Data Protection is a continuously growing research field. Personal data processing impacts not only the individuals, their dignity and autonomy, but also the society as a whole. In the words of Stefano Rodotà ‘the democratic nature of any society can be also gauged by the extent to which personal data are actually protected’.1

The COVID19 pandemic greatly illustrates the multi-faceted nature of data protection. Data concerning health became of paramount importance not only for the so-called social distancing measures, but also for medical research. At the same time, we all witnessed vast collection, commercialisation and often misuse of personal data. Health apps with the green certificates necessary for travelling, apps promising to limit the spreading rates of the virus by notifying citizens of infected persons in their proximity, and access policies involving temperature measuring of employees.2 The necessity and proportionality of processing of all those data in the name of public health is questionable. Especially, given the false promises of many of those measures.3 In parallel, Public Private Partnerships became the new norm, legitimising access to and use of data, often coupled with allegations on inappropriate data security guarantees.4 The COVID19 example teaches us the importance of personal data and of rules on fair and proportionate processing, but also the relevance of data protection as a regulatory field, and consequently of data protection research.

This Handbook aims at depicting the actual scholarly, state-of-the-art overview of research and the scope of current thinking in the field of European data protection in a multi-disciplinary manner, and reflecting on current issues that will mark the next generation of research.

Several reasons make the publication of this Research Handbook on European Data Protection so timely.

1 Rodotà, Stefano ‘Data protection as a fundamental right’ in Gutwirth Serge et al. (eds) Reinventing Data Protection? (Springer, 2009).
First, 2021 marks the five-year anniversary from the publication of the General Data Protection Regulation (GDPR),5 the European Union’s general legal framework providing rules on processing of personal data, and the three-year anniversary since the GDPR started applying. A considerable number of scientific articles have been published analysing and interpreting what the new framework entails and raising new and open questions. Guidance and opinions by national supervisory authorities and the European Data Protection Board have been published as well, aiding everyone – data controllers, processors, data subjects and regulators – in complying with the GDPR. Data Protection Authorities and courts are processing complaints and have imposed administrative fines for violation of a range of provisions such as insufficient legal basis for processing, data security measures, and insufficient fulfilment of data subjects’ rights.6 The long-awaited GDPR has now been published and tested long enough for researchers to be able to assess its strengths and weaknesses in terms of achieving its goal to safeguard fundamental rights, its application and enforcement.

Second, there is a rapidly evolving “act-ification”7 currently taking place in the EU law-making with Commission proposals for new legislation on a range of areas that are pertaining to data protection or have an impact on data protection as a regulatory field and its secondary legislation. Recent examples are the Data Governance Act Proposal,8 the Digital Services Act Proposal,9 the Digital Markets Act Proposal,10 but also the Proposal for AI Regulation.11 These developments create a need for tilting or reframing data protection as a research field. What are all these instruments adding to European data protection? How do they interact, compete or complement each other? Such questions are also relevant not only for new legislative proposals, but also for traditional fields of law such as consumer and competition law. In the past decade, we witnessed a growing co-evolution and interrelation of competition law, consumer law, and data protection12 reaching as far as using each other’s

12 Preliminary Opinion of the European Data Protection Supervisor ‘Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection
enforcement tools. One should, however, not look only outside the EU data protection law; the jigsaw between different data protection laws, such as the GDPR and the Law Enforcement Directive (LED) is an interesting one and a challenge to be solved.

Third, the judicial developments, especially by the Court of Justice of the European Union (CJEU), have an impact on the understanding of the fundamental right of Article 8 of the Charter of Fundamental Rights of the European Union (CFR). The recent Schrems II ruling, in which the Court annulled for the second time the Commission Decision finding the US a country with adequate level protection of personal data, and Privacy International, in which the Court ruled that bulk interception is not allowed for the purpose of safeguarding national security, are landmark cases that shape data protection concepts and force policy-makers back to the drawing board. The CJEU is taking a role similar to the one of a constitutional court in the area of human rights, including data protection, which requires to view the law and policy through the lens offered by the court’s rulings.

