4. Deep Dive: Data Protection

Aengus Collins (EPFL)

Content

Index of Figures

Index of Tables

Introduction

Data protection is one of the most important policy domains for the EU in terms of its global governance ambitions and successes. It is routinely cited as a paradigmatic case of the so-called Brussels effect (Bradford 2020, 2012), and after decades of consistent consolidation and development the EU's data protection framework is now an unavoidable point of reference for the growing number of countries that are developing frameworks of their own (Greenleaf 2021). In this deep dive, we assess the evolution of the EU's data protection framework from the perspective of the TRIGGER model of actorness and effectiveness (Teebken, Jacob, and Guske 2019). It is hoped that this exercise will provide an insightful analysis of the data protection domain, but our overarching objective across the four deep dives is to assess how well our definition and operationalisation of the actorness and effectiveness concepts can capture real-world developments across a diverse set of policy domains.

Our data protection analysis proceeds in four stages. In our first chapter, we outline how data protection governance, in the EU and globally, has evolved since the 1980s until 2020. We highlight the steady progression in the EU from a patchy set of national data protection measures through to the implementation of the GDPR since 2018 – a process that has seen the EU consolidate its position as a global leader in this field. In the second chapter, we focus on actorness. We assess how the EU has performed over time on each of the seven dimensions in the TRIGGER actorness model. We look at three broad periods: from 1980 until the 1995 Data Protection Directive, from the directive through to the agreement of the GDPR, and until 2020. Although there are important differences between how the EU fares on different dimensions, the overall picture that emerges is an unambiguous one of increasing actorness. In the third chapter, we turn to consider effectiveness, which is defined in terms of external goal attainment. We identify six key goals of the EU in the data protection domain. Two are of particular importance: the protection of individual rights (where we highlight concerns around compliance and consent) and the positioning of the EU as a global driving force (where we conclude the EU has been highly effective). The effectiveness chapter also includes two case studies that focus on narrower 'micro' goals in specific negotiation contexts: the EU's Privacy Shield negotiations with the US, and its work with the Council of Europe to ensure that the CoE's revised Convention 108 is aligned with the GDPR. The deep dive then concludes with a short final section which highlights four factors that in our view are likely to be important determinants of the outlook for the EU in the data protection domain. These are (i) the need to prevent slippage on data protection fundamentals, such as consent; (ii) continuing challenges related to national fragmentation; (iii) possible trade-offs between strong data protection and levels of EU innovation and growth; and (iv) the prospect of further increases in the EU's international influence.

1. Global and EU governance of data protection: an overview

1.1 Global governance

This chapter of the deep dive on data protection looks at the evolution of global and EU governance since the 1970s, when technological developments pushed data protection onto the policy agenda. Although the governance landscape has evolved very significantly in the intervening decades, it remains something of a patchwork globally, with different principles being applied in different ways in different places. There has not been a landmark global agreement on data protection, equivalent to the Paris Climate Accords or the Sustainable Development Goals. Consequently, the analysis that follows is structured around a series of phases of activity, rather than around individual milestones. These phases are not rigidly defined, but they identify broad periods in which significant governance change took place.

As we shall see, one of the key global governance challenges has been to accommodate deepening patterns of data globalisation within a fragmented regulatory landscape. The European Union has been central to that process, with both formal mechanisms (such as 'adequacy' decisions) and more informal weight of influence – the so-called Brussels effect'(Bradford 2020) – making the EU's approach to data protection an increasingly important part of the global governance landscape. For this reason, there is significant overlap between some of the key milestones analysed in the two subsections that follow. In the first of these, on the evolution of global governance, discussion of developments in the EU is limited to those aspects that have made a significant difference to the evolution of the global picture. The second subsection looks more closely at the dynamics within the EU that have shaped the bloc's changing approach to data protection over the decades. Both of these strands – internal dynamics and external influence – will then feed into the next section of this report, which focuses on the EU's actorness in this policy domain.

1.1.1. A timeline of global governance

The following table provides a timeline of selected important developments in the evolution of the global governance of data protection. It also indicates the three phases into which this evolution has been divided for analysis in subsequent subsections.

