9, para. 24, on intimidation as coercion.
[107] EDPB Consent Guidelines, p. 9; Recital 43 GDPR.

3.2.1.3 Withdrawing consent

Article 7(3), as well as Recital 42, explicitly state that the right to withdraw consent is a prerequisite for consent to be regarded as freely given. If the data subject cannot exercise their free and genuine choice in regards by withdrawing consent, such consent cannot be considered as freely given. Moreover, the controller must be able to demonstrate consent, as well as the possibility to freely withdraw consent, throughout the entirety of the processing activity.[108] Logically, if the data subject cannot withdraw consent, the controller cannot fulfil their obligation to demonstrate consent beyond the moment of receiving initial consent as further processing is no longer discretionary.

Furthermore, there is a threshold for the practicability of withdrawal of consent as 'it shall be as easy to withdraw as to give consent'.[109] Thus, when consent is given electronically, e.g., with a computer mouse-click, the data subject must be able to withdraw consent just as easily.[110] Consequently, if consent is obtained through a specific app, withdrawal must be possible on that same app and without cost or other undue effort. As such, if consent is given by simply clicking 'yes' on a controller's website, withdrawing consent must be as simple; if the controller only offers a possibility to withdraw such consent by calling their call centre during opening hours, the consent cannot be considered as freely given as withdrawal requires disproportionate effort. [111]

Fear of detriment and worsened conditions precludes consent also when the risks are in relation to withdrawal of consent.[112] The EDPB gives the following example: 'When downloading a lifestyle mobile app, the app asks for consent to access the phone's accelerometer. This is not necessary for the app to work, but it is useful for the controller who wishes to learn more about the movements and activity levels of its users. When the user later revokes that consent, she finds out that the app now only works to a limited extent. This is an example of detriment as meant in Recital 42, which means that consent was never validly obtained (and thus, the controller needs to delete all personal data about users' movements collected this way)'. However, the EDPB continues and clarifies that, to the contrary, if the consent is obtained by a clothing retailer with the purpose of collecting additional personal data in order to tailor the

[108] Articles 7(1) & 7(3) GDPR.
[109] Article 7(3) GDPR.
[110] EDPB Consent Guidelines, p. 23.
[111] Ibid., p. 24.
[112] Article 4(11) GDPR.

recommended offers based on shopping history, consent may still be considered as freely given despite withdrawal leading to less accurate recommendations. The EDPB explains that withdrawal in this case results in non-personalised fashion discounts and that 'does not amount to detriment as only the permissible incentive was lost'.[113]

3.2.1.4 Conditionality and granularity

The element of granularity is closely tied to specific consent and will thus be further examined under the following section.

As expressed under Article 7(4) GDPR, consent is not freely given if the consent is conditional for the performance of a contract. For instance, if a bank, as a condition for their banking services, requires their customers to consent to the collection of their personal data for direct marketing purposes, such consent cannot be valid. If the customer has to consent to marketing, in order to, e.g., get a loan or close their bank account, the consent to the marketing is not a genuine expression of the customers free will, but rather a coercion.[114] If the controller needs to process personal data for the performance of a contract, consent is the wrong choice of legal basis.[115]

Consequently, if a website makes access to their content conditional on consent to their cookie banner, such consent is not freely given. Thus, if a data subject tries to enter a website and a cookie consent banner pops up, blocking the data subject from viewing their content unless they click 'Accept cookies', consent collected in such a manner is not freely given as the data subject who wants to access the website has no real choice.[116]

If a controller wishes to process personal data for several different purposes and processing operations, there is a requirement of granularity, meaning that consent cannot be bundled and must be obtained separately, unless appropriate on a case-by-case basis.[117] However, while conditionality and bundling is not an absolute hindrance, the GDPR states that 'utmost account' must be taken into consideration and that bundled consent is presumed to be invalid.[118] In order to assess whether bundled consent is freely given, coercion must, as mentioned in relation to power imbalance, be interpreted in a broad sense that considers e.g., psychological intimidation.

[113] EDPB Consent Guidelines, p. 13.
[114] Ibid., p. 11.
[115] See Aricle 6(1)(2) GDPR.
[116] EDPB Consent Guidelines, p. 12.
[117] Recital 43 GDPR.
[118] Article 7(4) GDPR; Recital 43 GDPR.

Bundling consent for several processing activities reduces the data subject's ability to make a free choice and limits their control of their personal data, thus violating their fundamental rights.[119]

3.2.2 Specific consent

3.2.2.1 Introduction

Consent as a lawful basis under Article 6 GDPR must be given in relation to 'one or more specific purposes', making specificity fundamental for valid consent.[120] As shown above, in order for consent to be freely given and thus valid, there must be a level of granularity, and thus specificity, in the consent request. Moreover, specific consent is closely tied to 'informed'. 'Specific consent' is thus partly covered in relation to the other criteria, making this chapter relatively short.

The EDPB breaks down specificity into three elements: purpose specification, granularity and clear separation of information.[121]

3.2.2.2 Purpose specification

As a safeguard against the controller abusing consent by requesting consent for vague purposes whose interpretations can be widened and blurred, the GDPR requires the purpose to be specific. The purpose must also be specific in order to comply with the principle of purpose limitation under Article 5(1)(b) GDPR. The data subject must be able to understand to what specific purposes they consent to in order to make an informed decision and exercise control over their data.[122] Moreover, the principle of purpose limitation commands the data controller to limit the processing of personal data for purposes that could not reasonably be fulfilled by other means than processing of personal data.[123] As such, requiring the controller to specify the purpose reassures that the controller, who must be able to demonstrate specific consent, is not processing more personal data than necessary.

[119] EDPB Consent Guidelines, p. 10.
[120] Article 6(1)(a) GDPR.
[121] EDPB Consent Guidelines, p. 14.
[122] WP187, p. 17.
[123] Recital 39 GDPR.

The EDPB suggests that vague purposes, such as for instance 'marketing purposes', 'future research' or 'improving user's experience', do not meet the criteria of specific consent.[124] Thus, when collecting personal data, valid consent can only be given to a concrete and well-defined purpose. Giving consent for general use of one's personal data is not possible.[125]

The GDPR emphasises the importance of specifying the purpose for the processing of personal data. As stated under Recital 32, 'consent should cover all processing activities carried out for the same purpose or purposes'. This leaves the processing operation and means of processing excluded from the requirement to be specified.[126]

How specific the data controller must be regarding the purpose of the intended data processing is not clarified by neither the GDPR, the EDPB or the WP29.

3.2.2.3 Granularity

In the case where several processing purposes are bundled into one single consent request, the data subject does not have the possibility to consent to a specific purpose, making such consent invalid. If the controller wants to process the data subject's personal data for different purposes, the controller must offer separate consent requests for the respective purposes. Accordingly, if a controller wants to expand the processing for further purposes, separate consent by the data subject in relation to the new purpose must be collected.[127]

3.2.2.4 Clear separation of information

The need for clear separation of information overlaps with the criteria 'freely given' and 'informed consent'; the latter will be examined under the following section.

For consent to be specific, the consent request must be clear and separated from other information that does not relate to the processing purpose.[128] As stipulated by Article 7(2) GDPR, 'the request for consent shall be presented in a manner which is clearly distinguishable from the other matters'. In the case that consent is requested as part of a paper contract that covers other matters, the consent request must be identifiable; Information on the processing

[124] EDPB Consent Guidelines, p. 14 referring to WP29 Opinion 3/2013 on purpose limitation, 02 April 2013; See WP187, p. 17.
[125] WP187, p. 18.
[126] EDPB Consent Guidelines, p. 14.
[127] Ibid.
[128] Ibid., p. 15.

purpose must be distinctly and clearly provided and preferably presented in a separate document so that the consent information and request is specific rather than bundled with other matters.[129]

3.2.3 Informed consent

3.2.3.1 Introduction

Transparency is one of the fundamental principles of the GDPR.[130] As a means to ensure that personal data is processed in a transparent manner in relation to the data subject, consent must be informed. If the data subject is not provided adequate information that enables them to understand what they are consenting to, the user does not have actual control, thus making consent invalid.[131] Recital 39 GDPR specifies that transparency requires that the data subject whose personal data is to be processed must be able to easily access and understand information regarding the identity of the controller, the purposes for the processing and finally their risks and rights in relation to the processing of their personal data and how to exercise these rights. These requirements for transparency are further established as the requirements for informed consent.[132] While not mentioned under the articles and recitals concerning valid consent, as an expression of the principle of transparency, the data controller is obliged by Articles 12 and 13 of the GDPR to provide certain information to the data subject when obtaining their personal data.[133] The EDPB suggests that in practice, the conditions for transparency and valid consent lead to an integrated approach. Nevertheless, in the case the controller fails to provide such information, they would be acting in violation of the GDPR, although if they still comply with the requirements as set by the provisions on valid consent, the consent as such would still be valid. Therefore, the information that is not directly required to be provided for consent to be 'informed' will be excluded from examination.