Fourth and final, the constant driver for re-interpretation and adaptation of European data protection due to technology. The recurring question of mutual shaping between law and technology, becomes more imminent with the rise of computational capacity and the wide use of machine and deep learning algorithms. Questions of agency in algorithmic decision-making, the need for transparency, accountability, and human oversight are raised.

This Research Handbook offers analyses and research directions on all those current aspects of data protection as a research field. The audience of this Handbook is academics, students, legal scholars and post-graduate researchers working in the areas of privacy, data protection, big data, Information Technology, EU and human rights law. Practitioners and regulators will also benefit from this book. The volume provides theoretical insights on various issues such as state surveillance, control, participation, and transparency but also hands-on analyses of current topics such as data protection impact assessments, data portability and whistleblowing.

---

14 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
15 Judgment of the Court of 16 July 2020, Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, EU:C:2020:559.
Further, while the Handbook primarily focuses on European Union legislation, it is not only useful for European audience but for a world-wide audience, which becomes clear from the extraterritorial application of the EU data protection law and international data flows, as well as the adoption of EU data protection principles and even copying GDPR provisions in other jurisdictions, for instance through the Brussels-effect.

Data protection is constantly in transition and this Handbook covers a remarkable collection of contributions, both in terms of range of topics and depth of analysis.

The book starts with a Chapter from Vogiatzoglou and Valcke on data protection as a fundamental right. Until the CFR came into effect, data protection was covered under the right to privacy (for instance under Art. 8 ECHR). This has changed with the CFR, which contains data protection (Art. 8) as an independent right next to privacy (Art. 7). The Chapter provides the historical context to this relatively new fundamental right and delves into a discussion on its relation with other rights, such as privacy and informational self-determination, and the EU secondary data protection law. Further, the Chapter untangles the current conceptualisations and debates on the right to data protection, promises and pitfalls, and takes a normative stand by developing and demonstrating a novel approach to explaining the independence of the right to personal data protection. Next, in Chapter 2 Míšek discusses the GDPR as a performance-based regulation. In such an approach, the legislator only sets a goal which must be reached, instead of strictly outlining to the regulated subjects how specific actions should be done. Therefore, the regulated subjects can find their own ways to reach the set goal, which allows for more flexibility in fulfilment of their duties. The chapter argues that the combination of the principle of accountability and the risk-based approach constitute performance-based regulation in the GDPR. The provisions set out the objective that the processing of the data controller complies with GDPR. However, they do not regulate what specific steps are necessary and how the data controller should achieve the set objective. This decision is left to the data controller that must decide about the extent of the duties on their own and must be able to prove that their decision was correct.

The next two contributions focus on the interaction of the EU data protection instruments. Kosta in Chapter 3 examines the choices of the European legislator when regulating on data protection. The Chapter provides an overview of the complex matrix of primary law provisions that set the framework for the regulation of data protection in the European Union and questions the choices of the European legislator in developing a multi-partite system with fragmented data protection rules. Brewczyńska in Chapter 4 delves in the secondary law, the GDPR and LED, and identifies critical areas, which bring into question the process of harmonisation of the rules for data processing in the law enforcement context and invite a question.

21 Such as in the Kenya Data Protection Act 2019, see Mukiri-Smith, Hellen and Ronald Leenes ‘Beyond the Brussel’s effect? The Kenya’s Data Protection Act (DPA) 2019 and the General Data Protection Regulation (GDPR) 2018’, (forthcoming) for a comparison between the two regulations. Also the Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018, has many similarities to the GDPR. Also in the US, GDPR principles are increasingly being adopted, such as in the California Consumer Privacy Act of 2018 (CCPA), effective January 1, 2020.


23 The presentation that follows is based on summaries provided by the authors’ themselves, sometimes modified by the editors.
of legal certainty. Areas of concern are, according to Brewczyńska, the lack of clarity of the notion of criminal offence, the diversity of the domestic organisation of the criminal justice process that is unaccounted for by the LED, and the inclusion of the vague purposes of crime prevention and of safeguarding against and prevention of threats to public security in the scope of LED.