Table 1 - Timeline of significant global governance developments

	Year	Development
Phase 1	1948	Universal Declaration of Human Rights (Art .12 includes privacy)
	1970	World's first data protection law, in Hesse, Germany
	1973	First national data protection law, in Sweden
	1970s	Introduction of national laws in countries including: Sweden, Denmark, Norway, Germany, Austria, France and the UK
	1980	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
	1981	Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)
	1990	UN Guidelines for the Regulation of Computerized Personal Data Files
Phase 2	1995	EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
	1995	US Privacy And The National Information Infrastructure: Principles For Providing And Using Personal Information
	1997	US A Framework for Global Electronic Commerce
	2000	EU-US: Safe Harbor adequacy decision
	2005	APEC (Asia-Pacific Economic Cooperation) Privacy Framework
	2007	OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy
	2011	ISO 29100 Privacy framework
	2012	Global Privacy Enforcement Network (GPEN) Action Plan
Phase 3	2013	Snowden revelations; trigger launch of Schrems I case
	2013	Revision of 1980 OECD guidelines
	2014	AU (African Union) Convention on Cyber Security and Protection of Personal Data
	2015	EU Schrems I CJEU verdict: Safe Harbor invalidated
	2015	EU-US 'umbrella agreement' covering data transfer for law enforcement
	2015	UN Special Rapporteur appointed
	2016	EU-US Privacy Shield introduced to replace Safe Harbor
	2016	EU General Data Protection Regulation (GDPR)
	2017	China Cybersecurity Law
	2017	EU-US Schrems II challenge to standard contractual clauses
	2018	Cambridge Analytica scandal
	2018	GDPR into force
	2018	Council of Europe Revised CoE Convention 108 (Convention 223)
	2018	Major national and subnational laws. California; Brazil; first India draft
	2018	China Personal Information Security Specification
	2019	ISO 27701 Privacy management
	2019	India revised law
	2019	Schrems II advocate general opinion (supports SCCs)

1.1.2. Phase 1: Up to 1995

1.1.2.1. Beginnings in Hesse

Data protection first became a significant focus of governance attention in the 1970s. The first data protection regulation was passed in 1970, in the German state of Hesse. (In general, the evolution of data protection governance has been driven by national, international or supranational actors, but it is interesting to note that subnational influence has increased again recently, with state-level legislation setting the pace in the United States – see the discussion of Phase 3 below.) The Hesse regulation highlights a feature of data protection global governance that has remained crucial ever since: the role of technological change as a driver of governance evolution. The Hessian Data Protection Act was a response to the advent of large-scale government databanks (Simitis 2010). In Hesse, such databanks began being used in the 1960s, with a view to improving long-term policymaking in areas such as finance, social security and healthcare. However, the potential misuse of sensitive medical or financial data for other purposes, has the potential to contribute to a surveillance society. There is an echo of more recent debates in the fact that one of the specific motivations for the statute was concern that Hesse's databanks might be used to 'manipulate an individual's behavior through the increasingly sophisticated processing or personal data' (Simitis 1995). The law only covered the automated processing of personal data in the public sector; the assumption was that no private-sector entity could have the financial and technological resources that would be needed to engage in mass data processing at the level of the population, even in a subnational polity (Simitis 2010).

Even the drafting of this first subnational regulation demonstrated the inherently international nature of this policy domain. Simitis (2010) notes that the passing of the Hessian act was preceded by a study of how US legislators were approaching similar issues. Although no US legislation had been passed at that point, Congressional hearings had been held in the late 1960s on topics including 'computer privacy' and a Congressional report had been published on 'privacy and the national data bank concept'.

The regulation in Hesse was followed by the passage of a series of national data protection laws during the 1970s, predominantly in Europe. Sweden was the first to pass such a national law, followed by others including Germany, France, Norway and Denmark. In three European countries – Portugal, Spain and Austria – early data protection rules were given constitutional force during the 1970s.

Outside Europe, in 1974 the US passed the Privacy Act, which focused on the risk of public-sector data processing leading both to breaches of individual privacy and to wider harms resulting from the misuse of 'information systems'. This law came a year after an important Department of Health, Education and Welfare committee report, *Records, Computers and the Rights of Citizens*, which introduced 'fair information practices' for the first time, an idea that has since become central to the governance of data protection (US Department of Health and Welfare 1973). These are the five principles suggested by the report:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about himself.
- Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

In general, however, data protection legislation in the US developed on a sectoral basis from an early stage (Cody 1998).

