EU Data Protection Law in Action: Introducing the GDPR

Julia Krämer

Abstract

This chapter is intended to introduce the General Data Protection Regulation (GDPR) to social scientists, offering an overview of key legal concepts and provisions from Chapters II and III of the Regulation. The chapter has two main objectives: first, to bridge the gap between empirical and doctrinal research by explaining fundamental GDPR provisions to non-legal audiences; and second, to examine the extent to which these provisions have been explored through empirical research. This includes identifying common methods used, revealing that, only six years after the Regulation's implementation, a rich body of empirical research has emerged to evaluate its effectiveness. The chapter concludes with a discussion of the challenges social scientists face when empirically investigating the impact of the GDPR, such as translating empirical findings into legal conclusions.

1. Introduction

In May 2018, the implementation of the General Data Protection Regulation (GDPR) represented a landmark moment in EU data protection law. As the new legal framework governing the processing of personal data within the EU, the GDPR replaced the outdated provisions of the 1990s, which were drafted when the internet was still in its infancy. Six years after its implementation, the GDPR still stands out as one of the most advanced data protection laws globally (Streinz, 2021, p. 903), prompting questions and reflections on its actual impact. Prior to its implementation, some authors have claimed that the GDPR would not only change EU data protection law, but "nothing less than the whole world as we know it" (Albrecht, 2016, p. 287). Today, six years after the GDPR became enforceable, the empirical reality can help ascertain whether such statements and hopes have been exaggerated or accurately reflect the law's actual impact, and whether the Regulation can succeed in achieving its desired outcomes.

At the heart of the GDPR lies a dual objective: safeguarding fundamental rights and ensuring the free flow of personal data across the EU (Hijmans, 2020, p. 56). As a Regulation, the GDPR harmonises the rules concerning the processing of personal data and is directly applicable in EU Member States. This shift, however, does not imply that national data protection law is no longer applicable. The GDPR contains several opening clauses that permit Member States to establish more specific rules beyond those outlined in the Regulation. The GDPR marks a significant shift from the previous framework, the Data Protection Directive (DPD) (Directive 95/46/EC), which obligated Member States to implement provisions in national law first, resulting in the fragmentation of data protection rules across the EU (Recital 9 GDPR, Regulation (EU) 2016/679). While the shift from Directive to Regulation presented a significant legal transformation, most core concepts and principles of the DPD can also be found in the GDPR. However, despite this continuity, the data protection and business community alike have perceived the GDPR as revolutionary, which can be credited to the increased attention paid to the stringent new sanction regime (Streinz, 2021, p. 909).

The GDPR and its provisions have been subject to a growing body of doctrinal (legal) research, alongside an increasing number of empirical investigations aimed at exploring their impact and effectiveness. Whereas doctrinal research aims to systematically state the principles, rules, and concepts that apply to a particular area of law and create the connections thereof (Smits, 2017), empirical legal research uses observations to systematically examine how the law works (Bos, 2020, p. 3). While doctrinal research forms the theoretical basis for the empirical exploration of the law (Dagan, Kreitner and Kricheli-Katz, 2018, p. 292), empirical assessments can help determine if certain assumptions on which the law is based are actually correct in practice (Galligan, 2010, p. 998). This is particularly important in the context of the GDPR, which operates within a rapidly evolving digital environment where theoretical frameworks need to be tested against real-world data to ensure the Regulation's objective to effectively protect data subjects.

To support this goal, this chapter aims to bridge empirical and doctrinal research by introducing key GDPR provisions to non-legal audiences. Hence, the objective here is twofold: first, to introduce and explain provisions of the GDPR; and second, to investigate the extent to which these provisions have been the subject of empirical legal research. The chapter

presents research identifying the provisions that are effectively achieving their intended effects, as well as those that may be falling short. However, the list of analysed GDPR provisions presented is by no means exhaustive, as this would require more than a single book chapter to sketch the extensive catalogue of provisions and research already surrounding the GDPR.[1] Instead, this chapter offers a brief introduction to the central provisions and provides guidance on their use as the subject of empirical legal research. This approach is crucial as empirical research is most effective when the law presents testable propositions that can be investigated using social science methods (Davies, 2020, p. 135). Accordingly, the focus lies on the general provisions and data subject rights, thus prompting the exploration of Chapters II and III of the GDPR.

This chapter proceeds as follows. The first section clarifies the scope of the GDPR and introduces important concepts and principles. Secondly, the chapter introduces explanations of key provisions of the GDPR relating to data subject rights and transparency, and how they have already been assessed by empirical legal scholarship. The third section offers a comprehensive overview of the empirical methods employed to evaluate the Regulation. The last section highlights the complementary relationship between empirical legal studies and doctrinal research, and presents a method for integrating the two, followed by the conclusion.

2. Key concepts of the GDPR

This section presents key concepts important for social scientists delving into the GDPR, including its scope, the allocation of responsibilities among various actors, and the principles governing the law. For a deeper understanding of individual provisions, researchers can refer to legal commentaries,[2] which offer comprehensive insights into specific laws authored by legal scholars, or institutional guidelines. In the context of EU data protection law, such bodies as the European Data Protection Board (EDPB) and its predecessor, Art. 29 Working Party (Art29WP), routinely publish and

1 A systematic review of empirical research about the GDPR can be found in Li et al. (2025).

2 See, for instance, Kuner et al. (2020) for a GDPR commentary in English.

have published guidelines.[3] While these are non-binding, their influence has been substantial, as evidenced by their citation in judgments and opinions of the Court of Justice of the EU (CJEU), the highest court of the EU that is crucial in interpreting data protection law.[4]

2.1 The scope of the GDPR

The GDPR applies to "the processing of personal data [...]" (Art. 2(2) GDPR), which forms the law's material scope, or, in other words, the subject matter to which the law applies. The territorial scope of the GDPR, as outlined in Art. 3, defines the applicable geographical area. The GDPR covers:

a. The processing of personal data by controllers and processors within the EU, regardless of where data subjects are located.
b. The processing of personal data of individuals within the EU by controllers or processors outside of its borders, if the processing activities are related to offering goods or services to, or monitoring the behaviour of, individuals within the EU.

Consequently, the GDPR applies even if an EU-based company is processing personal data from a user outside the EU, or vice versa. As opposed to the narrower territorial scope of the DPD that was limited to the borders of the Member States, the reach of EU data protection law significantly expanded with the introduction of the GDPR (Svantesson, 2020).

2.1.1 Processing

Crucial in determining the application of the GDPR is the *processing* of personal data. Processing encompasses a very broad definition of activities through its definition as "any operation or set of operations which is performed on personal data or on sets of personal data [...]" (Art. 4(2) GDPR). Thus, processing data encompasses recording, collecting, structuring, or storing personal data, but also anonymising or destroying data. There are

3 A list of these guidelines with the corresponding GDPR provision can be found in Table 1.

4 See, for instance, the Opinion of the Advocate General Pikamäe in "UF and AB v. Land Hesse (Joined party: SCHUFA Holding AG)" (2023), para. 69.

also exceptions that are not covered by this provision, such as the processing of personal data during a "purely personal or household activity" (Art. 2(2)(c) GDPR). This exemption, often referred to as the "household exemption", clarifies that activities conducted by individuals for strictly personal purposes are excluded from the GDPR's scope. Furthermore, the Regulation does not apply to processing in the context of preventing criminal offences or public-security threats (Art. 2(2)(d) GDPR).