The following Chapters explore the interrelation of data protection with other fields of (legal) research. In Chapter 5, Aidinlis studies the Government-to-Business (G2B) data sharing and the emergence of a practice of applying advanced big data analytics to generate insights for the design and implementation of public policies using initiatives and developments in the COVID19 crisis as an example. The Chapter looks into G2B practice and questions of public-private partnerships, how the GDPR is equipped to address those current issues and proposes a new conceptualisation of ‘public’ interest under Article 6(1) (e) GDPR. Next, D’Amico analyses the interrelation between EU data protection regulation and competition law in the digital market, by developing a framework that classifies the different dimensions of their relationship. The identification of the diverse ways in which the regimes relate to one another, when it comes to issues around data and market power, sheds light on how to optimise the interrelation between the regimes and enhance the effectiveness of the regulatory framework as a whole. A main problem that has been identified in the chapter is data protection authorities’ refusal to perceive data within a market context, which prevents them from designing their policies in a way that supports the market functioning. In Chapter 7, Foss-Solbrek and Glenster delve into data protection and intellectual property. The Chapter examines how the use of the Trade Secret Directive (TSD) by data controllers to prevent the disclosure of algorithms and algorithmic data, is potentially at odds with the requirements in the GDPR. The authors compare the legal requirements under both the GDPR and the TSD, and suggest that there may be a yet-to-be explored public interest ground that could compel companies to be more forthcoming with their algorithms and algorithmic data to achieve algorithmic transparency. They propose the adoption of explicit guidance that give the national supervisory authority the right to demand algorithmic disclosure on public interest grounds. This will be one step in the direction of ensuring that companies are held accountable to the implicit standard of ‘algorithmic transparency’ that is already present in the law. Yet, it does not negate the conundrum of the inclusion of a reference to the right to trade secrets in the GDPR, if that inclusion is meant to have no effect. In Chapter 8, Thalia Prastitou Merdi addresses the very topical issue of the interface between consumer protection law, and in particular Directive (EU) 2019/770, concerning contracts for the supply of digital content and digital services (DCD) and data protection law. The DCD, through an innovative legislative addition, applies for the first time where the consumer provides personal data to the trader in exchange of digital content or a digital service. This Chapter examines how, and to what extent, EU data protection rules, fit in purely EU consumer protection legislation. The chapter looks both, inside and around the DCD, and examines the wording of this legislative initiative and the various questions, concerning ‘data paying’ consumers, that remain unanswered. The author concludes that, although the inclusion of personal data under the scope of application of the DCD, is a truly welcome outcome, as it aligns the level of consumer protection regardless of whether one pays a monetary price or provides personal data, this is not ‘an absolute champion’ and there is still space and need for improvement. In the following Chapter 9, Trzaskowski also looks at the relation between data protection and consumer law in the context of data-driven business models. The Chapter introduces a model with tiers of
information asymmetry that elucidates the position of power between service providers and users, and explores the implications of ‘free’ services and the user’s ability to ‘understand the deal’ is included. It concludes that despite many years of political attention, the CJEU still has not answered the three central questions in this domain which are: (1) To what extent is the commercialisation of our privacy allowed? (2) Do technology and markets serve the user, or vice versa? and (3) To what extent should we rely on individual citizens/consumers to read, understand, and fend for themselves in commercial markets with significant information asymmetries that are not easily levelled by means of information? The author argues that data protection law and consumer protection law have substantial overlaps in this area and can be used in tandem to cross-fertilize the legal framework that aims to ensure empowerment and transparency as well as the protection of citizens’/consumers’ privacy and economic interests.