3.2.3.2 What information to provide

The EDPB breaks down the minimum requirements for what information is necessary to provide to the data subject in order to enable them to make an informed decision: the controller's identity, the purpose of the processing, what type of data that will be processed, the existence of the right to withdraw consent, whether data will be used for automated decision-

[129] Ibid., pp. 15-17.
[130] See Article 5 GDPR.
[131] EDPB Consent Guidelines, p. 15.
132 Recital 42 GDPR.
133 Recitals 60-63 GDPR.

making and whether there is a risk of data transference where there is no appropriate safeguards.[134]

As there can be multiple controllers the identity of all controllers must be provided. Moreover, if the controller intends to transfer personal data to be processed by other controllers, provided that the other controllers plan to rely on the same consent, the additional controllers must be named. The identity of eventual processors is not required.[135]

In order to make an informed decision, the data subject must understand what they are agreeing to, especially as the consent must be specific to a purpose. The controller must therefore make sure that the data subject is provided a clear description of such a purpose. The information needed regarding the purpose must be assessed with the target audience in mind. The data controller must thus first determine what their intended audience needs to know in order to make an informed decision.[136]

As established by Article 7(3) GDPR, the consenting data subject must be informed of their right to withdraw consent, as well as how to do so. If the data subject does not know that they can withdraw their consent, the data subject is not given the possibility to express their genuine wish throughout the entirety of the processing activity, making the consent non-freely given and thus invalid. For that reason, information on withdrawal must be regarded as indispensable.

In case the purpose of the processing changes, the controller must seek new consent and thus provide the data subject with updated information enabling the data subject to make an informed decision in relation to the new purpose.[137]

3.2.3.3 How to provide information

The data controller must, based on their audience, assess how to appropriately provide information in a clear and understandable way as the GDPR doesn't dictate specific means of presentation. However, Article 7(2) GDPR and Recital 32 establish that information must be easily accessible, clear and expressed in plain language, as well as distinguished from other matters, as declared under section 3.2.2 on specific consent. As the information must be presented with the context and audience in mind, the consent request should be easily

[134] EDPB Consent Guidelines, p. 15; See Recital 42 GDPR.
[135] EDPB Consent Guidelines, p. 16.
[136] Ibid., pp. 16-17.
[137] WP187, p. 19.

understandable for an average person of such an audience. The EDPB specifies that a consent request cannot be presented with legal jargon in long privacy policies, as such request is neither easily intelligible nor distinguished.[138]

Recital 32 GDPR states that information could be provided 'by a written statement, including by electronic means, or an oral statement'. Such a statement could consist of information in connection to ticking a box when visiting a website or choosing technical settings on, e.g., social media services. As the information must be easily accessed, information required for valid consent must be given together with the consent request. The consent request can thus not refer to a document or webpage elsewhere. With consideration to the use of small screens, layered notices can be used when necessary and appropriate in order to avoid disproportionate disturbance of user experience. [139]

As the controller has the burden of proof that valid consent has been obtained, they must be able to demonstrate that they've assessed what information and by what means, their audience can easily access and understand the consent request. The EDPB has given an example of how such assessment can be done and demonstrated: A company, in the role of data controller, could organise 'voluntary test panels of specific categories of its customers and present new updates of its consent information to these test audiences before communicating it externally'.[140]

3.2.4 Unambiguous consent

3.2.4.1 Introduction

As the controller must be able to demonstrate that the data subject has consented to the processing of their personal data, there must not be any doubt as to whether the data subject intended to consent or not. If the consent is not a clear affirmative act, there is ambiguity in regard to the intention and such consent cannot be considered valid.[141]

[138] EDPB Consent Guidelines, p. 16; WP187, p. 20.
[139] Recital 32 GDPR.
[140] EDPB Consent Guidelines, p. 17.
[141] WP187, p. 21; The GDPR has raised the threshold for consent in comparison to the DPD. As such, the requirements for valid consent under the DPD remain, although stricter and extended. The WP29's opinion on consent, including requirements for unambiguous consent, in relation to the DPD is thus still applicable.

3.2.4.2 Active statement

A 'clear affirmative act' means that consent must be an active statement, rejecting consent as something that can be indicated through silence or inactivity on the part of the data subject.[142] As such, pre-ticked opt-in boxes are not valid; when visiting a website and a cookie consent banner pops up, the consent banner cannot have consent options initially on 'I consent', and must thus leave the affirmative action of consenting to the data subject.[143] Similarly, merely visiting a website or proceeding with a service does not constitute consent, as such action would neither be specific nor informed and thus not possible to attribute to consent.[144] Furthermore, as established in relation to 'freely given' consent, consent must be as easy to withdraw as it is to give; consenting by merely visiting a website would preclude a real possibility to withdraw consent in accordance with what is required for freely given consent.[145]

The unambiguity must also apply to the specificity of consent, meaning that not only must it be clear that the subject intended to give consent, but also to what particular processing such consent has been given.[146]

3.2.4.3 How consent can be given

As examined under section 3.2.3 on informed consent, the GDPR gives guidance on how consent requests and information thereto can be provided. The same goes for the consent indication, meaning that consent could be given 'by a written statement, including by electronic statement, including by electronic means, or an oral statement'.[147] As it would be unrealistic to demand data subjects to write letters every time they want to consent, Recital 32 GDPR states that an electronic statement can include 'ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the processing of his or her personal data'.

The EDPB recognizes that, while the user experience should not be excessively disrupted by the consent request, in order to ensure unambiguous and hence valid consent, disruption might be necessary. As long as the controller complies with the rules set out by the GDPR, they can

[142] Recital 32 GDPR.
[143] EDPB Consent Guidelines, p. 18.
[144] EDPB Consent Guidelines, p. 19, Example 15, e contrario.
[145] EDPB Consent Guidelines, p. 19.
[146] Ibid., p. 18.
[147] Recital 32 GDPR.

develop consent requests as they wish in order to fit their service or product design. For instance, the consent request could ask that the data subject swipes right on their screen or does a specific motion with their smart device as an indication of consent; nonetheless, it must be clear that such motion signifies specific consent, and that the data subject has been informed prior to consenting. The EDPB further acknowledges the reality and challenges of the digital era; data subjects are met with numerous consent requests on a daily basis. When the data subjects are overexposed to such requests and overwhelmed by having to click and swipe in order to declare their wish too many times, 'click fatigue' might set in and erode the intended effect of consent requests. Click fatigue essentially makes data subject to hastily agree to consent requests without reading the information, resulting in illusory consent. The GDPR gives no exact guidance on how to counter click fatigue. However, it is up to the controller, in accordance with what has been presented under the previous section on informed consent, to tailor the consent request so that the intended data subjects can easily and effectively attain the information needed for an informed decision. The EDPB suggests that one way for controllers to ensure that consent is not ambiguous and merely an indication of the data subject being tired, is to obtain consent via browser settings. [148]

3.3 As specified by the CJEU

3.3.1 C-673/17 – *Planet49*

3.3.1.1 Background

In 2013, a German company named 'Planet49' organised a promotional lottery where users could take part by entering their names and addresses. Moreover, the lottery form consisted of two bodies of text with a corresponding checkbox each. The first set of text requested that the user would consent to third party direct advertising and was accompanied by an empty checkbox that the user had to click on in order to follow through with the participation in the lottery. The second body of text requested the user to consent to Planet49's setting cookies on their devices, enabling the company to track online behaviour of users when they are visiting advertising partners' websites. This request was accompanied by a pre-ticked checkbox. In the

[148] EDPB Consent Guidelines, p. 19.

latter consent request, a hyperlink opened a web page with information about the names of the different cookies.[149]

The Federation of German Consumer Organisations claimed that such consent could not be regarded as neither freely given nor informed, thus initiating court proceedings that ultimately reached the Federal Court of Justice. The court referred questions on the scope of valid consent in the case where a consent checkbox is preselected to the CJEU for a preliminary ruling.[150] The case was decided on in October 2019 and was the first case directly based on the GDPR handed to the CJEU.[151]

3.3.1.2 Specific Consent

The court ruled that 'specific' must be interpreted as the consent being a direct indication of the data subject's wishes for the purposes of the data processing in question. In this case, it could not be shown that the data subjects' who entered their contact details into the lottery inquiry and sent in the application without un-clicking the checkbox, had other purposes than solely participating in a lottery in mind. In other words, the data subjects' consent was specific only to participation in the lottery, and not to the storage of cookies.[152]

3.3.1.3 Informed Consent

As the ePrivacy Directive requires consent as a legal basis for the storage of, and access to, cookies, the referring court asked what information on cookies the data subject must be provided for the consent to be clear and comprehensive.