1.1.2.2. The OECD and Council of Europe

By the beginning of the 1980s, with computerised data processing and resulting concerns about data protection both on the rise, the formal internationalisation of governance in this area begins. The two key developments here are the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, published in 1980, and the Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, published a year later. One important feature of both the OECD and Council of Europe data protection principles is that they explicitly apply across both the public and private sectors, an important shift from initial assumptions that only the public sector could amass enough data to require safeguards. However, in terms of the substantive principles of data principles, there was continuity with the consensus that had been developing among a growing number of advanced economies during the 1970s.

The title of the OECD's 1980 guidelines captures a tension that remains important to the evolution of data protection rules today. On the one hand, the OECD recognised the growing importance of the kinds of privacy concerns that had begun to cause 'alarm' in the 1970s and that had prompted national legislators to begin putting protections in place (OECD 2013). On the other hand, the organisation's mandate was 'to foster economic growth and contribute to the expansion of world trade', and so it sought to ensure that data protection rules did not create barriers to the free flow of information that might hold back growth. Privacy and the free flow of data are referred to in the OECD Council Recommendation preceding the guidelines as 'fundamental but competing values' (OECD 2011). The OECD's objective was to try to align these competing values – to establish fundamental principles of data protection that would apply across its member countries, thereby giving them the confidence to allow data to flow freely between them, without worrying about data protection standards dropping. The guiding objective was to protect privacy in a way that would avoid the need for new restrictions on cross-border data flows.

The OECD guidelines were agreed in September 1980 and comprised eight national data protection principles and four principles relating to cross-border data flows. The principles were non-binding (OECD 2011).

- **Collection limitation.** Data collection should be lawful and fair, and 'where appropriate' with the knowledge or consent of the individual.
- **Data quality.** Personal data should be accurate, complete, up to date and relevant to their intended purpose.
- **Purpose specification.** The purpose of personal data collection should be made clear at the time of collection, and data should only be used for other purposes if this does not conflict with the original purpose and if the individual is informed.
- **Use limitation.** Personal data should not be processed except (i) with the consent of the individual, or (ii) the law requires it
- **Security safeguards.** Personal data should be protected against risks such as loss, unauthorised access, destruction, disclosure, etc.
- **Openness principle.** Individuals should be able to establish the existence, nature and purpose of personal data, as well as the identity and residence of the data controller.
- **Individual participation.** Individuals should be able to receive 'in a form that is readily intelligible' the personal data that a data controller holds about him.
- **Accountability principle.** A data controller should be accountable for complying with these principles.
- **International principle 1.** Countries should take into consideration the implications for other countries of their domestic processing and export of personal data.
- **International principle 2.** Cross-border flows of personal data, including through transit countries, should be uninterrupted and secure.
- **International principle 3.** OECD countries should not restrict cross-border flows of personal data to another OECD country unless: (i) the OECD principles are not observed there, (ii) re-export of the data could breach domestic privacy rules, or (iii) restrictions are justified by domestic legislation relating to certain categories of personal data.
- **International principle 4.** Countries should not use privacy and individual liberties as pretexts for introducing rules that exceed their stated purpose and are actually intended to impede cross-border flows of personal data.

The principles embodied in the Council of Europe's Convention 108 are broadly in line with those of the OECD. The similarity between the two sets of principles reflects two things: the fact that international consensus was already emerging in this area, and the fact that the two teams drafting their respective sets of principles worked in 'close collaboration' with each other (Council of Europe 1981). There is a difference in emphasis, however. While the potential tension between domestic regulation and international data flows is foregrounded in the OECD guidelines, the former has greater priority in Convention 108. According to an explanatory paper published with the convention: 'The object of this convention is to strengthen data protection, i.e. the legal protection of individuals with regard to

automatic processing of personal information relating to them' (Council of Europe 1981). The convention is also framed in terms of power and responsibility – 'Information power' brings with it a corresponding 'social responsibility' – a formulation with contemporary resonance given current efforts to adapt the governance of data protection for an era of big data, social media and giant technology companies.

There are three notable differences between the OECD guidelines and Convention 108. The first is that the convention is binding, although governments are free to decide how to implement its principles. The second is that the convention requires sensitive data to be treated differently. The OECD guidelines allow for special treatment of sensitive data but do not require it. And the third difference is that the convention applies only to the automated processing of data, whereas the guidelines cover manual records and processing too. Together the two sets of principles encapsulate the consensus on data processing principles that had developed during the 1970s, and that was being implemented in a growing number of countries, particularly in Europe. A broadly similar set of principles was included in the UN's *Guidelines for the Regulation of Computerized Personal Data Files* in 1990. More significantly, Convention 108 formed the basis for the EU's Data Protection Directive 95/46, which marked an important step in the globalisation of data protection governance.