Next, Leiser analyses in Chapter 10 the legal frameworks for the protection of ‘consumers’ and ‘data subjects’ from manipulative design features. ‘Dark patterns’ describes a variety of techniques designed to push users towards taking certain steps that benefit the provider at the expense of the user’s autonomy. They are found in both the user interface and the system architecture and are usually characterised as malicious nudges that direct users to agreeing to terms and conditions or to the processing of personal data. The author argues that, not only is cooperation needed between consumer and data protection regulators, but that a pluralistic approach, that mixes the strengths of one regime while compensating for the weaknesses of the other, is needed to regulate manipulative design techniques like dark patterns. In Chapter 11, Almada and Dymitruk analysing the interplay between the rights to data protection and a fair trial in judicial automation. The chapter discusses the implications and barriers of introducing automated decision-making (ADM) in court proceedings. While this to some extent is no different than ADM in any other context, the requirement of fair trial colours the data protection assessment somewhat. The authors argue that any analysis of an automated decision-making system must consider how judicial automation might impact the rights of the parties to proceedings. If an automated decision-making system demands unacceptable compromises over procedural rights, particularly the right to a fair trial, then this form of automation is unlawful, regardless of its compliance with data protection requirements. The right to a fair trial in the context of judicial automation cannot be subsumed into data protection requirements. Nevertheless, data protection law contributes to judicial fairness by requiring the incorporation into judicial automation systems of measures and safeguards for the right to a fair trial. By imposing informational and procedural requirements for judicial automation systems, data protection by design requirements provide data subjects with some – but not all, at this point – of the information needed for contesting automated judicial decisions.

Having explored the interaction of data protection with other fields, the following two contributions examine the territorial scope of the EU data protection law. Henseler and Tamò-Larrieux in Chapter 12 discuss the extraterritorial application of the GDPR and its impact for compliance of companies globally. The authors show that European Union data protection law already had legal relevance beyond the EU borders prior to the GDPR through a discussion of the Google Spain, Weltimmo and Verein für Konsumenteninformation case law. The GDPR extends the extraterritorial reach of European data protection law by incorporating the ‘targeting criterion’. According to this criterion, data processing falls within the scope of application of the GDPR whenever data of a subject in the EU is processed relating to the offering of (free) goods and services or to the monitoring of behaviour. The authors argue that not only technical developments, such as the mentioned means of ‘surveillance cap-
italism’, but also social movements and economic rationales have influenced the evolution of data protection law. They notice a push for data protection and privacy regulation on a global level and that this push is partly motivated by the EC adequacy decision, i.e., the recognition of other countries’ compatibility with the GDPR as well as the extraterritorial reach of the GDPR. The GDPR’s reach beyond EU territory therefore plays a vital role in promoting the protection of fundamental rights and freedoms of natural persons in the digital world. In Chapter 13, Drechsler and Kamara focus on international data transfers, the impact of the CJEU Schrems II ruling on data transfers as regulated in the GDPR and the notion of ‘essential equivalence’ both as a standard and as a test to understand when the necessary conditions are fulfilled for data transfers to be permitted outside the Union. The Chapter shows that the regulation of data transfers is at a crossroads; while the rationale of the data transfers rules in the GDPR has not changed after Schrems II, the ruling placed fundamental rights at the core of contractual means for data transfers, and re-invited attention for the implementation of the GDPR data transfers rules on the ground and their enforcement.

The following contributions focus on the data protection law’s key concepts and principles and analyse and interpret those, taking into account how concepts and principles are influenced by technology. Wisman and Tijm focus on the purpose limitation principle. Chapter 14 analyses normative functions which the purpose limitation principle serves and adds clarity to the complex relationship between data protection law and the right to privacy. Article 6(4) GDPR allows EU Member States to adopt legislation for the deployment of invasive profiling practices. Legislation implementing such permissions and which could breach the purpose limitation principle still needs to meet the requirements imposed by Article 8 ECHR or Article 7 and 52 CFR. Moreover, even though this reframing in the GDPR seems to be positioned in a way that it allows for a permissive interpretation of the exceptions allowed from purpose limitation, this is still at odds with the ‘rule-exception rationale’ of Article 8 ECHR. The Chapter also sheds light on the rationale and the aims of the reframing of the purpose limitation principle in the GDPR by elaborating on the well-documented ambitions of the Dutch government regarding big data legislation for profiling purposes. The authors argue that Article 6(4) GDPR wrongfully implies that the substantive protection which follows from the law can also be broken down by the law. Doing so would disregard at least one of the goals data protection shares with human rights: to impose substantive limits on the power of the government. If such an instrumental approach is taken to the GDPR, legislators will use it to sideline fundamental rights and constitutional principles of law, which were developed to protect citizens against the concentration of power. The GDPR could turn out to be the Trojan horse for the right to privacy and all it intends to protect.