The court concluded that in order for the data subject to obtain clear and comprehensive information, the information must enable the data subject to easily determine the consequences of consent. The information must also be sufficiently detailed so that the user understands the functioning of the cookies.[153] Apart from the required information about the identity of the controller(s) and purpose(s) of processing, the court specified that when consent is requested for the use of cookies, the following information is required to provide: The duration of the operation of cookies as the data subject must be aware of to what extent their online behaviour

[149] Case C-673/17, Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbrauchrverbände – Verbraucherzentrale Bundesverband e.V, 01 October 2019, paras. 25-30.
[150] C-673/17, paras. 32-37.
[151] Kuner et al., p. 10; InfoCuria, Case-law, List of documents.
[152] C-673/17, paras. 58-59.
[153] Ibid., paras. 73-75.

will be tracked; and, information about the recipients of the data collected by the cookies, meaning that if third parties have access to the cookies, such recipients or categories of recipients must be indicated.[154]

3.3.1.4 Unambiguous Consent

In *Planet49,* the main question dealt with was the validity of consent obtained by a preselected tick in a checkbox.[155] As consent must be an indication and thus an active behaviour, passive consent such as proceeding with a pre-ticked checkbox could not constitute valid consent as defined by the GDPR. The court further established that unambiguous consent requires that informed and specific consent can in practice be objectively proven; when a data subject is presented with a pre-ticked checkbox, there is a risk that the data subject has not read the information thereto or even noticed the existence of such a checkbox.[156]

3.3.2 C-61/19 - *Orange Romania* SA v ANSPDCP

3.3.2.1 Background

The Romanian DPA (ANSPDCP) imposed a fine on Orange Romania, a provider of mobile telecommunications services, on the grounds that Orange Romania had processed customers' personal data without valid consent. Orange Romania had concluded written contracts with the purpose to provide telecommunications services. The contracts stated that the customers had been informed of, and consented to, the collection and storage of their identity documents. Orange Romania claimed that their sales agents, prior to concluding the contracts, had called and informed the customers with the necessary information regarding processing before obtaining their oral consent. Based on the alleged consent, the sales agents ticked in the checkboxes regarding consent to the collection of copies of identity documents, before providing the customers with the contract. The customers who refused to consent, were given separate forms to sign that confirmed their refusal. The case was referred to the CJEU by the Regional Court of Bucharest for a preliminary ruling on the questions regarding what conditions must be fulfilled in order for consent to be regarded as freely given, specific and informed under

[154] Ibid., paras. 77-81.
[155] Ibid., para. 37.
[156] Ibid., paras. 52-55.

the DPD.[157] However, in order to provide guidance on the interpretation of EU law, the CJEU ruled that the questions would be answered on the basis of the DPD and the GDPR.[158]

3.3.2.2 Freely given consent

In its Judgement delivered in November 2020, the court underlined the importance of consent requests being presented in a clearly distinguishable manner from other matters in the context of a written declaration. However, the CJEU stated that it is up to the referring court to assess whether the consent checkbox was distinguished enough from other contractual clauses.[159]

The court went on to emphasise that for the data subject to enjoy genuine freedom of choice, the data subject must be given a real possibility of refusing and withdrawing consent as they might otherwise be misled into believing that the contract cannot be concluded otherwise; the right to withdrawal includes information about how to exercise such a right. The court established that consent is not valid where 'the freedom to choose to object to that collection and storage is unduly affected by that controller in requiring that the data subject, in order to refuse consent, must complete an additional form setting out that refusal'. However, the court maintained that it is up to the referring court to determine whether the data subjects being required to sign a separate form were given such a freedom of choice.[160]

3.3.2.3 Unambiguously specific and informed consent

While the referring court requested the CJEU to provide guidance on what constitutes 'freely given', 'specific' and 'informed' consent, the CJEU did not go into the requirements of specific and informed consent, instead commented on the ambiguity of such consent. The notion of unambiguous consent was only mentioned as a requirement for consent to be a clear affirmative action, with reference to the Planet49 case. Nevertheless, the court maintained that the necessary information for, and specificity of, consent is to be determined by the referring court, without further commenting on the content of the consent request. Instead, the court held that for consent to be freely given, specific and informed, the controller must be able to prove it.[161]

[157] Case C-61/19, Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), 11 November 2020, paras. 20-27.
[158] Ibid., para. 32.
[159] Ibid., paras. 39 & 47.
[160] Ibid., paras. 41 & 52.
[161] See the court's findings under the previous section on *Planet49*.

The court concluded that a signed contract with a clause stating that the data subject has been informed of, and consented to, the processing of their data, does not demonstrate consent if the box referring to the clause is pre-ticked and if the contract is capable of being misleading in terms of the right to 'freely given' consent, e.g., the right to information about, and possibility to, refuse and withdraw consent.

In the Opinion to the case, the Advocate General states that if one does not know whether the data subject has read and digested the information, as is the case with pre-checked boxes, consent cannot be unambiguous as the data subject might have conceded 'out of pure negligence'.[162]

Moreover, when assessing the case in question, the Advocate General notes that, while not subject for interpretation as to the referral, hypothetically, Orange Romania has clearly failed to demonstrate the consent. Hence stating that such lack of clarity does not indicate valid consent.[163] While not explicitly stating that there is an obvious lack of unambiguity, based on the problematisation of the case and presented requirements under the law, it is reasonable to understand it as that the consent has been ambiguous, rather than directly uninformed and unspecific.

3.3.3 Author's remarks

In *Planet49* the German court referred questions on the validity of consent in relation to pre-checked boxes. The CJEU provided guidance on the requirements for specific, informed and unambiguous consent while excluding 'freely given' consent. It could be presumed that if the validity of the first checkbox that was conditional for participating in the lottery would have been subject for preliminary ruling, freely given consent would have been expounded on. The judgement in *Planet49* indicates that the criteria are to be differentiated and appointed to separate elements of each predicament.

Contrarily, in *Orange Romania* the court did not explicitly give guidance on the requirements for consent to be unambiguous, despite problematising elements that they themselves have attributed to the notion of unambiguous consent. This could be explained by the fact that the

[162] Opinion of Advocate General Szpunar, Case C-61/19, Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), para. 45.
[163] Ibid., para. 62.

referring court only requested interpretations of ‘freely given’, ‘specific’ and ‘informed’. However, the CJEU still chose to emphasise the essence of unambiguous consent while attributing it to lack of specificity and information. In his opinion, the Advocate General did attempt to make a distinction of the criteria and clarify that pre-checked boxes and difficulty with demonstrating consent precludes unambiguous consent. Yet, in the judgement, there is no such attribution to unambiguity and delineation of the criteria. By not making a clear distinction and providing specific guidance on all of the criteria, the criteria themselves risk becoming ambiguous and thus difficult to interpret.

4 Valid consent under the GDPR: As interpreted by national authorities

4.1 Danish DPA decides against Danish Meteorological Institute's cookie banner

In August 2018, the Danish DPA received a complaint that the website of the Danish Meteorological Institute (DMI) had embedded third-party plugins from Google's ad platform that stored cookies on users' devices without valid consent. While users visiting the website were met by a cookie banner with only an option 'OK' button, cookies were stored before the user had interacted with the cookie banner. A couple months after the complaint, DMI had updated their website, with the cookie banner now having the two options 'OK' and 'Show details', where refusal was only possible if the user first clicked to see more details, where several checkboxes for different specific purposes were pre-ticked. Moreover, the cookie banner used an overlay design so that the users could not access the website until the users had either pressed 'OK' or rejected the request.[164]

In February 2020, the Danish DPA decided against DMI. When addressing consent, the DPA divides their reasoning into the sections of 'freely given' and 'informed'. On whether consent has been freely given, the DPA states that consent could not be obtained by users pressing the 'OK' button as such consent is not granular enough and that the description of purposes was too vague. The DPA noted that despite more granular consent options being available after clicking 'Show details', the use of 'a click away' is a violation of the GDPR. Under the headline 'regarding informed', the DPA states that the consent is not informed as it does not mention that Google is a joint controller and because the purposes are too vague with only general indications.[165]

Noteworthy is that the DPA did not consider whether the criteria 'specific' or 'unambiguous' were met. Despite the fact that this case was decided after *Planet49*, no consideration was made

[164] Datatilsynet, 2018-32-0357, DMI's behandling af personoplysninger om hjemmesidebesøgende, 11 February 2020.
[165] Ibid.

regarding the pre-ticked boxes. The DPAs choice to not address specificity nor unambiguity while discussing elements of such under 'freely given' and 'informed' suggests that the understanding of the consent provision has been challenging. Important to keep in mind is that this case was decided before the release of the EDPB Consent Guidelines.