2.1.2 Personal data

Another central element of the GDPR is the legal concept of personal data, as processed data must be *personal* in order for the GDPR to apply. This is further specified in Article 4(1), which defines personal data as "any information relating to an identified or identifiable natural person [..]". This identified or identifiable person is referred to as a "data subject". In general, if the identification of a data subject is not possible, taking into account all of the means *reasonably likely* to be used (Recital 26 GDPR), these data are regarded as non-personal, or "anonymous", data (Bygrave and Tosoni, 2020, p. 105). The "reasonably likely" criterion takes into account the costs, time, effort, and available technological resources at the time of processing, and should thus be regarded as an objective criterion (Hildebrandt, 2020, p. 140). The definition of personal data is almost the same as in the preceding DPD, which is why pre-GDPR case law continues to be relevant today (Bygrave and Tosoni, 2020, p. 108).

One landmark case is "Breyer v. Bundesrepublik Deutschland" (2016), in which the CJEU significantly broadened the scope of the concept of personal data. In this case, the CJEU ruled that "it is not required that all the information enabling the identification of the data subject must be in the hands of one person" (Breyer v. Bundesrepublik Deutschland, 2016, para. 43). In essence, this signifies that, even if an entity lacks the technical means to directly identify someone, if there exists a legal framework or likely means to identify said person, the data must be treated as personal. As an illustration, consider dynamic IP addresses, which are identifiers assigned to devices to connect them to the internet. Despite a website owner's inability to directly connect an IP address with a specific visitor, if there is a lawful method for another party to use said address to ascertain the visitor's identity, the GDPR mandates treating IP addresses as personal data. As such, website hosts are obliged to afford IP addresses the same level

of protection as other identifiable personal data, irrespective of their ability to link the address to a data subject.

2.1.3 Controllership

The GDPR imposes obligations and responsibilities on the controller of personal data. A data controller is defined as the entity "that determines the purposes and means of the processing of personal data" (Art. 4(7) GDPR). Next to controllers, joint controllers, who jointly determine purposes and means of data processing with other controllers (Art. 26 GDPR), and processors, who process data on behalf of a controller (Art. 4(8) GDPR), can be held accountable under the GDPR. Accordingly, the concept of purposes and means of data processing is emphasised, which can be assessed by asking who decides *why* the processing is occurring and *how* this objective, or the purpose of processing, can be reached (EDPB, 2020d, para. 35). When designated as a controller under the GDPR, the responsible entity must implement appropriate technical and organisational means that adequately address the processing in question and minimise risks for data subjects (Art. 24 GDPR). Failure to do so may result in controllers being subject to fines of up to €20 million or up to 4% of their global annual turnover, as outlined in Art. 83(5) GDPR.

Recent jurisprudence has specified some further guidance on the scope of the controllership concept. In "Tietosuojavaltuutettu v. Jehovan todistajat" (2018, para. 75), the CJEU held that an entity can be deemed a controller regardless of whether it has access to personal data. In "Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH" (2018), the CJEU ruled on a similar issue. The question concerned the responsibility of a fan page owner on the social network Facebook. Despite lacking direct access to the data of visitors or the ability to influence its processing, the owner was deemed jointly responsible with Facebook for the processing under Art. 26 GDPR. The CJEU justified its decision by emphasising the entity's role in defining the purpose of the processing, such as establishing criteria for collecting statistics about fan page visitors (para. 36). This case highlights the challenges that platforms pose in determining controllership under the GDPR, especially in situations where platforms influence the extent of data processing practices conducted by their business users. The court, after all, applies the concept of (joint) controllership very broadly.

2.2 Principles of data processing

The processing of personal data is governed by the following principles, enshrined in Art. 5 GDPR, to which data controllers must adhere: fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

The first principle encompasses *lawfulness*, *fairness*, and *transparency* (Art. 5(1)(a) GDPR). *Lawful* processing means that all legal requirements posed by the GDPR should be met. *Fair* processing demands that data subjects are not given misleading information or that the processing is not based on other deceptive means. *Transparency* requires that individuals are informed about who possesses what information about them, and the time and circumstances under which this information was obtained, thus aligning with the principle of informational self-determination. The principle is further specified in Arts. 12–15 GDPR and gives controllers a more detailed overview of what is expected of them.

Purpose limitation (Art. 5 (1)(b) GDPR) requires personal data to be processed solely for the explicit purposes defined by the data controller prior to the data collection. It is one of the most important principles in EU data protection law as it places constraints on data processing and holds the controller, who determines the purposes, accountable and liable (Hildebrandt, 2020, p. 149). The principle consists of two building blocks: (1) the purpose specification, which requires the data processing only for specified, explicit, and legitimate purposes; and (2) the compatible use, which prohibits further processing that is not compatible with those purposes (Art29WP, 2013b, pp. 11–12). Adhering to this principle prevents "function creep" (i.e., the expansion of a process or technology beyond its original purpose) by safeguarding users from privacy risks associated with unforeseen data processing (EDPB, 2020c, p. 14). Furthermore, in order to be effective, the principles of data minimisation and storage limitation depend on this concept.

Data minimisation (Art. 5(1)(c) GDPR) requires that data are processed to the extent necessary for the processing's purpose, by minimising the quantity of processed data to the greatest extent possible.

Accuracy (Art. 5(1)(d) GDPR) means that personal data should be kept up to date and accurate, as inaccurate personal data could put data subject rights at risk, especially when decision-making is based on this inaccurate information (EDPB, 2020a, p. 23).

Storage Limitation (Art. 5(1)(e) GDPR) mandates controllers to implement technical measures and safeguards to ensure that personal data are retained only for the duration necessary for processing purposes, such as by employing internal anonymisation or deletion procedures to prevent data from being stored beyond their intended use (EDPB, 2020a, p. 25).

Integrity and Confidentiality (Art. 5(1)(f) GDPR) aim to prevent security breaches by requiring data controllers to include appropriate technical or organisational measures. These are derived from the "CIA Triad" (Confidentiality, Integrity, and Availability), a fundamental model in information security. Art. 32 GDPR is closely connected to this principle, mandating that data controllers ensure an appropriate level of security relative to the risks posed to data processing

Lastly, *accountability* (Art. 5(2) GDPR) mandates the controller to assume responsibility for ensuring and showcasing compliance with all the aforementioned principles and is linked to transparency, as controllers are obliged to be able to demonstrate their data processing's compliance with the GDPR (Art29WP, 2018, p. 5).

3. Key provisions in the GDPR

The GDPR has frequently served as a subject for empirical research in recent years. These empirical assessments not only shed light on what the implementation of the GDPR has changed with respect to the foregoing DPD, but also on the effectiveness and implementation by data controllers. The following subsections describe some of the provisions that have been subject to empirical legal assessments, and a short description of their results.

3.1 Art 6 GDPR – lawful grounds for processing

The processing of personal data is forbidden, except when based on one of the legal grounds specified in Art. 6(1) GDPR. This involves (a) the consent of the data subject, (b) the performance of a contract, (c) compliance with a legal obligation of the controller, (d) the protection of vital interests of the data subject, (e) the performance of a task in the public interest, and (f) the legitimate interest of the data controller (Art. 6(1)(a–f) GDPR).

Every step of processing of personal data must be based on one of these grounds. Consequently, a legal basis is crucial for ensuring compliance

with the GDPR. A controller should always carefully evaluate which legal basis is appropriate for the intended processing; consent, for instance, is only lawful if the data subject can freely, and without facing negative consequences, accept or reject the proposed terms (EDPB, 2020c, p. 5). Under the legal basis of legitimate interest, a data subject's consent is not necessary to process personal data. A legitimate interest is an interest recognised by EU or national law, and purely commercial interest can thus not qualify as one (Kotschy, 2020, p. 337). Examples include processing data for direct marketing purposes, which could be based on the freedom to conduct a business, or processing data to prevent fraud, linked to the right to property (Kotschy, 2020, p. 337). However, there are also limitations, as the data subjects may still object to the processing based on legitimate interest (Art. 21(1) GDPR) and the controller's interests may be overridden by the fundamental rights or freedoms of data subjects (Art. 6(1)(f) GDPR). For instance, in "Meta Platforms v. Bundeskartellamt" (2023), the CJEU ruled that, following a balancing test, Meta could not rely on legitimate interest as a legal basis for processing personal data for the purposes of personalised advertising (para 117).