1.1.3. Phase 2: 1995 to 2012

The second phase of the evolution of global governance of data protection, from 1995 to 2012, spans a period in which digital technology and economic globalisation advanced rapidly and in tandem, with the advent of the internet and e-commerce. If the first phase was characterised by the emergence of a broad consensus on data protection principles, the second phase is characterised by very different approaches taken on the two sides of the Atlantic. The EU built on Convention 108 to create its own binding data protection rules in the 1995 Directive. Two years later the US adopted an approach relying much more heavily on corporate self-regulation. The tension between these two approaches risked a rupture in transatlantic data flows. Efforts to square that circle began with the Safe Harbor programme in 2000 and still have not been fully resolved at the time of writing in 2020.

1.1.3.1. The EU: The 1995 Data Protection Directive

The dynamics that led to the agreement of the 1995 Data Protection Directive 95/46/EC are dealt with in the next section, which focuses on the evolution of European data protection governance. Our concern here is the impact that the directive, which took effect in 1998, had on the global governance landscape. The answer is that it had a very significant impact. Amply fulfilling the intention expressed by the European Council in 1994 'to set an example', the directive put in place a system of extraterritorial influence which over time has allowed the EU to become a regulatory superpower in this area (Simitis 1995).

The key provisions of the directive in this respect are the principle of adequacy (Article 25) and a series of derogations (Article 26), which set out the conditions under which data can be transferred to third

countries. In important ways, the directive closely mirrors the OECD and guidelines and the CoE's Convention 108. It establishes the principles of data protection that should apply across the EU, and it ties the free flow of personal data to the upholding of these principles. Where the directive differs is that it is backed by the economic heft of a bloc which in 1995 accounted for around 27% of global GDP. The directive ties data protection to market access, in a move described as 'aggressive' by more than one scholar (Salbu 2002).

The data protection principles embodied in the directive are based on those in Convention 108. Birnhack (2008) summarises them as follows:

> 'The core principles (art. 6), are that personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; that the data collected is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; that it is accurate and, where necessary, kept up to date; that it is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Furthermore (art. 7), personal data may be processed only under certain circumstances: if the data subject has unambiguously consented to the processing; if it is necessary for performing a contract to which the data subject is a party or complying with a legal obligation, protecting vital interests of the data subject, or if the processing is necessary for the public interest or for the controller's legitimate interests. The directive further prohibits the processing of special categories of data (art. 8), such as racial origins, political beliefs or data relating to health or sexuality.'

Chapter IV of the directive deals with the export of data to third countries. The adequacy principle is introduced in Article 25(1), which states that :

> 'The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this directive, the third country in question ensures an adequate level of protection.'

> The directive does not spell out what constitutes 'an adequate level of protection.' This question was left to a working party established by the directive and comprising representatives of the Member State supervisory authorities and of the EU institutions. In a working paper adopted in July 1998, the working party pointed to a set of 'core' requirements based on the provisions of the directive itself, covering both (i) legally enshrined data protection principles, and (ii) procedural and enforcement standards (WP12 1998). The working party added, however, that the definition of adequacy should 'not be set in stone', and it introduced the idea of risk-based assessment: 'The degree of risk that the transfer poses to the data subject will be an important factor in determining the precise requirements of a particular case.'

The directive goes on in Article 25(4) to spell out the consequences of a decision that a country does not have adequate levels of data protection: 'Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.' In practice, however, this situation did not arise. In the decade after the directive took effect, no countries were declared to have inadequate levels of data protection. This is not because all countries had adequate data protection measures in place. It is because the directive provided a number of derogations (Article 26) which data controllers in third countries could rely on to permit data transfers even if country-level protections were insufficient. Such a data transfer could be permitted if:

- the data subject had unambiguously consented to it (Article 26(1)(a)), or the transfer was necessary for the contractual reasons (Article 26(1)(b-c)) or to protect the public interest (Article 26(1)(d)) or the data subject's vital interests (Article 26(1)(f));
- it was part of a business-to-business data flow that was based on 'standard contractual clauses' written by the Commission with a view to ensuring adequate levels of data protection (Article 26(4));
- it was an intra-company transfer within a multinational company, and was covered by 'binding corporate rules' that embody the directive's data protection principles (Article 26(2); Birnhack 2008, 514).