4.2 Spanish DPA on the ambiguity of double denial

In March 2019 the Spanish DPA received a complaint against a hospital. The claimant claimed when getting admitted after going to the emergency department, they had to fill in a form containing an empty checkbox accompanied by a text stating that if she did not check the box, their personal data would be sent to a third party. After handing in the document without ticking the checkbox, the claimant argued that their consent had not been valid.[166]

In February 2020, the DPA decided against the hospital and decided that such consent had in fact not been given in a way that is required by the GDPR. By referring to Recital 32 GDPR that lays down unambiguous consent as a clear affirmative action excluding passivity, the DPA established that formulating the consent request with a double denial results in that the alleged consent is a result of a data subject's inaction. Thus, the claimant had not given their valid consent and the personal data had been processed unlawfully.[167]

As can be observed, this case shows a different approach from the above-mentioned Danish decision issued during the same month; despite having the same material guiding material to consider, this decision recognizes the requirement of an unambiguous, affirmative action for valid consent.

4.3 Regional Court of Rostock, Germany rules against deceptive cookie banner designs

The Federation of German Consumer Organisations (VZBV) filed a lawsuit against *Advocado*, a German online platform for finding legal services, with the Regional Court of Rostock. The claimant argued that the cookie banners on Advocado's website violated the rules established by the GDPR. Prior to filing the lawsuit, ZVBV had contacted and informed the defendant

[166] Agencia Española de Protección de Datos, Procedimiento No: PS/00187/2019, 25 February 2020, p. 1.
[167] Ibid., p. 8.

about the unlawful collection of data, whereafter Advocado changed their cookie banner. However, ZVBV held that the second cookie banner still was a violation of the GDPR.[168]

The first cookie banner in question had the options 'OK' or 'Show details' as well as four pre-selected checkboxes each in connection to the texts 'Necessary', 'Preferences', 'Statistics' and 'Marketing' with no further information. By clicking on 'Show details' a list of cookies used for the four purposes was shown, without any additional option to deselect any checkbox or refuse processing for the non-necessary cookies altogether. [169]

The updated version of the cookie banner remained as the initial in terms of preselected checkboxes while having changed the two options to 'Allow cookies' and 'Only use necessary cookies'; the 'Allow cookies' had a contrasting green background while the second option to only allow necessary cookies was designed in a way that did not make it clear that it was a clickable button.[170]

In their judgement issued in September 2020, the court ruled against Advocado and concluded the following: Presenting the data subject with only short indications of purposes and naming what cookies are technically to be used does not satisfy the requirement of consent to be informed and specific. Information must be clear, comprehensible and appropriate in relation to the audience, which merely technical naming is not. Moreover, the short declarations accompanying the checkboxes were not specific enough.[171]

This case was tried after *Planet49* and the court upholds that the use of pre-selected checkboxes is unlawful. Additionally, the court makes an observation regarding the updated version of the cookie banner. The fact that it is possible to only allow necessary cookies, does not make the consent freely given as it is not unambiguous. By designing the option to 'reject cookies' in a misleading and deceptive way, unambiguous consent is precluded.[172]

[168] Landgericht Rostock, 3 O 762/19, 15 September 2020, paras. 1-4.
[169] Ibid., paras. 5-7.
[170] Ibid., paras. 82
[171] Ibid., paras. 67-78.
[172] Ibid., paras. 59 & 79-81.

4.4 Danish DPA rules against deceptive cookie banner designs

In October 2021 the Danish DPA found that Ahlstrøm, a Danish retailer, had collected personal data by using cookies without valid consent as their cookie banners did not comply with the requirements for consent under the GDPR. Prior to initiating the investigation of Ahlstrøm's data processing procedures, the company had collected personal data by using two different cookie banners, of which both were found to have been inadequate.[173]

The first cookie banner gave a presentation of the company and informed users that information was collected. The banner had two clickable options: 'Read more about cookies' and 'Close'. The DPA stated that such consent request was not valid as the users were not given a reject option nor was the consent granular and specific.[174]

The second cookie banner was an improvement as it provided the users with more information and empty checkboxes for 'Functional', 'Statistical' and 'Marketing' enabling the users to consent by an affirmative action. However, the banner had two buttons, one with 'Accept' and another with 'ACCEPT ALL' (capital letters). Moreover, the 'Accept' option was written in orange on a white background matching the rest of the cookie banner while the 'ACCEPT ALL' button used a white font with a rectangular orange background. The DPA held that such a difference in design of the two options made it more difficult to refrain than to give consent and thus unduly influenced the data subject's choice. With this, the DPA established that the visual appearance of a consent request must be considered when assessing whether the consent is truly free and unambiguous.[175]

4.5 France v. Big Data's cookies

4.5.1 CNIL's first strike against Google – January 2019

In January 2019 the French DPA, ('CNIL'), imposed their first fine under the GDPR against Google. Individuals who had bought mobile phones with Google's operative system 'Android'

[173] Datatilsynet, Alvorlig kritik af Alstrøm – Din Isenkræmmer ApS' behandling af personoplysninger om hjemmesidebesøgende, 2021-431-0125, 20 October 2021
[174] Ibid.
[175] Ibid.

had to accept Google's terms and conditions when setting up an account in order to use the phones. The terms and conditions included a privacy clause and the button that had to be clicked in order to proceed with the creation of an account was followed by a text stating that by clicking the user consents to the terms and use of information as detailed in the privacy clause. Users were able to click on 'more options' where they could opt-out from processing purposes such as 'display of personalised ads'. As consent must be an affirmative action, CNIL established that pre-ticked boxes preclude unambiguous consent. Moreover, the decision laid down that bundling of purposes under the 'Accept' option, regardless of whether more settings are available in a separate page, did not provide specific consent. CNIL pointed out that the specific purposes must be given granularly before data subjects are given any choice of action. Similarly, as the consent request lacked clear and accessible information on the purposes, users were not able to make informed decisions.[176] CNIL thus ruled that Google's consent request did not satisfy the requirements for specific, informed or unambiguous consent.

4.5.2 CNIL decides against Amazon – December 2020

In December 2020 Amazon was fined by CNIL for using cookies without valid consent. Amazon's cookie banner merely stated that cookies were being placed for service improvement. Users were neither informed or even given a choice as the banner only had an 'OK' option and data was being processed regardless. CNIL held that such a banner was an obvious violation of the GDPR as data was processed from the moment users visited the company's French website and that the alleged consent did not provide sufficient information for consent to be regarded as valid.[177]

Amazon tried to challenge the French DPAs territorial competence and further claimed that it was too difficult to comply with the consent requirements in relation to cookies as there was no common EU doctrine providing clear guidance.[178]

[176] Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC.
[177] Deliberation of the Restricted Committee n° SAN-2020-013 of 07 December 2020 concerning AMAZON EUROPE CORE, paras. 105-106.
[178] Ibid., para. 86.

4.5.3 CNIL's second strike against Google – December 2020

In December 2020 CNIL once again fined Google for violating the consent provisions under the GDPR. First of all, the DPA found that Google had put cookies on users' devices without asking for consent as the only information provided when visiting the search engine was a pop-up asking users if they wanted a reminder on Google's privacy policy. When pressed on 'view now', a brief notice on data processing appeared. However, CNIL held that such information was neither sufficiently clear and complete in terms of processing purposes nor was information provided about the right to make a choice prior to initiating processing of user data. Prior to the proceedings Google had updated their banner options to 'I Accept' and 'More information'. By clicking on the latter users were able to opt-out. Yet, CNIL concluded that such a solution failed to provide information on the ability to reject in the initial layer, thus precluding informed consent. Additionally, when users did opt-out, several advertising cookies remained stored on the devices, making refusal, thus freely given consent, impossible.[179]

4.5.4 CNIL third strike against Google – December 2021

Yet again, one year after CNIL's latest strike against Google's consent solution, the French DPA found that Google had violated data protection rules when processing personal data. This time CNIL looked into the cookie banners on the websites 'google.fr' and 'youtube.com'. The consent banner on the websites offered a one-step option to allow deposit of cookies while refusal required the data subject to select 'Personalise' and then complete a minimum of four additional steps. CNIL held that the GDPR requires consent to be as easy to give as to refuse and that data subjects are equally informed of both options, thus making the consent requests invalid. While emphasising that it is not a strict requirement, the DPA recommends the use of an 'Refuse all' option whenever providing an 'Allow all' button as refusal must be as simple as consent on the first layer of the banner.[180]

Google opposed the proceedings by claiming that the principle of *ne bis in idem* hindered ruling on the same facts as already tried during the deliberations the previous year. CNIL dismissed such a claim and stated that while the previous case addressed the failure to provide users with,

[179] Deliberation of the Restricted Committee n° SAN-2020-012 of 07 December 2020 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED.
[180] Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED.

on the one hand, a choice to refrain from cookies, and on the other hand adequate information on the processing and means to refusal/withdrawal. The preceding case concerned information and the means to refuse cookies, whereas the current case concerns the methods of such refusal.[181]