Kyi et al (2023) investigated the usage of the legal basis of legitimate interest in the context of privacy notices and the user perceptions thereof. The authors identified a lack of enforcement regarding the use of legitimate interest as a legal basis in cases where advertising practices may have been unaligned with genuinely legitimate grounds, thus highlighting the potential for this provision's exploitation. This empirical assessment thus enhances our understanding of how Art. 6 GDPR is used in practice. Empirical research centred around user consent (Art. 6(1)(a) GDPR), which is further specified in Art. 7, is explained in the following section.

3.2 Art. 7 GDPR – conditions for valid consent

Compared to the previous data protection regime, which defined consent as "any freely given specific informed indication of his wishes by which the data subject signifies his agreement to personal data [...]" (Art. 2 (h) DPD), the rules introduced with the GDPR are stricter. Here, consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Art. 4(11) GDPR). More context when consent is

lawful is delivered in Art. 7 GDPR. For instance, the request for consent should be intelligible and easily accessible (Art. 7(2) GDPR), and can be revoked by a data subject at any time (Art. 7(3) GDPR). A pre-ticked box, silence, or inactivity cannot constitute valid consent (Recital 32 GDPR), which also has been confirmed by the CJEU in "Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH" (2019).

Obtaining consent is crucial for tracking activities on the web and on mobile devices, as consent constitutes the only lawful basis for tracking that is not technically necessary (Kollnig, Binns, Dewitte, et al, 2021, p. 6).[5] Hence, several studies have investigated the GDPR's impact on the EU's cookie banner landscape. For instance, Degeling et al (2019) illustrated a notable 16% increase in the prevalence of websites displaying cookie banners by examining 6,579 popular EU websites before and after the GDPR's implementation.

The conditions for consent become especially important with the rise of dark patterns, which is an umbrella term for design patterns that steer user behaviour towards actions that benefit the entity implementing the design (Kyi et al, 2023). Often, user interfaces are designed so as to nudge users to agree to options that share personal data with a variety of third parties. However, this stands at odds with the GDPR's requirements, which demand consent to be *an unambiguous indication of wishes*, meaning that controllers should design consent banners that are clear to data subjects (EDPB, 2020c, p. 19). Furthermore, Art. 7(3) GDPR mandates that giving consent shall be as easy as withdrawing consent, which can also be extended to cookie banners.

Against this background, one could assume that the GDPR has reduced the prevalence of dark patterns. However, the analysis of 1,000 cookie banners post-GDPR showed that over half (57.4%) contained dark patterns (Utz et al, 2019, p. 976). Shedding light on user behaviour, Utz et al (2019) additionally showed that, when given a choice, only 0.1% of users would consent to the use of their data by third parties. In addition, some studies have investigated the impact of certain dark pattern designs on user behaviour, which helps to assess which design decisions are most likely to be manipulative, and could thus help enforce the GDPR (Machuletz

5 In this case, in addition to the GDPR, the ePrivacy Directive (2002/58/EC) is applicable to tracking activities on mobile devices, which must be transposed into national law. In Germany, for instance, the Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) (BGBl. I Nr. 149/2024) applies as soon as mobile devices are involved.

and Böhme, 2020; Nouwens et al, 2020). The issue does not only relate to the design of cookie banners: Santos et al (2021) studied the text of 407 banners, revealing that 89% of them did not comply with GDPR standards, notably by omitting or vaguely describing the purposes of data processing.

Moving from websites to the mobile ecosystem, Kollnig, Binns, Dewitte, et al (2021) studied consent notices offered by mobile apps to their users. Their study revealed that a considerable number of the 1,297 investigated Android apps failed to comply with the GDPR: of the 76% of apps that had been updated following the GDPR, and could thus have implemented the necessary adaptation, only 9% asked for user consent (Kollnig, Binns, Dewitte, et al, 2021, p. 7). On a yet-larger scale, Nguyen, Backes and Stock (2022, p. 13) studied consent notices across 239,381 Android apps, revealing that 13,082 implemented consent notices, and over 20% of those failed to meet the GDPR's consent standards.

These studies are important as they highlight the shortcomings of the GDPR's enforcement regarding consent on multiple fronts: first, by showcasing instances of non-compliance where the option to provide consent is not even offered; second, by exposing instances of uninformed consent resulting from the implementation of dark patterns; and third, by shedding light on user behaviour indicating a general reluctance to consent to tracking activities.

3.3 Art. 9 GDPR – Data revealing special categories of personal data

Art. 9 GDPR protects data revealing special categories of personal data, often referred to as "sensitive data" (Recital 10 GDPR). The following information is considered sensitive: "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data for the purpose of uniquely identifying a natural person and data concerning health or data concerning a natural person's sex life or sexual orientation" (Art. 9(1) GDPR). The rationale behind Art. 9 GDPR is to protect types of data whose processing may facilitate human rights violations or other serious consequences for an individual (Georgieva and Kuner, 2020). While the DPD already included a provision concerning special categories of data (Art. 8 DPD), the GDPR introduced additional categories, namely genetic and biometric data, and data concerning a person's sexual orientation. Recent advancements in data mining and the increased availability of data have made it possible to

infer sensitive information from seemingly harmless data, which poses a challenge to their effective protection (Quinn and Malgieri, 2021, p. 1596). To illustrate, accelerometers in mobile phone are used to stabilise images captured by the camera or detect certain movements like the shaking of a device. While considered non-sensitive, accelerometer data from mobile devices may be used to reveal a wide range of (sensitive) personal data, such as a data subject's location, degree of mobility, sleep patterns or gender (Kröger, Raschke and Bhuiyan, 2019).

Several studies have investigated the compliance of apps collecting their users' sensitive data. For instance, Parker et al (2019) analysed disclosures of 61 prominent mental health apps, including their privacy policies and permissions that process personal data concerning health. They highlighted that, while the GDPR has prompted some improvements in transparency, half of the investigated apps had no privacy policy whatsoever (Parker et al, 2019). These results are particularly alarming, considering that the disclosure of personal health information could result in serious emotional harm to users. Fan et al (2020) examined the degree of GDPR compliance among 736 general Android health apps. Their findings indicate non-compliance with transparency provisions and data minimisation, with a considerable number of apps failing to ensure the encryption of collected health data (Fan et al, 2020).

Shipp and Blasco (2020) conducted a study on 30 period tracking apps, which enable users to monitor menstruation and sexual activity to gain insights into their menstrual health. These apps track sensitive data, such as a user's sexual orientation or pregnancy-related information. The researchers discovered that 23 of these apps shared user data with third parties, raising concerns about insufficient disclosure regarding data collection purposes, user rights, and the failure to classify the collected data as sensitive (Shipp and Blasco, 2020). The findings are particularly concerning given the potential exploitation of sensitive data for targeted advertising purposes, especially considering the heightened vulnerability of users in such contexts (Siapka and Biasin, 2021).