The absence of many formal adequacy decisions, coupled with the ability of third-country data controllers to use the derogations to justify data transfers, may suggest that the directive had limited direct global governance impact. But this would miss the catalysing role that the directive played by establishing a new benchmark for data protection and creating incentives for third-country actors to increase their standards. These incentives were material, via the easing of commerce with the EU and the facilitation of domestic data-based economic activity. But there was also an important symbolic incentive in some cases, where adoption of the EU's best practice was a marker of a country's modernity (Birnhack 2008). However, neither of these incentives carried much weight for the US, which in the mid-1990s was the world's unrivalled superpower and the engine of the burgeoning era of e-commerce. Its approach to data protection in the internet era was to be very different from the EU's.

1.1.3.2. The US: Self-Regulation and Safe Harbor

As we will see in the next section on EU governance, one important background factor in the development of the 1995 Directive was the evolution of the EU into an increasingly political as well as an economic union. The responsibility of the EU institutions for the smooth functioning of the single market began widening to include the protection of individuals' fundamental rights. Accordingly, the directive strikes a balance between focusing on data flows as a matter of economics or individual rights. As Simitis notes, this marked a particular change for the Commission, the engine behind the directive's development, which had previously seen data more narrowly in terms of economic activity and the single market (Simitis 1995).

In the US, the direction of travel was in the other direction. In the mid-1990s the debate on data protection governance shifted firmly towards innovation and growth and towards relying on market-based regulatory mechanisms. It is easy to over-simplify the regulatory differences between the US and the EU (Wiener et al. 2017). However, this broad pattern of the US leaning more towards markets and the EU more towards rights persists as a feature of transatlantic data protection governance (Schwartz and Peifer 2017). It also influences digital governance trends more generally (Collins et al. 2020).

As we saw earlier, it was in the US that the first list of 'fair information practices' was drafted, before being taken up and consolidated by the OECD and CoE. With the advent of the internet in the 1990s, there was renewed debate about fair information practices and principles (Cody 1998). For example, sets of principles were drawn up by the Information Infrastructure Task Force (IITF), the Federal Trade Commission (FTC) and the National Telecommunications and Information Administration (NTIA). However, the landmark statement of internet governance principles in the US during the 1990s was a 1997 document from President Clinton entitled 'A Framework for Global Electronic Commerce' (White House 1997). Although this acknowledged the principles developed by the IITF, FTC and NTIA, its overriding message was the internet – including privacy and data protection issues arising on the internet – should be governed by private-sector self-regulation, as opposed to the kind of top-down government regulation embodied by the EU Directive. This overarching philosophy rests on the role of innovation and growth. The US view was that the early growth and commercialisation of the internet had been due to private initiative and that this process should be allowed to continue:

> 'Though government played a role in financing the initial development of the internet, its expansion has been driven primarily by the private sector. For electronic commerce to flourish, the private sector must continue to lead. Innovation, expanded services, broader participation, and lower prices will arise in a market-driven arena, not in an environment that operates as a regulated industry. Accordingly, governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organisations to develop mechanisms to facilitate the successful operation of the Internet' (White House 1997).

This approach extended to privacy concerns, with the government arguing that the private sector should lead, and there is only a weak suggestion that the government will step in if the private sector is found lacking. It is also important to note that any envisaged government intervention is seen as grounded on individuals' rights as consumers rather than their fundamental political rights as in the EU:

> 'The Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution. The Administration also anticipates that technology will offer solutions to many privacy concerns in the online environment, including the appropriate use of anonymity. If privacy concerns are not addressed by industry through self-

regulation and technology, the Administration will face increasing pressure to play a more direct role in safeguarding consumer choice regarding privacy online' (White House 1997).

This approach was seen by some as a missed opportunity to develop an omnibus approach to privacy and data protection in place of the status quo, an ad hoc approach that had 'led to incoherence and significant gaps in the protection of citizens' rights' (Reidenberg 1999). Given this backdrop, one unavoidable question was how data flows (and related trade in goods and services) between the US and the EU – by far the two largest economic centres in the world at the time – would be facilitated. Greer (2011) notes unsurprisingly that the US assessed that its data protection regime would not be declared 'adequate' by the EU. Rather than rely on the EU Directive's Article 26 derogations, two years of EU-US negotiations were launched, with a view to establishing a joint legal framework that would meet the adequacy threshold.