Google requested CNIL to refer a question on whether the absence of a 'refuse all' button in this case should be regarded as a violation of Article 4(11) and Article 7 of the GDPR to the CJEU for a preliminary ruling. As CNIL is not a court as defined by the TFEU they lack such capacity, thus dismissing Google's request.[182]

4.5.5 CNIL decides against Facebook – December 2021

The same day as Google was struck by CNIL's sanctions, the French DPA imposed a 60 million Euro fine for unlawful processing of personal data. To enter the social network website a cookie banner had to be interacted with whereas the two options provided were 'Accept all' and 'Manage data settings'. When the latter option was chosen, checkboxes concerning specific processing purposes were empty, requiring the user to actively consent to each purpose before continuing with the option 'Accept cookies'. Regardless, CNIL maintained that the option to 'Accept all' was easier and simpler than rejecting consent, thus a violation of consent as defined by the GDPR. Additionally, by referencing a university study on how consent pop-up designs influence people, the DPA introduced the term 'Dark patterns', a deliberate use of deceptive design patterns used to trick data subjects into giving consent.[183]

4.6 Cross-border action against IAB Europe's Transparency and Consent Framework ('TCF')

During 2019 various NGOs filed four complaints with the Belgian DPA and five with DPAs in other Member States against Interactive Advertising Bureau Europe ('IAB Europe'). As IAB Europe has their only registered office in Belgium, the Belgian DPA declared themselves as the lead supervisory authority and the nine actions were merged into one cross-border case.[184] In

[181] Ibid.
[182] Article 267 TFEU.
[183] Deliberation of the restricted committee No. SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED.
[184] DOS-2019-01377.

February 2022 the Belgian DPA, in agreement with all 27 Member States' DPAs, ruled that IAB Europe's Transparency and Consent Framework ('TCF') violated various GDPR provisions, such as by processing personal data unlawfully.[185]

IAB Europe's TCF is a set of policies and specifications providing the European advertising technology ('AdTech') industry with guidance on how to provide accountability and transparency when processing personal data, based on e.g., consent, in real-time bidding ('RTB'). According to IAB Europe, the TCF provides best practice guidance on the requirements for lawfulness under the GDPR and ePrivacy Directive.[186] The TCF governs 80% of the European internet and is relied upon by most AdTech players, including major companies such as Google, Amazon, and Microsoft.[187]

Generally, online advertising uses RTB, a programmatic advertising system, in order to automatise and personalise the placement of advertisements. Working behind the scenes of websites and apps, RTB works as an instantaneous auction ('Ad exchange') where thousands of advertisers using demand-side platforms ('DSPs'), algorithmically bid for an advertising space with publishers using sell-side platforms ('SSPs'). Data Management Platforms ('DMPs') collect immense volumes of personal data from various sources, e.g., cookies and from third party data brokers, and centralises such data enabling the creation of advanced categorisations and profiling.[188] RTB can be exemplified as follows:

A user surfing the internet clicks on a link to visit a news site. The second the link is clicked on, the news site (publisher) signals the SSP. If the user has consented to cookies or other means of tracking, the SSP is informed. The SSP gathers the available data on the user and sends a bid request to the Ad exchange, the auction of RTB. If the SSP has access to information about what previous websites the user has visited, what they have searched for, the gender, location or mobile operator of the user, such information is provided in the Ad exchange. DSPs, using DMPs enrichment data, create a profile of the user and match the user to ads. The advertisers with the best profile matches bid for the ad space on the news site and the highest bidding advertiser gets their ad displayed for the user to see.[189]

[185] Ibid., paras. 1-13.
[186] Ibid., para. 37 & 39.
[187] Irish Council for Civil Liberties, 'GDPR enforcer rules that IAB Europe's consent popups are unlawful', 5 February 2022.
[188] DOS-2019-01377, paras. 20-27.
[189] See Ibid., paras. 24-29.

Included under the scope of the TCF are Consent Management Platforms ('CMPs') that provide data controllers with cookie consent banner solutions. When a user interacts with such a cookie consent banner, the CMP generates a Transparency and Consent String' ('TC String') that captures and stores the user consent preferences.[190] In the 127-page decision, it was established that TC Strings consisted of personal data and that IAB Europe was identified as the controller for the TCF.[191] Amongst the many GDPR infringements, the DPA found that personal data collected under the TCF by using CMPs with TC Strings was unlawful considering that the criteria for valid consent under the GDPR had not been met.[192]

The cookie banners did not enable data subjects to give informed consent as the banners lacked an overview of the categories of data collected. Additionally, within RTB as dictated by the TCF, consent has been given to numerous data controllers whose identities data subjects have not had access to, prior to consenting. However, the number of recipients to whom consent is given to would make information about all controllers practically impossible to digest.[193] Finally, the users were unable to give informed consent due to the inability to in advance determine the scope and consequences of the processing of their data under the above mentioned RTB model.[194] Conjointly, consent has not been granular as the information provided by the CMPs has been too general to indicate specific processing operations of each actor within the RTB ecosystem.[195]

When a user gives consent by interacting with a cookie banner, a series of instantaneous operations are launched where the TC String carrying personal data is transmitted between numerous actors. If a data subject later withdraws consent as instructed by the cookie banner, the various actors processing their personal data in accordance with the TCF no longer have

access to the new consent signal. As the signal withdrawing consent does not reach the controllers processing personal data, withdrawal becomes virtually impossible. As users cannot withdraw consent as easily as giving it, such consent cannot be valid.[196]

[190] Ibid., paras. 40-41.
[191] Ibid., para. 44.
[192] Ibid., paras. 424 & 440.
[193] Ibid., paras. 434-435.
[194] Ibid., para. 469.
[195] Ibid., para. 436.
[196] Ibid., para. 438.

4.7 Author's remarks

In the first Danish decision against the Danish Meteorological Institute, the DPA refrains from considering whether consent has been specific and unambiguous, despite the decision being delivered after the guidance provided by the CJEU in *Planet49* and before CJEUs judgement in *Orange Romania*. Moreover, the DPA does problematise the vagueness of purposes without attributing it to a shortcoming of the need for specific consent. However, almost two years later, in the decision against Ahlstrøm, the Danish DPA applied a far stricter interpretation of the criteria as well as the distinction therein. On the one hand, this development might show how initial lack of guidance from EDPB leads to misinterpretations of the provisions, and on the other hand how the national DPAs look to each other for guidance. Between the two Danish decisions, the German court established a high threshold for unambiguous consent by introducing the chastising of 'dark patterns'. Additionally, the French DPA had a similar approach to the German DPA, perhaps adding to the pressure to interpret the provisions in a certain way. While the national authorities' decisions do not directly change the legal discourse beyond their respective jurisdictions, the European legal method entails reliance on interpretations made by other Member States.

Noteworthy is that the Danish DPAs reasoning, in regard to their first decision, differed considerably from the Spanish decision. This indicates that there is room for interpretation on the notion of consent, resulting in fragmentation at national level which counteracts the GDPRs aim of harmonisation. Similarly, it is obvious the French DPA has significantly raised the threshold for consent without directions from the CJEU or EDPB. Not only has CNIL chosen to actively enforce the GDPR with a strict interpretation of the criteria for consent, CNIL has also established, and perhaps introduced, a requisite to strictly delineate the criteria as such a distinction might predicate the assessment of *ne bis in idem*. While CNIL's unparalleled approach risks fragmentation within the union, the emphasis on the interpretation's effect on *ne bis in idem* further highlights the importance of a harmonised approach.[197]

[197] Ne bis in idem is fundamental for the free movement within the European are of freedom, security and justice, See Article 54 of The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, Official Journal L 239, 22/09/2000 P. 0019 – 0062; See also Article 50 CFR.

As the recent decision against IAB Europe is a cross-border action with all Member States on board, the interpretation of the criteria for consent in relation to RTB and CMPs succeeds with establishing uniformity and harmonising the legal discourse. However, while the free movement of data is facilitated, such interpretation of consent might disregard technological neutrality as well as adventure fundamental rights and freedoms. The Belgian led decision declared that the standard practice within an entire industry is illegal; while consent is required by the ePrivacy Directive, consent is virtually precluded. The Belgian DPA stated that the consent banners did not provide obligatory information, e.g., identity of all controllers. Paradoxically, the decision noted that if such information was to be provided, it would be impossible to digest and thus not clear enough to meet the requirement for clear information. Additionally, the DPA concluded that the consent requests failed to provide the necessary information for data subjects to in advance determine the scope and consequences of the processing. However, the requirement is not possible to meet within RTB as such an AdTech solution is based on automated operations where the outcome is not possible to know prior to giving consent. Consequently, in relation to this particular technology consent and thus lawfulness can currently be deemed as unattainable.