The purpose limitation principle is also the topic of Bentzen’s chapter (Chapter 15) which examines the evolution of the purpose limitation principle, and how it became a central principle in EU data protection law. Through examining CJEU’s jurisprudence, the author identifies a strong focus on the importance of context and on the individual's reasonable expectations, aligning with Nissenbaum’s theory of contextual integrity. The theory of contextual integrity shares similarities with the principle of purpose limitation, as they both aim to protect people by limiting data about them being used in a way or for purposes they find unexpected or inappropriate. The author shows that empirical data protection research emphasizes this point. People do not mind sharing personal data about themselves, or for the personal data to be reused for other purposes, provided that they consider the data sharing to be appropriate. She argues that the purpose limitation principle must itself consider the context it functions within.
Specifically, respect for social principles and context norms will help determine the individual’s reasonable expectations of the data processing and any subsequent reuse. Only then can we rest assured that the data processing is not just legally, but also societally acceptable.

In Chapter 16, Lee et al. delve into the risks of ADM systems using AI and how these risks can be understood. The Chapter discusses the inherent ambiguities of AI and ADM definitions to come to an extensive set of definitions of algorithms, profiling, ADM, and AI models and how they relate to each other. The terminology developed in the Chapter is then used to provide a holistic risk assessment that takes into consideration a broader set of risk factors than the selected technology. This kind of risk assessment is illustrated by looking at different kinds of hiring systems. The authors argue that rather than a top-down approach of applying blanket governance changes to all systems using AI, organisational risk management should entail a more holistic approach considering technology-agnostic risk factors. They suggest three dimensions (context, process, technology) and six sub-dimensions of risk factors (technique, data, technical process, business process, domain, and potential impact) as exemplar considerations for driving a more complete risk assessment, accounting for the relevant regulations and guidance materials. This approach would support more appropriate and effective organisational governance regimes across all algorithmic systems.

In Chapter 17 Nisevic et al. research the implications of the legal bases for ADM under the GDPR. Although the GDPR establishes the framework in which ADM can take place under Article 22, it leaves much to be desired. The chapter introduces ADM processes and Article 22 of the GDPR, the legal bases for ADM – contract, member state law, and explicit consent – in more detail. Issues with Article 22, such as the meaning of ‘necessary for entering into... a contract’, which seems to imply that the ADM process can be carried out without a contract between the data controller and the data subject, which should not be the case, and the meaning of ‘explicit consent’ (as opposed to ‘regular’ consent) are discussed. The authors conclude that Article 22 GDPR requires data controllers should acquire consent from the data subject in writing or a similarly definitive form of expressing consent on top of the requirements of regular consent; moreover, consent needs to be obtained separately for each purpose for which the personal data is used. They also argue that since the ADM is a process based on complex rules that are poorly understood and can adversely affect individuals’ personal lives, their inherent complexity and the speed with which decisions are being made challenge the transparency of the processes and their explainability, which only further frustrates the data subject’s ability to adequately consent.

Next, in Chapter 18, Custers et al. analyse the role of consent in the algorithmic society and offer a re-conceptualisation to address system failures of consent. Consent is enshrined in data protection law since its very beginning. In particular, within the private sector, the legal ground of consent today under the GDPR, and already under the preceding Directive 95/46/EC, plays a central role. With the GDPR, the formalities of how consent must be obtained have been further harmonised throughout the EU keeping constant its goals: empowerment of the users, (informational) self-determination, autonomy. While it has been claimed that consent combined with the information requirements of the GDPR can be helpful in managing (privacy) expectations of a data subject, it has become clear that consent mechanisms have many failures. The authors argue that rethinking of consent might include reforming the data protection framework in a way that consent is no longer a stand-alone legitimate basis for processing, but merely a factor in determining legitimate interests, or, that the self-determination approach of data protection law could be altogether abandoned. Instead, regulation would
Introduction