These observations contribute to the discussion on the protection of sensitive data. Past incidents, such as data protection violations by Grindr – a dating app predominantly used within the queer community – underscore the critical need for adherence to the GDPR-mandated safeguards. Grindr, which collects data encompassing a data subject's sexual orientation, HIV status, and precise location, incurred a fine from the Norwegian Data Protection Authority for sharing these sensitive data with third parties without

valid user consent (Datatilsynet, 2021). While the GDPR was enforced, this instance likely represents only a fraction of the cases where controllers have failed to implement adequate safeguards for protecting users and their sensitive data. The case underlines the importance for further research in these areas of data protection law, particularly where marginalised communities are affected.

3.4 Arts. 12-14 GDPR – Transparency

In order to make informed decisions about who collects user data and under which circumstances, users should be provided with adequate information. Art. 12 GDPR specifies *how* this information should be provided to the user. The provision involves an entirely new transparency standard, namely that information should be "concise, transparent, intelligible and easily accessible form, using clear and plain language" (Art. 12(1) GDPR). Furthermore, Arts. 13 and 14 GDPR specify on *which* elements users should be informed. This list includes such elements as the identity of the data controller, for what the data will be used, the period for which the data are stored, and information about the user's rights under the GDPR. This information must be provided when personal data are obtained. The rationale behind these provisions is to ensure the effectiveness of personal data protection, as users can only exercise their rights if they are aware of the details of the processing of their data (Zanfir-Fortuna, 2020, p. 415). A privacy policy is the most popular form of providing this information.

3.4.1 Privacy policies (Arts. 12, 13, 14 GDPR)

Several studies have evaluated the GDPR's impact in the realm of transparency by evaluating the content of privacy policies with text-as-data methods over time (Degeling et al, 2019; Linden et al, 2019; Amos et al, 2021; Frankenreiter, 2022; Wagner, 2023). Advances in text-based methods allow for large corpora of privacy policies, and the patterns within them, to be analysed and identified. Web scraping, i.e. downloading website content from the internet, enables the creation of large text corpora. A particularly powerful tool for collecting and comparing pre- and post-GDPR privacy policies over a long period of time is the web scraping of past web pages. This is made possible by the Wayback Machine, a non-profit initiative which has archived over 850 billion web pages since 1996 (Internet Archive,

2024) and has been used in several studies investigating the impact of the GDPR (see, for instance, Wagner, 2023; Linden, 2019; Ganglmair, Krämer and Gambato, 2024).

In 2018, privacy policies in the EU underwent substantial revisions, as evidenced by Degeling et al (2019), who observed updates on the majority of 6,579 popular webpages post-GDPR enforcement. Similar observations were made by Linden et al (2019), who analysed 6,278 privacy policies both within and outside the EU. After the GDPR became enforceable, policies within the EU expanded by a third in length, while those outside the Union experienced a slightly smaller, but still notable, increase (Linden et al, 2019, p. 7).

Privacy policies have also been used to advance the computational methods for analysing legal content. The CLAUDETTE project, for instance, developed a methodology for the automated analysis of privacy policies using machine learning (Contissa et al, 2018). While the project remains in its preliminary stages, an automated analysis of privacy policies could help users, consumer associations, and researchers alike efficiently identify GDPR violations. Recent developments in natural language processing are likely to further develop the automated analysis of privacy policies, such as by analysing their content with the help of large language models (Rodriguez et al, 2024).

To test the impact of the higher standards of clear and plain language in privacy policies, which Art. 12(1) GDPR mandates, the readability of privacy policies has been measured quantitatively. This assessment can be done, for instance, via so-called readability indices that compute scores based on the length of words or sentences or the counting of obfuscating words perceived to lower a text's readability. While Becher and Benoliel (2021) found that privacy policies have become more readable, Wagner (2023) showed how they tend to use more obfuscating words since the GDPR. However, compared to Wagner's (2023) corpus of 56,416 unique privacy policies, Becher and Benoliel (2021) investigated a corpus of 24 pre- and post-GDPR policies, and their findings may, therefore, overgeneralise the GDPR's actual impact. Using a corpus of 585,000 Germany privacy policies, Ganglmair, Krämer and Gambato (2024) showed that, although the length of the average policy tripled after the GDPR came into force and contained more information, the average results for readability remained mixed. The authors argued that the enforcement of Art. 12(1) GDPR is inherently challenging due to its subjective nature, in contrast to the objective and readily enforceable information requirements in Arts. 13–14

(Ganglmair, Krämer and Gambato, 2024, p. 4). This study thus illustrates the "tension" inherent in the GDPR between improving the readability of privacy policies and the parallel obligation to add more comprehensive information (Art29WP, 2018, para. 34).

Further to quantitative assessments, some authors have conducted qualitative evaluations by individually analysing privacy policy content. Using this approach, Serveto (2020, p. 597) demonstrated that rules already established within the DPD were more frequently incorporated into the privacy policies of internet service providers than those newly introduced by the GDPR.

The effectiveness of GDPR provisions can also be assessed through the observation of users' responses and behaviours towards them. Before the adoption of the GDPR, empirical evidence had already demonstrated that users tend not to read lengthy legal documents online (Bakos, Marotta-Wurgler and Trossen, 2014). Ben-Shahar and Chilton (2016) demonstrated that, even when privacy policies are drafted in a readable manner, as the GDPR prescribes in Art. 12(1), user behaviour remains largely unchanged, with an overwhelming majority of individuals opting not to read them. These findings indicate that the anticipated behaviour envisioned by the GDPR is often not realised among data subjects. Subsequently, it should come as no surprise that doctrinal legal research has been critical of transparency provisions in data protection and privacy laws. Indeed, Solove (2012) claimed that, due to cognitive and structural limitations, data subjects are not able to engage effectively in privacy self-management. Similarly, Waldman (2021, p. 61) criticised the GDPR's "privacy-as-control" approach, which mandates readable privacy policies for data controllers, but does little to protect users from structural power imbalances and deceptive practices employed by powerful platforms.

3.4.2 Privacy labels and standardised icons (Art. 12(7) GDPR)

Due to the overwhelming criticism of privacy policies and the evidence that users rarely read online legal documents, researchers have devised various strategies with which to inform users about data processing practices. Examples are so-called privacy labels, which inform users more quickly and efficiently than privacy policies by using icons or other images (Kelley et al, 2009). A provision about privacy labels has also been incorporated into the GDPR and allows for the combination of the information delivered with "standardised icons in order to give an easily visible, intelligible and

clearly legible manner a meaningful overview of the intended processing" (Art. 12(7) GDPR).

Although the European Commission bears the responsibility of establishing a procedure to introduce these standardised icons (Art. 12(8) GDPR) – which has yet to make use of its competence (Polčák, 2020, p. 411) – an initial large-scale adoption of privacy labels has been launched in the Apple App Store and Google Play Store. In the absence of established procedures, these private actors have introduced their own (native) label designs. However, while these may enhance a data subject's awareness of data processing within apps, they have faced criticism for failing to adequately reflect privacy risks (Kollnig et al, 2022), as well as for favouring Apple's and Google's native tracking practices while not complying with the GDPR (Krämer, 2024). Furthermore, recent qualitative studies have shown that the categories chosen by the app stores confuse users and developers (Gardner et al, 2022; Zhang et al, 2022), which calls into question whether the labels can meet the GDPR's transparency standards. These examples make it clear that alleged improvements should be critically and empirically examined in order to determine whether the new measures actually improve user privacy.

3.5 Measuring data flows and tracking – transparency and data minimisation

The aforementioned studies investigated compliance with the GDPR based on the disclosures firms have made in their privacy policies. Rather than analysing statements by data controllers, certain authors opted to directly measure data flows and assess whether the GDPR has effectively reduced personal data collection.