The result was the Safe Harbor programme, which was declared adequate by the EU in July 2000 and which took effect in November 2000, becoming a key feature of the global governance landscape until 2015, when it was ruled invalid by the CJEU. The idea at the heart of Safe Harbor was to 'bridge the gap' between the self-regulatory regime of the US and the EU's requirement for legally enforceable protections (Kobrin 2004). The FTC was given a crucial role in achieving this aim. Participation in Safe Harbor was entirely voluntary for US companies. Those that decided to participate had to declare that they were in compliance with a series of data protection principles that met the EU's requirements. There were seven principles (Stevens 1999):

- **Notice:** individuals must be informed about the processing of their personal data;
- **Choice:** individuals must be able to choose whether and how their personal data are used;
- **Onward transfer:** individuals must be able to choose whether and how their data are transferred to third parties;
- **Security:** reasonable steps must be taken to protect data and ensure they are only used for the intended purpose;
- **Data integrity:** data must be accurate, complete and up to date;
- **Access:** individuals have the right to access their data and to amend or delete inaccurate information (unless the cost would be disproportionate);
- **Enforcement:** mechanisms should be in place to ensure compliance with the principles.

Under Safe Harbor, federal enforcement was provided indirectly – via companies' self-declarations of compliance with the principles. These declarations could be enforced by the FTC because of its jurisdiction over 'unfair or deceptive acts or practices' (Reidenberg 2001). Safe Harbor was contentious from the outset, and it was approved despite a (non-binding) vote against it in the European Parliament (Salbu 2002). Concerns became particularly acute in the wake of 9/11, when the US government began requiring access to greater amounts of private-sector data for counter-terrorism purposes (Birnhack 2008). Safe Harbor weathered these storms in the first half of the 2000s, but the trigger for its collapse

a decade later was for similar reasons, namely concerns about US data breaches in the wake of the Snowden revelations.

1.1.3.3. Other developments

It is worth noting that while this second phase of data protection global governance was dominated by the EU and US, there were also a number of initiatives that marked the involvement of a growing number of actors in this domain. For example, at a regional level 2005 saw the 21-member Asia-Pacific Economic Cooperation (APEC) produced a regional privacy framework including nine data protection principles and seeking, like most of the Phase 2 initiatives we have discussed to balance the protection of privacy and the free flow of data. However, Birnhack (2008) notes that the APEC framework had little impact outside the APEC membership. In 2011, the International Organization for Standardization published an international standard for privacy principles (ISO 29100), which contained 11 privacy principles, all of which are familiar in light of the various frameworks we have been discussing (Wright and Raab 2014). And in 2012, an action plan was published by the Global Privacy Enforcement Network (GPEN), a network of privacy enforcement authorities that had been established on the basis of an OECD recommendation that there should be greater international coordination in this area (OECD 2007).

1.1.4. Phase 3: 2013 to 2020

The period since 2013 has been exceptionally significant for the evolution of data protection global governance. As in previous phases, this is partly a reflection of trends in technology and society. The exponential rise of social media and connected devices has led to an explosion of personal data, and therefore of data protection challenges. Similarly, the nature of the data ecosystem has changed. In earlier phases of regulatory activity, data flows were assumed to be relatively simple: transfers from one point to another. In the era of cloud computing, the locations where data are stored, processed, accessed and used are much more dispersed. The US and China have been at the technological vanguard during this period, but the EU has remained at the heart of the global governance discussion, building on the influence of the 1995 Directive in the 2016 General Data Protection Regulation (GDPR) which consolidated the extraterritorial scope of the EU's data protection regime. The influence that the GDPR enjoys has been reinforced by a succession of crises that have highlighted the increasing risks associated with personal data breaches. An example in the private sector is the Cambridge Analytica scandal, which took place around the time that the GDPR was coming into force. In the public sector, the Snowden revelations upended the Safe Harbor programme; uncertainty still persists over the legal basis of hugely significant EU-US data flows.

1.1.4.1. From Safe Harbor to Privacy Shield

The most significant development in the latest phase of the evolution of data protection global governance was the agreement of the GDPR in 2016. However, this was preceded by a collapse in the EU-US data governance arrangement which highlights important elements in the changing governance landscape. The trigger for the collapse was Edward Snowden's leaking of information about the extent

of global surveillance by the US National Security Authority (Landau 2013; Kalyanpur and Newman 2019). The chain of events that this led to demonstrates the increasingly complex network of actors and cross-border interventions that were now characterising the governance landscape for EU data protection: an Austrian citizen lodged a complaint with the data protection authority in Ireland questioning the legality of data transfers being carried out by a US-based company (Facebook), leading to a judgment by the CJEU that the entire Safe Harbor programme was invalid.