In the light of technological neutrality, such interpretation and enforcement of the consent provisions is problematic. On the one hand, the interpretation shows that the GDPR truly can be applied to an array of technologies; on the other hand, however, the DPAs interpretation does discriminate against the use of a particular technology and it does hinder the technological development without reflecting on the technology's role in society from a larger perspective. One reason for entailing technological neutrality with respect to the GDPR is to maintain the synergy with technological advancements. Reading this together with the GDPR's goal to contribute to the accomplishment of economic and social progress, suggests that the provisions under the GDPR must be interpreted in a way that facilitates both economic and social growth without preventing the advancement of technologies.

While the strict interpretation is a means to protect data subjects' personal data and thus succeeds with safeguarding the right to protection of personal data under the CFR, it can be debated whether the right to data protection has been proportionally balanced against other rights and freedoms.

5 Recent developments and noteworthy proceedings

5.1 EDPS – Case 2019-0878 against the CJEU

This particular case was not brought before the CJEU, instead Case 2019-0878 was brought to the EDPS against the CJEU.[198] It is not an interpretation of EU Law by the CJEU as a judicial authority, instead it sheds light on the almost ironically perpetual negligence of the conditions for valid consent.

In October 2019, ensuing the ruling in *Planet49*, the EDPS received a complaint stating that the CJEU's main website (curia.europa.eu) requested consent for the use of cookies in a way that violates the consent requirements as stipulated by the GDPR. The complainant alleged that the cookie banner on the website offered the options 'OK' and 'More Information', making it more difficult to refuse consent than to give consent. By the time of the complaint reaching the EDPS, the CJEU had rectified their cookie banner. The complainant however, responded that unlawful processing persisted as the cookies put on his device prior to the complaint remained. Additionally, the complainant added that the third-party services hosting CJEU's videos, branded under the CJEU, stored cookies without even informing of such processing and thus without prior consent.[199]

The EDPS concluded that the CJEU had violated the provisions on consent under the GDPR. However, as the CJEU remedied the infringements soon after the submitted complaint, the EDPS refrained from exercising his corrective powers.[200]

[198] Decision of the European Data Protection Supervisor in complaint case 2019-0878 submitted by Mr Michael Veale against the Court of Justice of the European Union, 03 May 2021.
[199] EDPS, Case 2019-0878, pp. 1-3.
[200] Ibid., p. 8.

5.2 C-129/21 - Proximus (Pending)

5.2.1 Background

While case C-129/21 is still pending and yet to be decided by the CJEU, Advocate General Collins issued his Opinion in April 2022.[201]

The Court of Appeal in Brussels, Belgium requested a preliminary ruling on the interplay between the GDPR and the ePrivacy Directive in terms of requirements for consent.[202] The case arises from that a customer to Proximus, a telecommunications service, requested that his telephone number, that was collected based on consent, would be removed from public electronic telephone directories and directory enquiry services. Despite Proximus initially removing the complainant's number from their services, a couple months later the complainant discovered that his number was made public.[203]

The ePrivacy Directive proclaims that in respect of data processing by providers of electronic telephone directories and directory enquiry services, consent obtained by a data subject at a single instance can be relied upon by other providers of directories. On the other hand, the GDPR requires that each controller must obtain separate consent from the data subject for the processing of their personal data. One consequence of this discrepancy is that when the data subject wishes to withdraw consent, his singular consent has been used by multiple controllers, making the withdrawal of consent non-consistent with the requirements for consent under the GDPR. [204]

5.2.2 Freely given consent

The Advocate General notes that consent under the ePrivacy Directive must be interpreted in accordance with the requirements for consent under the GDPR.[205] When consent for the purpose of being included in directories is withdrawn, any further processing for that specific purpose is no longer lawful, including the processing by other controllers as consent is given to, and

[201] Opinion of Advocate General Collins, Case C-129/21, Proximus NV (Public electronic directories) v Gegevensbeschermingsautoriteit**,** Delivered on 28 April 2022.
[202] C-129/21, para. 1.
[203] Ibid., paras. 3-10.
[204] Ibid., para. 2.
[205] Ibid., para. 48.

withdrawn from, a specific purpose. As withdrawing consent should be as easy as giving consent, the Advocate General suggests that a data subject should be able to approach any of the controllers that rely on that single consent; the chosen controller should thereafter be responsible for making sure that all processing based on the singular consent for that specific purpose ceases.

While the CJEU has not issued a preliminary ruling yet, the Opinion indicates that for consent to be valid as a legal basis, withdrawal of such consent must be enabled in accordance with the requirements for freely given consent. As a consequence, many controllers may have to re-evaluate their processing activities and implement new measures in order to be able to comply with the provisions under the GDPR.[206]

5.2.3 Unambiguous consent

If consent collected in accordance with the ePrivacy Directive is to satisfy the requirements for valid consent as defined by the GDPR, the validity of such consent must be demonstrable and unambiguous. The Advocate General remarks on the challenge in respect to demonstrating the validity of consent that has been given to, and later derived from, another controller.[207]

5.3 C-252/21 - Facebook and Others (Pending)

The most recent development in case law that touches on the notion of consent is the referral for a preliminary ruling by the CJEU by the Higher Regional Court of Düsseldorf, Germany, on the clarification of provisions under the GDPR, inter alia, the validity of consent. [208]

Even though the case has not been attended yet, it has already caught the public's attention.[209] Originally, this was a case on competition law examining the dominant position of Facebook in the social network's market.[210] The German competition authority ruled that Facebook holds a dominant position and thus imposed several restrictions, such as restraining Facebook from further processing personal data without consent in accordance with the GDPR. Facebook

[206] Ibid., para. 69.
[207] Ibid, para. 45.
[208] Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on 22 April 2021, Facebook Inc. and Others v Bundeskartellamt, (Case C-252/21).
[209] See e.g., Reuters, 'Meta criticises German antitrust watchdogs flawed data curb order', May 2022; Eu Law Live, 'Preliminary ruling request on the collection and use of data by Facebook Ireland published', August 2021.
[210] Bundeskartellamt, B6-22/16, 15 February 2019.

appealed such a decision to the Federal Court of Justice of Germany, which ultimately ruled against Facebook. The competition authority claimed that Facebook made their services conditional on the collection of user data, without obtaining valid consent.[211] Facebook claimed that their processing of data is lawful on the grounds of on the one hand fulfilment of contract, and on the other, legitimate interest.[212] The court however, judged in line with the authority that contended such a claim and concluded that Facebook could not rely on such grounds and that users' consent had to be obtained for the processing to be lawful. Subsequently, the competition authority referred to the consideration of imbalance of power regarding freely given consent under the GDPR and held that in the view of Facebook's dominant position, users' consenting to Facebook's terms and conditions cannot provide their free consent to processing of their data within the meaning of the GDPR as such consent is a result of coercion.[213]

The case made it to the Regional Court of Düsseldorf where the court in April 2021 lodged a request for a preliminary ruling on an extensive list of questions on the interpretation of EU Law. While one question referred to the assessment of appropriate legal basis, the sixth question targets the interpretation of valid consent: Can consent, as defined by the GDPR, be given freely to a dominant undertaking such as Facebook?

5.4 BEUC against Google

On 30th of June 2022, the European Consumer Organisation ('BEUC') sent a letter to the Commissioner for Justice at the EC announcing their launch of a coordinated GDPR enforcement action against Google. The BEUC and ten of its members called for the EDPB and DPAs to prioritise Google's GDPR infringements in line with the EDPB's Statement on enforcement cooperation adopted in Vienna April 2022. The different national consumer groups have sent complaints to their respective DPAs about Google's actions in hope that a cross-border operation will be initiated.[214]

[211] Ibid., p. 1.
[212] Ibid., p. 3.
[213] Ibid., pp. 8 & 10.
[214] BEUC, BEUC-X-2022-074/MGO/UPA/rs, 30 June 2022.

5.5 Author's remarks

Companies as Google and Facebook have an obvious financial interest in claiming consent regardless of its genuine validity and their violations of the GDPR might be blamed on intentional negligence, the criteria can be difficult to comprehend and comply with. Despite the fact that the CJEU is the highest interpretive authority as well as processing of personal data on their website is superfluous for their operations, the CJEU still managed to violate the GDPR. While the EDPSs decision against CJEU does not add to the interpretation of the criteria for consent, it does suggest that the criteria are difficult to meet, which is problematic with respect to the rationale.

The CJEU is yet to rule in *Proximus*. However, the opinion by the Advocate General illustrates yet another case of where consent is not virtually possible within certain technologies and operations. Similarly to the decision against IAB Europe as examined under sub-chapter 4.6, the Advocate General's opinion indicates that for some processing activities that are required to obtain consent under other laws, consent is impossible, thus the technology is automatically unlawful. Consequently, the consent provisions fail to be technologically neutral.