In the realm of mobile apps, this has been done by Kollnig, Binns, Van Kleek et al (2021), who investigated how the amount of tracker libraries in apps has developed post-GDPR. The authors found that third-party tracking has not changed significantly, which they interpreted as a lack of GDPR enforcement within the mobile ecosystem (Kollnig, Binns, Van Kleek et al, 2021). Regarding webpages, Sanchez-Rola et al (2019) investigated 2,000 popular websites around the world. While the majority of websites (e.g., those in the US) try to somehow comply with the GDPR by having privacy policies or consent banners, 90% of those investigated engage in tracking by placing long-lasting identifiers on user devices, despite the

GDPR's mandate that personal data should only be stored for a minimum necessary duration. Relatedly, Matte et al (2020) investigated whether data subjects' cookie choices are respected. They examined 1,426 websites to determine which choices were actually saved in the browser and found that 141 websites recorded positive consent despite the user having rejected cookies.

These findings are alarming as they showcase the extent of tracking via the web or mobile devices. Tracking can facilitate various harms, including discrimination, financial harms, or threats to democracy (Cofone, 2023, p. 112). For example, individuals may suffer financial harm when coerced into purchasing products they neither want nor need (Cofone, 2023, p. 112). The preceding empirical studies can, therefore, provide the necessary evidence to support doctrinal assessments that have pointed out various privacy risks and harms connected to tracking.

3.6 Art. 15 GDPR – right of access

Art. 15 GDPR gives data subjects the right to confirm whether their personal data has been processed, to obtain access to their processed personal data, and to receive information about the processing activities themselves. Consequently, the right of access empowers data subjects to confirm the accuracy of their personal data and ascertain whether the data controller holds any such data in the first place (EDPB, 2023, p. 8).

While data subject rights are empowering, they must also be respected by data controllers so that they can unravel their full potential. Dexe et al (2020) explored the responsiveness of the Swedish home insurance market to data subject requests during late 2018 and early 2019. They identified deficiencies in adequately describing requested components, such as legal bases or processing descriptions, and noted failures to meet designated time limits. In a subsequent study encompassing insurance companies across five EU countries in 2021, the researchers analysed access requests detailing automated decision-making (Dexe et al, 2022). Although responses were received from all contacted data controllers, the majority were notably vague, with the researchers uncovering disparities among these responses, possibly due to the subtle differences in the translations of the GDPR (Dexe et al, 2022).

The effectiveness of Art. 15 GDPR in relation to online service providers was investigated by Dewitte and Ausloos (2024), who sent access requests

to 70 data controllers in 2020 and 2022. The results show that, although the majority of the controllers surveyed responded to the requests, many of the responses were generalised and untailored to the individual case, thereby possibly violating Art. 15. In addition, over half of the responses took more than a month to be issued (Dewitte and Ausloos, 2024, p. 21) despite this exceeding the deadline stipulated in Art. 12(3). Instead of looking at the compliance of controllers, Borem et al (2024) explored the experiences of 33 data subjects to the responses of data access requests. While the responses often left participants' specific questions unanswered, some participants were shocked and angry about the privacy implications after discovering the amount of data that was held by the controller.

Furthermore, the scope of Art. 15(1)(h) has been examined, which, in the context of automated decision-making, requires controllers to provide meaningful information about the logic involved and the significance and envisaged consequences of data processing for the data subject. Custers and Heijne (2022) examined the interpretation of these elements by conducting a survey addressed to data protection authorities, which was accompanied by several expert interviews. The survey revealed that only a small fraction of respondents considered code as relevant, while the majority viewed the categories in which a data subject is placed as "meaningful information" (Custers and Heijne, 2022, p. 11).

In conclusion, the presented studies serve as useful guides for understanding and assessing the extent of GDPR compliance among data controllers in different EU Member States, and thereby offer valuable guidance to data protection authorities and policymakers.

3.7 Art. 17 GDPR – right to be forgotten

The right to erasure, also known as the right to be forgotten, grants users the possibility to have their personal data erased from the records of data controllers under specific circumstances, such as if the data subject withdraws consent, the data have been unlawfully processed, or the data are no longer necessary in relation to the purposes for which they were initially collected (Art. 17(1) GDPR). This obligation can involve users requesting search engines to delist websites that appear when searching for the user's name (EDPB, 2020b, p. 4). The CJEU established the right to be forgotten in the landmark case "Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"

(2014), by interpreting provisions of the DPD as ensuring such a right. The GDPR subsequently codified this right, elevating it to a standalone Article. While this seems to represent a significant deviation from the DPD, it is also viewed by some as merely a "more detailed elaboration of the already existing right of erasure" (Kranenborg, 2020, p. 477).

The right to erasure has been tested regarding its effectiveness and how controllers manage these challenges. For instance, Rupp et al (2022) sent erasure requests to 90 different service providers, of which 27% failed to respond. To explore potential challenges that data controllers face when complying with this right, Mangini et al (2020) conducted a structured survey to explore the right's implications for data controllers. The authors found that tight deadlines and a lack of knowledge connected with complying to the right have been particularly challenging for controllers, but the GDPR also introduced advantages regarding processing, such as an increased awareness regarding internal data processing activities. In highlighting the continued challenges for both data subjects and controllers, these studies showcase that there is still room for improvement in complying with the right to be forgotten.

4. A rich methodological toolbox

The preceding section has demonstrated how empirical research provides valuable insights into the effectiveness of the GDPR, highlighting the diverse methods available for studying its provisions. Table 1 lists the research discussed above, accompanied by the types of measurement employed.

Table 1: Overview of empirical (legal) research regarding specific GDPR provisions, and the type of method used

GDPR provision	Official Guidelines	Prior empirical work	Type of method
Lawful grounds for processing			
Art. 6(1)(f)		Kyi et al (2023)	Observational data analysis
Consent	European Data Protection Board (2020c)		
Art. 7 GDPR		Santos et al (2021)	Observational data analysis
		Utz et al (2019) Nouwens et al (2020)	Field experiment
		Kollnig, Binns, Dewitte et al (2021) Nguyen et al (2022)	Dynamic analysis of mobile data flows
Sensitive data			
Art. 9 GDPR		Parker et al (2019) Fan et al (2020) Shipp and Blasco (2020)	Systematic analysis of health apps
Transparency	Art. 29 Working Party (2018)		
Art. 5(1) GDPR, Arts. 12–14 GDPR		Degeling et al (2019) Linden et al (2019) Amos et al (2021) Wagner (2023) Contissa et al (2018)	Natural language processing and text-as-data methods
		Bakos et al (2014)	Field study into online browsing behaviour
		Ben-Shahar and Chilton (2016)	Experiment
Art. 12(7) GDPR		Kollnig, Binns, Van Kleek et al (2022) Gardner et al (2022) Krämer (2024)	Observational data analysis
		Zhang et al (2022)	Interviews

GDPR provision	Official Guidelines	Prior empirical work	Type of method
Transparency, data minimisation, and storage limitation			
	ENISA (2017) Art. 29 Working Party (2013a)	Kollnig, Binns, Van Kleek et al (2021)	Static analysis of mobile apps
		Matte, Bielova and Santos (2020)	Systematic analysis of back-end cookie banner choices
		Sanchez-Rola et al (2019)	Systematic analysis of cookie banners and trackers
Right to access Art. 15 GDPR	European Data Protection Board (2023)	Dexe et al (2020) Dexe et al (2022) Dewitte and Ausloos (2024)	Field study
		Borem et al (2024) Custers and Heijne (2022)	Survey
Right to erasure / right to be forgotten Art. 17 GDPR	European Data Protection Board (2020b)	Mangini, Tal and Moldovan (2020)	Survey
		Rupp, Syrmoudis and Grossklags (2022)	Field study

Surveys and studies involving data controllers and subjects that send out erasure or access requests can showcase how controllers perceive and respond to certain GDPR provisions. Experiments complement this perspective by showing how data subjects behave when confronted, for instance, with cookie banners or privacy policies. A rich methodological toolbox can thus paint a detailed picture of the GDPR's impact on different aspects of data processing.