target the design and infrastructure of products and services by providing clear obligations on how data may be processed. Such attempts, however, likewise trigger serious challenges (e.g. lack of innovation, paternalism), which the authors discuss in their contribution. In the following Chapter 19, Chen, Dove, and Bhakuni critically examine the boundaries, in the context of sensitive personal data, between explicit consent and alternative data protection processing grounds for health research from three interrelated perspectives, i.e., normative, doctrinal, and comparative. The authors identify a divergence which most likely stems from a combination of the unsettled debates about the merits of consent, the conceptual conflation of consent within different fields, and the remarkable segmentation of national approaches in this regard. Finally, the authors suggest that a plausible approach for data subject consent in the health research context lies somewhere between the baseline GDPR model, where consent is not privileged at all, and the stringent regimes where consent is given too much favoritism.

Christofi et al. in Chapter 20 examine data protection, control and participation beyond consent. The chapter analyses Article 35(9) GDPR, discussing why data subjects should be involved in DPIAs and how such involvement faces practical challenges. It shows the potential of Article 35(9) GDPR, alongside its challenges, to transform DPIAs to participatory processes, rather than technocratic ones that solely solicit input from information security and legal compliance experts. The authors argue that such participation can increase the legitimacy of DPIAs by enabling checks-and-balances vis-à-vis controllers’ decisions, improve the quality of DPIAs and, in line with data protection’s overarching goal of empowerment, supplement classic data protection control tools, such as consent and data subjects’ rights, with tools that enable understanding and influencing decisions on risks. Connected to data subjects’ empowerment, in the following Chapter 21, Naudts, Dewitte, and Ausloos contribute to on-going discussions regarding the role and function of data subjects’ rights in a digital society. More specifically, they seek to ascertain the function and role data rights can have in achieving meaningful transparency. In order to better harness the versatility of data transparency rights, the Chapter develops and advances a modular and multidimensional framework through which data transparency rights can be critically reflected upon, evaluated and further developed in a more nuanced and goal-oriented manner. The Chapter’s overarching goal is to offer researchers a comprehensive theoretical understanding concerning the role and function of data transparency rights, while also advancing a conceptual, critical and modular framework through which data transparency rights can further evolve as versatile tools towards a more transparent and balanced digital society. Continuing the perspective on data subject rights, Li in Chapter 22 explores the new right to data portability (RtDP). The author argues that the right to data portability is the end product of political compromise. It strays from the Commission’s initial proposal to mirror pro-competition measures and eventually got squeezed into the data protection straitjacket at high costs. This compromise leads to the conundrum that one can barely do anything with the RtDP unless more related data are provided, but the provision of such additional data would be disallowed under the GDPR. The chapter argues that the EU is trying to fix this flaw by incrementalism, but that this would be of little use if the fragmented framework isn’t subject to change. The EU approach is contrasted with that of the UK, which even before Brexit facilitated data portability and interoperability independent of its data protection framework. This contrast, according to Li, is helpful to consider the way forward for the EU.

The last Chapter explores solutions beyond data subjects rights. In Chapter 23, Lachapelle explores whistleblowing as an enforcement tool of data protection. While representing a key
player in vigilance mechanisms, ‘whistleblowers’ have not been given any role in the ‘governance structure’ established by the initial ‘Data Protection Directive’ and by the GDPR. The author, however, argues that the principle of accountability and by putting the focus on the awareness raising of members of staff, the GDPR creates a setting for the development of whistleblowing. By promoting a new corporate culture based on transparency and reporting, the GDPR further initiates progressive decentralisation of law enforcement in Europe. The discussion then focuses on the impact of the 2019 Directive on the protection of persons who report breaches of Union law, may have on enforcement of data protection law arguing that whistleblowers are increasingly considered as guardians of the public interest. In the light of freedom of speech and the ECHR case law, the whistleblower is further no longer considered as a ‘private’ enforcement tool, but it is increasingly considered as a guardian of the public interest (‘watchdog’).