While the CJEU still has not voiced their opinion in C-252/21 *Facebook and Others*, the extent of how broadly the criteria can be interpreted is illustrated. The German Federal Court of Justice ruled in favour of the German competition authority that during the proceedings asserted that, as Facebook is a dominant undertaking in accordance with EU Competition Law, there is a power imbalance that precludes freely given consent. As this case and its binding powers are restricted to Germany, it does not directly dictate the definition of valid consent under the GDPR. However, it illuminates the wide range of interpretation and perhaps even unpredictability of the criteria. The court's particularly strict interpretation and enforcement of the requirements for 'freely given' consent has most likely added to the fragmentation of Data Protection within the Union as the disparate threshold for valid consent interferes with a uniform application of EU law. The interpretation of the criteria for valid consent as upheld by the German court might be correct as the WP29 has made it clear that coercion encompasses all forms of coercion. However, neither Recital 43 GDPR nor EDPB (see sub-section 3.2.1.2), has expressed that the requirement of absence of imbalance of power is absolute. Where the line is drawn is not clear. If the rationale was best ensured by completely forbidding all instances of power imbalances, there would reasonably not be room for interpretation. However, the

rationale is dual and the fundamental rights and freedoms must be balanced proportionally. The lack of guidance on how such balancing is to be approached has plausibly led to the unprecedented discernment that is seen in Germany.

The dissatisfaction with on the one hand lack of compliance, and on the other hand fragmentation of EU Data Protection law has been made clear by BEUCs united launch against Google. Alongside the initiatives by nyob as mentioned under sub-chapter 1.1, the launch of coordinated enforcement actions highlights the perpetual violations with regard to invalid collection of consent.

6 Concluding remarks

6.1 Ambiguous criteria

While Amazon's claim that the provisions were too difficult to comply with due to lack of common EU doctrine providing guidance was a rather futile excuse considering the obvious violation, there might have been some legitimacy in their claim. As shown, compliance has been indisputably inadequate and perhaps it is too unclear what the criteria require as even the CJEU encountered difficulties in regard to compliance.

While it is clear that freely given consent aims at capturing the genuine will of a data subject by acknowledging all forms of coercion, the limits to what is considered as inappropriate and unduly coercion are unknown. Similarly, it is not clear where the line is drawn between enough and too much information. Additionally, there is ambiguity regarding the distinction of the four criteria; while the CJEU in *Planet49* attributed different elements to specific criteria, the criteria were deliberated *en masse* in *Orange Romania*. CNIL elevated the importance of differentiation of criteria by basing the *ne bis in idem* assessment on such a distinction, thus showing that clearly outlining each condition is imperative.

The different interpretations of the GDPR consent provisions cannot be solely based on the Member States' diverging interests and balancing of rights and freedoms as the Danish DPAs significantly different approaches indicate that the criteria themselves are ambiguous.

There are several risks with ambiguous criteria; on the one hand, it gives more room for private actors to provide soft law. As soft law *de facto* is given considerable authority within the European Legal Methodology, private actors end up steering EU law implementation, thus risking jeopardising the intended goals of EU Law as private actors plausibly interpret provisions in benefit of their interests. Moreover, as seen with the TCF, soft law might be determined as unlawful by authorities. On the other hand, discrepancies in interpretation and enforcement amongst Member States give rise to fragmentation, thus contravening harmonisation and free flow of data within the Union.

6.2 Free flow of data within the Union

If the criteria leave room for interpretation, fragmentation is likely inevitable. Part of the rationale is to protect the free movement of data as one goal of the GDPR is to contribute to an area of freedom, security and justice and of an economic union. Thus, fragmentation contravenes the rationale.

France has interpreted the criteria in a strict manner and put a higher threshold for valid consent under the GDPR than many other Member States. Companies conducting business across several Member States, as most businesses operating in the digital realm do, must now conduct separate assessments for each state and cannot freely and lawfully transfer collected data across the Union. As indicated by the cross-border action led by the Belgian DPA against IAB Europe, EDPBs Statement of enforcement cooperation along with BEUCs coordinated enforcement action, there is a need for a more uniform approach.

6.3 Technological Neutrality

Technologies are being cornered as compliance with the consent provisions is practically impossible while still legally required by the ePrivacy Directive. Such a consequence of the GDPR contradicts the intention of the GDPR to be technologically neutral.

While the heightened requirements for e.g., unambiguity by introducing the consideration of dark patterns, does prevent circumvention of the GDPR as intended, a heightened threshold can come with a price. If the provisions are not practically possible to adhere to, the legislation essentially fails with regard to its rationale.

6.4 Safeguarding fundamental rights and freedoms

Part of the GDPR's rationale is to protect fundamental rights and freedoms while the right to protection of data is central, it must be proportionally balanced to other fundamental rights and freedoms. E.g., when examining 'freely given' consent, it is clear that the condition is vital to retain control of personal data with the data subject. However, when the limits of the criteria are unclear, there is a risk that other fundamental rights and freedoms are put at risk.

Remembering that personal data is currency that data subjects use to pay for services provided by companies that have built their business models around consumer data, necessitates an assessment of the consequences of a rather absolute approach to data protection. While the CJEU is yet to provide a preliminary ruling on whether it is possible to consent to Facebook due to a power imbalance, the German court's decision fails to provide a solution that does not compromise other interests than protection of data. If Facebook, or perhaps Google, would no longer be allowed to process personal data by using RTB and relying on the revenue from AdTech, users might have to pay with actual money instead. It is questionable whether such consequences would serve mankind and contribute to economic and social progress within the Union as prescribed by the rationale. It is furthermore questionable whether the hindrance of certain technologies is balanced against fundamental rights and freedoms; obstructing entire industries might not be optimal for the protection of the freedom to conduct business; forcing social communications services to no longer offer free access regardless of financial wealth, could have negative implications on the freedom of expression and information. While further research is needed in order to assess the consequences on the different fundamental rights and freedoms, it can be noted that the current consent criteria might be problematic in relation to the rationale. As recital 6 GDPR recognises the importance of technology for economic and social life, the disproportionate strain on technology that is currently put as a result of the consent criteria, does not align with the goal of the GDPR.

Additionally, as mentioned above, if the provisions are not possible to comply with, the rationale is jeopardised. If consent, which is supposed to be the cornerstone of data protection, fails to protect individuals' data autonomy, there might be something fundamentally wrong with the current EU data protection regime.

6.5 Barking up the wrong tree

While perhaps reaching beyond the scope of this paper, it is of relevance to note that the issues that arise from the interpretation of the criteria for consent under the GDPR in regard to the rationale might be an issue of when consent is required rather than the essence of consent. After all, the criteria themselves are aimed at ensuring that consent is an expression of individuals' genuine and bare wishes. However, consent is forced to be relied on when perhaps other legal bases would be more suitable. Perhaps, in the light of the rationale and technological neutrality,

the criteria for valid consent under the GDPR are neither good or bad, but rather dependant on the context and whether its limits are fairly considered.

Bibliography

International Instruments

The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, Official Journal L 239, 22/09/2000 P. 0019 – 0062.

European Union Instruments

EU Treaties

Charter of Fundamental Rights of the European Union, 2000/C 364/01, ('CFR').

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007); entry into force on 1 December 2009.

Treaty on European Union (Consolidated version 2016), OJ C 202, 7.6.2016.

Treaty on the Functioning of the European Union, OJ C 202, 76.2016 ('TFEU').

EU Regulations

General Data Protection Regulation 2016: 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, As consolidated by the Corrigendum to General Data Protection Regulation, May 2018 ('GDPR').

EU Directives

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 (Directive on privacy and electronic communications), ('ePrivacy Directive').

Directive 2009/136/EC of the European Parliament and 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.

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, ('DPD').

EU Recommendations

Court of Justice of the European Union, Recommendations to National Courts and Tribunals in relation to the initiation of Preliminary Ruling Proceedings, 2019/C 380/01, 08 November 2019.

European Data Protection Board, European Data Protection Supervisor and Art 29 Working Party Documents

European Data Protection Board ('EDPB') Documents

EDPB, Endorsement 1/2018, Brussels, 25 May 2018.

EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, Adopted on 04 May 2020, ('EDPB Consent Guidelines').

EDPB, Statement on enforcement cooperation, Adopted on 28 April 2022.

European Data Protection Supervisor ('EDPS') Documents

Decision of the European Data Protection Supervisor in complaint case 2019-0878 submitted by Mr Michael Veale against the Court of Justice of the European Union, 03 May 2021.

Art 29 Working Party ('WP29') Documents

Guidelines on consent under Regulation 2016/679, 17/EN, WP259 rev.01.

Opinion 04/2012 on Cookie Consent Exemption, 00879/12/EN, WP 194, Adopted on 07 June 2012.

Opinion 15/2011 on the definition of consent, 01197/11/EN, WP187, Adopted on 13 July 2011, ('WP187').

Opinion 2/2010 on online behavioural advertising, 00909/10/EN, WP 171, Adopted on 22 June 2010.