4.1 Challenges for empirical (legal) studies in the context of the GDPR

The previous sections have shown a growing field of empirical (legal) research connected to the GDPR, with a variety of methodological approaches employed. These studies are crucial for understanding the practical implementation of the GDPR. Nevertheless, there are also challenges. Empirical research begins with certain basic ideas about how laws work, and how these ideas are put into practice within legal systems (Dagan, Kreitner and Kricheli-Katz, 2018, p. 302). Some authors have claimed, therefore, that empirical research should use legal theory as a point of departure so as to prevent it from operating in isolation (Smits, 2017, p. 17; Davies, 2020, p. 9). Thus, two challenges arise: first, how to properly design empirical studies exploring the GDPR and, second, how to translate these empirical insights into normative statements within legal doctrine.

For this reason, Towfigh (2014, p. 678) suggested some key points to consider for ensuring that empirical evidence can be effectively integrated into legal expertise. Firstly, an empirical study should define variables according to existing legal norms. Secondly, results should be generalisable to the legal context and properly operationalised. Lastly, the design, methods, statistics, and conclusions of an empirical study must pass tests of validity (Towfigh, 2014).

The first step in Towfigh's (2014) method ensures the correct definition of legal concepts to avoid any inconsistencies between legal concepts and social science methods, which may carry different assumptions. In the context of privacy, for instance, there is often a conceptual gap between the legal concept and the mathematical understanding of this concept (Cohen and Nissim, 2020, p. 8344). In addition to legal provisions, further guidance for defining a legal concept may be found in CJEU rulings, which are legally binding, and EDPB guidelines, which, while not, can still serve as valuable tools.

Secondly, the operationalisation of the legal concept is of importance, as it is not always easy to measure the legally defined concepts of the first step. Determining operators that define legal compliance is complex, particularly in the case of the GDPR, where legal uncertainty remains regarding its newly introduced provisions. To give a well-designed example in the context of consent, Nouwens et al (2020) translated GDPR provisions into three quantifiable minimum requirements necessary for cookie banners to be compliant (e.g., no pre-ticked boxes, consent being an explicit act like clicking a button, accepting being as easy as rejecting cookies). While

the authors acknowledged that meeting these conditions alone does not guarantee compliance, as additional factors must be assessed qualitatively, they were able to demonstrate that only 11.8% of cookie banners met these minimal requirements, with the rest violating the GDPR (Nouwens et al, 2020, p. 5). Consequently, these findings, while not covering all elements of compliance, are useful for highlighting widespread non-compliance in cookie banners.

Thirdly, in the final step of Towfigh's (2014, p. 680) method, the results must be checked for validity. When considering the implications of results, it is important to distinguish between challenges that can be addressed within the framework of the GDPR and those challenges that question the Regulation's underlying assumptions or structural issues. For example, the issue of privacy label designs being influenced by private interests (as discussed in Section 3.4) could be resolved through a procedure that standardises these labels, as permitted by the GDPR (Art. 12(7)). However, the European Commission (who must initiate the procedure) has yet to materialise this competence. Furthermore, many studies have cited a lack of enforcement of GDPR provisions as the reason why empirical results consistently identify non-compliance, which could also be mitigated within the existing framework.

On the other hand, the problem that users rarely read privacy policies because they often lack the cognitive ability and training to process large amounts of text written in legalese (Waldman, 2020) is a structural problem that will not be solved by the (properly enforced) GDPR. This problem persists despite the new requirement for readability in privacy policies (Art. 12(1) GDPR). In fact, while the GDPR mandates clearer disclosures, it also requires that users be informed about more categories of information, which has led to studies showing that the length of the average privacy policy post-GDPR has tripled (Ganglmair, Krämer and Gambato, 2024) and that more obfuscatory words are used (Wagner, 2023). As such, mechanisms dependent on transparency, such as *informed* consent (Art. 4(11) GDPR), may fall short of realising their potential, not necessarily because to a lack of enforcement by data protection authorities, but due to the underlying assumptions within the GDPR itself. It is therefore important to reconcile the conclusions from empirical studies with the distinction between challenges that can be resolved within the legal framework of the GDPR and those that fundamentally challenge its basic principles.

While empirical research is a powerful and necessary tool for exploring GDPR provisions next to a doctrinal analysis, it is important for both legal

scholars and social scientists to also consider the challenges that may arise when employing these methods. As this section has shown, a plurality of methods can help evaluate the GDPR's impacts from data subject and controller perspectives, and allows for the identification of dynamics that can inform regulators and policy makers.

5. Conclusion

This chapter has introduced several key provisions of the GDPR, with the aim of inspiring future empirical studies and mapping existing ones on EU data protection law. While doctrinal analysis in the GDPR's context has traditionally received more attention, the chapter has shown that empirical (legal) research in the context of the GDPR is already prominent. The described studies have helped identify areas in which compliance presents several shortcomings, such as the challenge stemming from a lack of the Regulation's enforcement. Despite legal obligations imposed on controllers, the empirical evidence provided reveals non-compliance, such as the absence of privacy policies, deceptive consent practices, and irregular data handling, which calls into question the effectiveness of the Regulation. A distinction must be made here as to the extent to which these shortcomings are due to the GDPR's design or to a lack of enforcement and compliance that could potentially be mitigated in the future.

Moreover, this chapter has stressed the need for interdisciplinary research regarding the GDPR and data protection law in general. As seen in the research surrounding the effectiveness of privacy policies and the prevalence of dark patterns, empirical research can provide the necessary evidence to pinpoint major deficiencies in the assumptions on which the law is based. By bridging legal analysis with empirical findings, interdisciplinary research can yield important insights into the practical implications and shortcomings of data protection laws. Such collaborative efforts pave the way for more effective policy interventions and regulatory responses aimed at safeguarding fundamental rights in the Digital Age.

References

Albrecht, J.P. (2016) 'How the GDPR will change the world: the General Data Protection Regulation: foreword', *European Data Protection Law Review (EDPL)*, 2(3), pp. 287–289.

Amos, R., Acar, G., Lucherini, E. et al (2021) 'Privacy policies over time: curation and analysis of a million-document dataset', in *Proceedings of the Web Conference 2021. WWW '21: The Web Conference 2021*, ACM, pp. 2165–2176.

Art29WP (2013a) *Opinion 02/2013 on apps on smart devices*. 00461/13/EN WP 202. Article 29 Working Party [Online]. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (Accessed: 30 January 2025).

Art29WP (2013b) *Opinion 03/2013 on purpose limitation*. Article 29 Working Party [Online]. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (Accessed: 30 January 2025).

Art29WP (2018) *Guidelines on transparency under Regulation 2019/679*. 17/EN WP260 rev.01. Article 29 Working Party [Online]. Available at: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf (Accessed: 30 January 2025).

Bakos, Y., Marotta-Wurgler, F. and Trossen, D.R. (2014) 'Does anyone read the fine print? Consumer attention to standard-form contracts', *The Journal of Legal Studies*, 43(1), pp. 1–35.

Becher, S.I. and Benoliel, U. (2021) 'Law in books and law in action: the readability of privacy policies and the GDPR' in Mathis, K. and Tor, A. (eds.) *Consumer law and economics*. Cham: Springer International Publishing, pp. 179–204.

Ben-Shahar, O. and Chilton, A. (2016) 'Simplification of privacy disclosures: an experimental test', *The Journal of Legal Studies*, 45(S2), pp. S41–S67.