The specific complaint in the so-called *Schrems I* case (named for the complainant, Maximilian Schrems) was that in light of the Snowden revelations, Facebook could not guarantee the protection of personal data being transferred from the EU to the US because it was now clear that US security authorities were intercepting them (Lam 2017). The complaint was lodged with the Irish Data Protection Commission (IDPC) because that was where Facebook's EU servers were located. The IDPC rejected Schrems's complaint, on the basis that Facebook was a participant in Safe Harbor, which had been deemed adequate by the Commission. Schrems appealed this decision to the Irish High Court, which in turn referred the matter up to the CJEU, which used the opportunity to assess the overall validity of Safe Harbor. Its judgment turned on the interpretation of the adequacy requirement in Article 25 of the 1995 Directive. It took an expansive view, interpreting adequacy to mean a level of protection is 'essentially equivalent' to the protection guaranteed within the EU (Drechsler 2019).

The CJEU's decision that Safe Harbor was invalid marked an important shift in the underlying governance philosophy that shaped data protection in Europe. As we have seen repeatedly, and following the lead taken by the OECD and CoE, the EU sought to balance fundamental rights and economic growth in its approach to cross-border data flows. The CJEU decision came down more firmly on the side of fundamental rights, insisting that EU levels of protection be in place in third countries.

The *Schrems I* verdict in October 2015 affected around 4 500 US companies using it as the basis for their data transfers with the EU. This triggered emergency negotiations to find a legal framework to replace Safe Harbor. The result was the Privacy Shield, which was agreed in February 2016 and deemed adequate by the Commission in July 2016. The new programme included four core principles (Schwartz and Peifer 2017):

- **Data Integrity and Purpose Limitation Principle.** In particular, the Privacy Shield included an 'express prohibition on incompatible processing'. It also added new safeguards protecting EU personal data from US government access.
- **Choice.** Here the Privacy Shield moves closer than Safe Harbor to requiring the same protections as prevail within the EU.
- **Enforcement.** This was the area where the Privacy Shield moved furthest in terms of requiring additional protections on the US side, with multiple mechanisms stipulated, including:
    - the ability of EU data subjects to complain with US companies using Privacy Shield, or with their own national data protection authorities
    - the availability of alternative dispute resolution (ADR) mechanisms

- the establishment of an arbitration mechanism (the Privacy Shield Panel) with the power to make binding decisions against US companies
- the establishment of an independent US Ombudsperson

- **Oversight.** The Privacy Shield is subject to an annual joint review by EU and US officials, and enforcement proceedings are overseen by the FTC and the Department of Commerce.

1.1.4.2. The General Data Protection Regulation

While the adequacy of the Privacy Shield programme was being assessed by the Commission, in April 2016, the EU adopted the GDPR, the successor to the 1995 Directive and another milestone in the evolution of data protection global governance. The EU governance implications of the GDPR – notably its directly binding impact across Member States – are discussed later in this report. Here we focus on its impact on wider patterns of global governance. One of these is general: the GDPR consolidates the EU's position at the centre of the global governance landscape. Not in the sense that EU rules or norms prevail across the globe, but that those rules and norms are an unavoidable part of the debate about governance. Increasingly, other countries' approaches are understood and evaluated relative to the EU benchmark, a sign of significant soft power.

There are some substantive data protection changes in the GDPR, such as an expansion of the definition of personal data to include genetic data, GPS data and pseudonymous data (Houser and Voss 2018). In addition, new financial enforcement mechanisms were introduced, with fines of up to 4 % of companies' global revenues or USD 20 million, whichever is higher (Article 83). For our purposes, however, and the direct impact of the GDPR on the global governance landscape, the main provisions in the GDPR relate to adequacy and extraterritoriality.