WP29 Opinion 3/2013 on purpose limitation, 02 April 2013.

European Commission Documents

European Commission, Brussels, 25.1.2012 COM(2012), 11 final 2012/0011 (COD), Proposal for a Regulation Of The European Parliament and the Council on the protection of individuals

with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), ('GDPR Proposal').

Commission of the European Communities, Brussels, 10.11.1999 COM (1999) 539 final, 'Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Towards a new framework for Electronic Communications infrastructure and associated services – The 1999 Communications Review'.

National Data Protection Authorities' ('DPAs') Decisions

Belgium

DOS-2019-01377, Autorité de protection des données Gegevensbeschermingsautoriteit, Litigation Chamber, Concerning: Complaint relating to Transparency & Consent Framework, Decision on the merits 21/2022 of 2 February 2022.

Denmark

Datatilsynet, DMI's behandling af personoplysninger om hjemmesidebesøgende, 2018-32-0357, 11 February 2020.

Datatilsynet, Alvorlig kritik af Alstrøm – Din Isenkræmmer ApS' behandling af personoplysninger om hjemmesidebesøgende, 2021-431-0125, 20 October 2021.

France

Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC.

Deliberation of the Restricted Committee n° SAN-2020-012 of 7 December 2020 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED.

Deliberation of the Restricted Committee n° SAN-2020-013 du 7 December 2020 concerning AMAZON EUROPE CORE, paras. 105-106.

Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED.

Deliberation of the restricted committee No. SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED.

Spain

Agencia Española de Protección de Datos, Procedimiento No: PS/00187/2019, 25 February 2020.

Table of cases

Court of Justice of the European Union ('CJEU')

Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, 05 June 2018.

Case C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, 29 July 2019.

Case C-673/17, Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbrauchrverbände – Verbraucherzentrale Bundesverband e.V, 01 October 2019.

Case C-61/19, Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), 11 November 2020.

Cases C-131/12, Google Spain SL, Google Inc. V Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 13 May 2014.

National Courts

France

Conseil d'Etat, N° 430810, Sanction infligée à Google par la CNIL, 19 June 2020.

Germany

Bundeskartellamt, B6-22/16, 15 February 2019.

Landgericht Rostock, 3 O 762/19, 15 September 2020.

Literature

Beyleveld, Deryck & Brownsword, Roger, Consent in the Law, Legal Theory Today, Hart Publishing, Oxford and Portland, 2007.

Bieker, Felix, 'The Right to Data Protection - Individual and Structural Dimensions of Data Protection in EU Law', Information Technology and Law Series, Volume 34, Springer, Germany, 2022.

Brinnen, Martin & Westman, Daniel, 'What's wrong with the GDPR? Description of the challenges for business and some proposals for improvement', Svenskt Näringsliv, December 2019, Available at https://www.svensktnaringsliv.se/material/skrivelser/xf8sub_whats-wrong-with-the-gdpr-webbpdf_1005076.html/What%27s+wrong+with+the+GDPR+Webb.pdf (Accessed 10 July 2022).

IT Governance Privacy Team, 'EU General Data Protection Regulation (GDPR) - An implementation and compliance guide', Fourth edition, IT Governance Publishing, United Kingdom, 2020.

Kosta, Eleni, 'Consent in European Data Protection Law', Nijhoff Studies in EU Law, Volume 3, Martinus Nijhoff Publishers, Leiden, 2013.

Kuner, Christopher, Bygrave, Lee A., Docksey, Christopher & Drechsler, Laura, The EU General Data Protection Regulation: A Commentary, Impression: 1, Oxford University Press, 2020.

Lanham Napier, Jim Curry, Barry Libert & K.D. de Vries, 'Modern Business Models Will Drive the Post-Pandemic World', MIT Sloan Management Review, 2020-08-17, Available at https://sloanreview.mit.edu/article/modern-business-models-will-drive-the-post-pandemic-world/ (Accessed 09 July 2022).

Nääv, Maria & Zamboni, Mauro, Juridisk metodlära [Electronic book, (DAISY 2.02)], 2nd edition, Studentlitteratur, Lund, 2018.

Politou, Eugenia, Alepis, Efthimios, Virvou, Maria & Patsakis, Constantinos, 'Privacy and Data Protection Challenges in the Distributed Era', Learning and Analytics in Intelligent Systems, Volume 26, Springer, Switzerland, 2022.

Reed, Chris, 'Taking Sides on Technology Neutrality', SCRIPT-ed, Volume 4, Issue 3, September 2007, pp. 264-266.

Sharma, Sanjay, 'Data Privacy And GDPR Handbook', Wiley, New Jersey, 2020.

Varadarajan, Rajan, 'Customer information resources advantage, marketing strategy and business performance: A market resources based view', Industrial Marketing Management, Volume 89, August 2020, Pages 89-97, Available at

https://www.sciencedirect.com/science/article/abs/pii/S0019850120300389?via%3Dihub (Accessed 09 July 2022).

Walker, Neil, 'Legal Theory and the European Union: a 25th Anniversary Essay, Oxford Journal of Legal Studies, Vol. 25, No. 4, 2005, pp. 581-601.

Digital sources

EDPB,'Who we are', https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en (Accessed 18 June 2022).

EFTA, European Free Trade Association, 'General Data Protection Regulation incorporated into the EEA Agreement', Published 06 July 2018, https://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291 (Accessed 19 June 2022).

EU Law Live, 'Preliminary ruling request on the collection and use of data by Facebook Ireland published', 09 August 2021, https://eulawlive.com/preliminary-ruling-request-on-the-collection-and-use-of-data-by-facebook-ireland-published/ (Accessed 24 July 2022).

European Commission, 'Infringement Procedure', https://ec.europa.eu/info/law/law-making-process/applying-eu-law/infringement-procedure_en#non-compliance (Accessed 26 June 2022).

European Commission, Newsroom, 'The Article 29 Working Party ceased to exist as of 25 May 2018', Published 11 May 2018, Https://ec.europa.eu/newsroom/article29/items/629492/en (Accessed 18 June 2022).

Eurostat, 'Internet use and activities', 2020, Individual type: Individuals living in cities, individuals living in towns and suburbs and individuals living in rural areas, Information society indicator: Frequency of internet access: daily, 2021, European Union, 27 Countries, <https://ec.europa.eu/eurostat/databrowser/view/isoc_bde15cua$DV_289/default/table?lang=en> (Accessed 09 July 2022).

FRA, European Union Agency For Fundamental Rights, 'Technological advances and data protection should go hand-in-hand', 28 January 2021, https://fra.europa.eu/en/news/2021/technological-advances-and-data-protection-should-go-hand-hand (Accessed 10 July 2022).

GDPR.eu, 'Cookies are an important tool that can give businesses a great deal of insight into their users' online activity. Despite their importance, the regulations governing cookies are split between the GDPR and the ePrivacy Directive', https://gdpr.eu/cookies/ (Accessed 17 July 2022).

IMY, ’Lawful grounds for personal data processing’, Latest updated 17 May 2022, https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/lawful-grounds-for-personal-data-processing/ (Accessed 06 July 2022).

InfoCuria, Case-law, List of documents, https://curia.europa.eu/juris/recherche.jsf?language=en (Accessed 29 July 2022).

Irish Council for Civil Liberties, ‘GDPR enforcer rules that IAB Europes consent popups are unlawful’, Updated 5 February 2022, https://www.iccl.ie/news/gdpr-enforcer-rules-that-iab-europes-consent-popups-are-unlawful/ (Accessed 29 July 2022).

Noyb, ‘More Cookie Banners to go: Second wave of complaints underway’, 04 March 2022, https://noyb.eu/en/more-cookie-banners-go-second-wave-complaints-underway (Accessed 09 July 2022).

Reuters, ’Meta criticises German antitrust watchdogs flawed cata curb order’, 10 May 2022, https://www.reuters.com/technology/meta-criticises-german-antitrust-watchdogs-flawed-data-curb-order-2022-05-10/ (Accessed 24 July 2022).

Miscellaneous

BEUC, BEUC-X-2022-074/MGO/UPA/rs, 30 June 2022, Available at https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-074_letter_to_commissioner_reynders_-_google_gdpr_action.pdf.

LIBE draft report 2012/0011 (COD) dated Dec. 17, 2012 (12 PVLR 65, 1/14/13), Available at https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf, (the Albrecht Report).

Opinion of Advocate General Collins, Case C-129/21, Proximus NV (Public electronic directories) v Gegevensbeschermingsautoriteit, Delivered on 28 April 2022.

Opinion of Advocate General Szpunar, Case C-61/19, Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)

Request for a preliminary ruling from the Hof van beroep te Brussel (Belgium) lodged on 02 March 2021 – Proximus NV v Gegevensbeschermingsautoriteit, (Case C-129/21).