Borem, A., Pan, E., Obielodan, O. et al (2024) 'Data subjects' reactions to exercising their right of access', in *33rd USENIX Security Symposium. USENIX* [Online]. Available at: https://www.usenix.org/conference/usenixsecurity24/presentation/borem (Accessed: 22 July 2024).

Bos, K. (2020) *Empirical legal research: a primer*. Cheltenham: Edward Elgar Publishing.

Bygrave, L.A. and Tosoni, L. (2020) 'Article 4(1). Personal data' in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 103–115.

Cofone, I. (2023) *The privacy fallacy: harm and power in the information economy*. Cambridge: Cambridge University Press.

Cohen, A. and Nissim, K. (2020) 'Towards formalizing the GDPR's notion of singling out', *Proceedings of the National Academy of Sciences*, 117(15), pp. 8344–8352.

Contissa, G., Docter, K., Lagioia, F. et al (2018) '(C)laudette meets GDPR: automating the evaluation of privacy policies using artificial intelligence'. Rochester, NY. Available at: https://doi.org/10.2139/ssrn.3208596.

Custers, B. and Heijne, A.-S. (2022) 'The right of access in automated decision-making: The scope of Article 15(1)(h) GDPR in theory and practice', *Computer Law & Security Review*, 46, 105727 [Online]. Available at: https://doi.org/10.1016/j.clsr.2022.105727 (Accessed: 30 January 2025).

Dagan, H., Kreitner, R. and Kricheli-Katz, T. (2018) 'Legal theory for legal empiricists', *Law & Social Inquiry*, 43(02), pp. 292–318.

Datatilsynet (2021) *The NO DPA imposes fine against Grindr LLC*. Datatilsynet [Online]. Available at: https://www.datatilsynet.no/en/regulations-and-tools/regulations/avgjorelser-fra-datatilsynet/2021/gebyr-til-grindr/ (Accessed: 26 April 2024).

Davies, G. (2020) 'the relationship between empirical legal studies and doctrinal legal research', *Erasmus Law Review*, 13(2), pp. 3–12.

Degeling, M., Utz, C., Lentzsch, C. et al (2019) 'We value your privacy ... now take some cookies: measuring the GDPR's impact on web privacy', in *Proceedings 2019 Network and Distributed System Security Symposium. Network and Distributed System Security Symposium*, Internet Society [Online]. Available at: https://doi.org/10.14722/ndss.2019.23378 (accessed: 30 January 2025).

Dewitte, P. and Ausloos, J. (2024) 'Chronicling GDPR transparency rights in practice: the good, the bad and the challenges ahead', *International Data Privacy Law*, pp. 106–133.

Dexe, J., Franke, U., Söderlund, K. et al (2022) 'Explaining automated decision-making: a multinational study of the GDPR right to meaningful information', *The Geneva Papers on Risk and Insurance – Issues and Practice*, 47(3), pp. 669–697.

Dexe, J., Ledendal, J. and Franke, U. (2020) 'An empirical investigation of the right to explanation under GDPR in insurance' in S. Gritzalis et al. (eds.) *Trust, privacy and security in digital business*. Cham: Springer International Publishing, pp. 125–139.

'Digitale-Dienste-Gesetz (DDG)' BGBl. I Nr. 149/2024 [Online]. Available at: https://www.recht.bund.de/bgbl/1/2024/149/VO (Accessed on: 30 January 2025).

'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' (1995) *Official Journal* L 281, 23 November, pp. 31–50 [Online]. Available at: http://data.europa.eu/eli/dir/1995/46/oj (Accessed: 30 January 2025).

'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)' (2002) *Official Journal* L 201, 31 July, pp. 37–47 [Online]. Available at: http://data.europa.eu/eli/dir/2002/58/oj (Accessed: 30 January 2025).

EDPB (2020a) *Guidelines 4/2019 on Article 25 data protection by design and by default*. Brussels: European Data Protection Board [Online]. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (Accessed: 30 January 2025).

EDPB (2020b) *Guidelines 5/2019 on the criteria of the right to be forgotten in the search engines cases under the GDPR* [Online]. Brussels: European Data Protection Board. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf (Accessed: 30 January 2025).

EDPB (2020c) *Guidelines 05/2020 on consent under Regulation 2016/679* [Online]. Brussels: European Data Protection Board. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (Accessed: 30 January 2025).

EDPB (2020d) *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Brussels: European Data Protection Board [Online]. Available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (Accessed: 30 January 2025).

EDPB (2023) *Guidelines 01/2022 on data subject rights – right of access*. Brussels: European Data Protection Board [Online]. Available at: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf (Accessed: 30 January 2025).

ENISA (2017) *Privacy and data protection in mobile applications – a study on the app development ecosystem and the technical implementation of the GDPR*. European Union Agency for Network and Information security [Online]. Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications (Accessed: 31 January 2025).

Fan, M., Yu, L., Chen, S. et al (2020) 'An empirical evaluation of GDPR compliance violations in Android mHealth apps', in *2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE)*, IEEE, pp. 253–264.

Frankenreiter, J. (2022) 'Cost-based California effects', *Yale Journal on Regulation*, 39(3), pp. 1155–1217.

Galligan, D.J. (2010) *Legal theory and empirical research*. Oxford: Oxford University Press.

Ganglmair, B., Krämer, J. and Gambato, J. (2024) 'Regulatory compliance with limited enforceability: evidence from privacy policies', *ZEW Discussion Paper No. 24-012* [Preprint Online]. Available at: https://doi.org/10.2139/ssrn.4774514 (Accessed: 30 January 2025).

Gardner, J., Feng, Y., Reiman, K. et al (2022) 'Helping mobile application developers create accurate privacy labels', in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, pp. 212–230.

Georgieva, L. and Kuner, C. (2020) 'Article 9 processing of special categories of personal data' in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 365–384.

'Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' (2014) Case no. C-131/12. *European Court of Justice*, ECLI:EU:C:2014:317 [Online]. Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62012CJ0131 (Accessed: 31 January 2025).

Hijmans, H. (2020) 'Article 1 subject-matter and objectives', in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 48–59.

Hildebrandt, M. (2020) 'Privacy and data protection', in Hildebrandt, M. (ed.) *Law for computer scientists and other folk*. Oxford: Oxford University Press, pp. 99–162.

Internet Archive (2024) *Wayback machine* [Online]. Available at: https://web.archive.org/ (Accessed: 28 April 2024).

Kelley, P.G., Bresee, J., Cranor, L.F. et al (2009) 'A "nutrition label" for privacy', in *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*. *the 5th Symposium*, ACM Press, pp.1-12.

Kollnig, K., Binns, R., Dewitte, P. et al (2021) 'A fait accompli? An empirical study into the absence of consent to {third-party} tracking in Android apps', in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* [Online]. Available at: https://www.usenix.org/system/files/soups2021-kollnig.pdf (Accessed: 30 January 2025).

Kollnig, K., Binns, R., Van Kleek, M. et al (2021) 'Before and after GDPR: tracking in mobile apps', *Internet Policy Review*, 10(4) [Online]. Available at: https://doi.org/10.14763/2021.4.1611 (Accessed: 30 January 2025).

Kollnig, K., Shuba, A., Van Kleek, M. et al (2022) 'Goodbye tracking? Impact of iOS app tracking transparency and privacy labels', in *2022 ACM Conference on Fairness, Accountability, and Transparency. FAccT '22*, ACM, pp. 508–520.

Kotschy, W. (2020) 'Article 6 lawfulness of processing' in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 321–344.

Krämer, J. (2024) 'The death of privacy policies: how app stores shape GDPR compliance of apps', *Internet Policy Review*, 13(2) [Online]. Available at: https://doi.org/10.14763/2024.2.1757 (Accessed: 30 January 2025).

Kranenborg, H. (2020) 'Article 17 right to erasure ("right to be forgotten")' in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 475–484.

Kröger, J.L., Raschke, P. and Bhuiyan, T.R. (2019) 'Privacy implications of accelerometer data: a review of possible inferences', in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. ICCSP*, ACM, pp. 81–87.

Kuner, C., L.A. Bygrave, and C. Docksey (eds) (2020) *The EU General Data Protection Regulation (GDPR): a commentary*. Oxford: Oxford University Press.

Kyi, L., Shivakumar, S. A., Santos, C. T. et al (2023) 'Investigating deceptive design in GDPR's legitimate interest', in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI '23*, ACM, pp. 1–16.

Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2025). 'Mapping the empirical literature of the GDPR's (In-) effectiveness: A systematic review', in *Computer Law & Security Review*, *57*, 106129 [Online]. Available at: https://doi.org/10.1016/j.clsr.2025.106129 (Accessed: 9 May 2025).

Linden, T., Khandelwal, R., Harkous, H. et al (2019) 'The privacy policy landscape after the GDPR'. arXiv [Online]. Available at: https://doi.org/10.48550/arXiv.1809.08396 (Accessed: 30 January 2025).

Machuletz, D. and Böhme, R. (2020) 'Multiple purposes, multiple problems: a user study of consent dialogs after GDPR', *Proceedings on Privacy Enhancing Technologies*, 2020(2), pp. 481–498.

Mangini, V., Tal, I. and Moldovan, A.-N. (2020) 'An empirical study on the impact of GDPR and right to be forgotten – organisations and users perspective', in *Proceedings of the 15th International Conference on Availability, Reliability and Security. ARES 2020*, ACM, pp. 1–9.

Matte, C., Bielova, N. and Santos, C. (2020) 'Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework', in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 791–809.

'Meta Platforms v. Bundeskartellamt' (2023) Case no. C-252/21. *European Court of Justice*, ECLI:EU:C:2023:674 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0252 (Accessed: 31 January 2025).

Nguyen, T.T., Backes, M. and Stock, B. (2022) 'Freely given consent?: Studying consent notice of third-party tracking and its violations of GDPR in Android apps', in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. CCS '22*, ACM, pp. 2369–2383.

Nouwens, M., Liccardi, I., Veale, M. et al (2020) 'Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence', in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. CHI '20*, ACM, pp. 1–13.

Parker, L. Halter, V., Karliychuk, T. et al (2019) 'How private is your mental health app data? An empirical study of mental health app privacy policies and practices', *International Journal of Law and Psychiatry*, 64, pp. 198–204.

'Patrick Breyer v. Bundesrepublik Deutschland' (2016) Case no. C-582/14. *European Court of Justice*, ECLI:EU:C:2016:779 [Online]. Available at: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:62014CJ0582 (Accessed: 31 January 2025).

Polčák, R. (2020) 'Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject', in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 398-412.

Quinn, P. and Malgieri, G. (2021) 'The difficulty of defining sensitive data – the concept of sensitive data in the EU data protection framework', *German Law Journal*, 22(8), pp. 1583–1612.

'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)' (2016) *Official Journal* L 119, 4 May, pp. 1–88, [Online]. Available at: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: 30 January 2025).

Rodriguez, D., Yang, I., del Alamo, J. M. et al (2024) 'Large language models: a new approach for privacy policy analysis at scale', *Computing* [Preprint Online]. Available at: https://doi.org/10.1007/s00607-024-01331-9 (Accessed: 30 January 2025).

Rupp, E., Syrmoudis, E. and Grossklags, J. (2022) 'Leave no data behind – empirical insights into data erasure from online services', *Proceedings on Privacy Enhancing Technologies*, 2022(3), pp. 437–455.

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P. et al (2019) 'Can I opt out yet?: GDPR and the global illusion of cookie control', in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. Asia CCS '19*, ACM, pp. 340–351.

Santos, C. Rossi, A., Chamorro, L. S. et al (2021) 'Cookie banners, what's the purpose?: Analyzing cookie banner text through a legal lens', in *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. *CCS '21*, ACM, pp. 187–194.

Serveto, M.M. (2020) 'Exercising GDPR data subjects' rights: empirical research on the right to explanation of news recommender systems reports: practitioner's corner', *European Data Protection Law Review (EDPL)*, 6(4), pp. 593–601.

Shipp, L. and Blasco, J. (2020) 'How private is your period?: A systematic analysis of menstrual app privacy policies', *Proceedings on Privacy Enhancing Technologies*, 2020(4), pp. 491–510.

Siapka, A. and Biasin, E. (2021) 'Bleeding data: the case of fertility and menstruation tracking apps', *Internet Policy Review*, 10(4) [Online]. Available at: https://doi.org/10.14763/2021.4.1599 (Accessed: 30 January 2025).

Smits, J.M. (2017) 'What is legal doctrine? On the aims and methods of legal-dogmatic research' in Van Gestel, R., Micklitz, H.-W. and Rubin, E.L. (eds.) *Rethinking legal scholarship: a transatlantic dialogue*. New York: Cambridge University Press, pp. 207–228.

Solove, D.J. (2012) 'Privacy self-management and the consent dilemma', *Harvard Law Review*, 126, pp. 1880-1903

Streinz, T. (2021) 'The evolution of European data law' in Craig, P. and De Búrca, G. (eds.) *The evolution of EU law*. 3rd edn. Oxford: Oxford University Press, pp. 902–937.

Svantesson, D.J.B. (2020) 'Article 3 territorial scope' in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 74–99.

'Tietosuojavaltuutettu v. Jehovan todistajat' (2018) Case no. C-25/17. *European Court of Justice*, ECLI:EU:C:2018:551 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62017CJ0025 (Accessed: 31 January 2025).

Towfigh, E.V. (2014) 'Empirical arguments in public law doctrine: should empirical legal studies make a "doctrinal turn"?', *International Journal of Constitutional Law*, 12(3), pp. 670–691.

'UF and AB v. Land Hesse (Joined party: SCHUFA Holding AG)' (2023) Joined Cases C-26/22 and C-64/22. *Opinion of Advocate General Pikamäe*, ECLI:EU:C:2023:222 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0026 (Accessed: 31 January 2025).

'Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH' (2018) Case no. C-210/16. *European Court of Justice*, ECLI:EU:C:2018:388 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CC0210 (Accessed: 31 January 2025).

Utz, C., Degeling, M., Fahl, S. et al (2019) '(Un)informed consent: studying GDPR consent notices in the field', in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. *CCS '19*, ACM, pp. 973–990.

'Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH' (2019) Case no. C-673/17, *European Court of Justice*, ECLI:EU:C:2019:801 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62017CJ0673 (Accessed: 31 January 2025).

Wagner, I. (2023) 'Privacy policies across the ages: content of privacy policies 1996–2021', *ACM Transactions on Privacy and Security*, 26(3), pp. 1–32.

Waldman, A.E. (2020) 'Cognitive biases, dark patterns, and the "privacy paradox"', *Current Opinion in Psychology*, 31, pp. 105–109.

Waldman, A.E. (2021) *Industry unbound: the inside story of privacy, data, and corporate power*. Cambridge, New York: Cambridge University Press.

Zanfir-Fortuna, G. (2020) 'Article 13 information to be provided where personal data are collected from the data subject' in Kuner, C. et al (eds) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 413–433.

Zhang, S., Feng, Y., Yao, Y. et al (2022) 'How usable are iOS app privacy labels?', *Proceedings on Privacy Enhancing Technologies*, 2022(4), pp. 204–228.