The basic adequacy framework (Article 45) remains broadly aligned with that contained in the 1995 Directive. The GDPR still refers to the need for 'an adequate level of protection'. However, Recital 104 now clarifies that 'adequate' is to be understood in light of the 'essentially equivalent' meaning laid down by the CJEU in *Schrems I*. Article 45 specifies that an adequacy decision need not relate to an entire country, but can also be sought by 'a territory or one or more specified sectors' within a third country. It also lists a number of factors that the Commission must take into account when assessing adequacy, including the rule of law, respect for human rights, the relevant legal context (including defence, criminal and national security law), independent supervision and commitments to international data protection instruments. As with the 1995 Directive, there are other avenues that data controllers can use to justify transfers in the absence of an adequacy decision.

On extraterritoriality, the GDPR is clearer than the 1995 Directive was on the circumstances in which its provisions have force beyond the borders of the EU (Houser and Voss 2018). Article 3 addresses this point directly.

- Article 3(1) stipulates that the GDPR applies to all data controllers in the EU, even if they conduct their data processing elsewhere: 'This Regulation applies to the processing of personal data in

the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.'

- Article 3(2) stipulates that the GDPR also applies to data controllers outside the EU when they process the personal data of individuals in the EU for certain purposes: 'This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.'

The combination of the GDPR's adequacy and extraterritorial provisions puts in place a powerful set of de facto and de jure mechanisms through which the EU's data protection framework now exerts influence on actors across the global governance landscape[1]. Influence at the country level is achieved formally through the adequacy principle and informally through the GDPR's de facto role as a global benchmark for data protection best practice. In practice, the annual reviews of the new national and international data protection instruments that have been introduced conducted by Greenleaf (2019a; 2019b) highlight the strong de facto influence that the EU framework exerts on the evolving global system. This is discussed further in the next subsection. As for formal influence via the adequacy principle, the 12 adequacy decisions under the 1995 Directive remain valid until they are replaced (Drechsler 2019). The Commission has made one adequacy declaration since the GDPR came into force, relating to Japan (Schwartz 2019). Negotiations with South Korea are ongoing.

In terms of influence over private sector actors, as we have seen the GDPR explicitly applies to many companies operating or based overseas. A more informal source of influence on private sector actors is via the so-called Brussels effect, which refers to the incentives that large companies have to align their operations around a single set of rules rather than to manage multiple fragmented systems across their operations. As Anu Bradford, who coined the phrase, puts it: '[M]ultinational corporations often have an incentive to standardize their production globally and adhere to a single rule. This converts the EU rule into a global rule' (Bradford 2012). A good example of the Brussels effect in practice is Microsoft, which in the week the GDPR took effect announced that it would apply its core provisions globally: 'As an EU regulation, GDPR creates important new rights specifically for individuals in the European Union. But we believe GDPR establishes important principles that are relevant globally. That's why today we are announcing that we will extend the rights that are at the heart of GDPR to all of our consumer customers worldwide' (Brill 2018).

[1] For a useful discussion of changing patterns of cross-border regulatory influence, see Chander, Kaminski, and McGeveran (2019).

1.1.4.3. Data protection proliferation

Although milestones such as the 1995 Directive and the GDPR stand out particularly prominently, one of the clearest indicators of the evolution of data protection global governance has been the increase in the number of countries with data protection laws in place. We saw earlier that the first such law was enacted in Sweden in 1973. By 2011, 76 countries had data protection laws in place, an average increase of around two per year in the intervening four decades. Between 2011 and 2019 the number of countries with laws in place increased by 56 to 132, an average increase of 7 per year (Greenleaf 2019a).

Many of the newest laws to be adopted have been modelled on or at least strongly influenced by the GDPR (Greenleaf 2021; Schünemann and Windwehr 2020). Examples include Brazil, which adopted a new national law in 2018 (Perrone and Strassburger 2018), and Kenya where the Data Protection Act was signed into law in November 2018 (Monyango 2019). However, the spread of data protection laws around the world is not simply a story of the EU approach being replicated. This is particularly true of the US and China, the other two giants in the landscape of data processing and protection, to which we will turn presently. But it can also be true elsewhere and India provides a useful example. Although the country's data protection law has yet to be enacted, its difficult evolution points to the fact that for all its global weight, the GDPR's strong data protection principles still have to compete with other governance priorities. The entry into force of the GDPR has coincided with a tumultuous era in international relations in which multilateralism has been weakened and a growing number of countries have sought to re-emphasise the importance of nationalism, sovereignty and strong central leadership. These governing traits do not necessarily sit easily alongside the protection of fundamental rights embodied in the GDPR.

In July 2018, India published a draft data protection bill, in response to an instruction from the Supreme Court (Determann and Gupta 2018). The bill was drafted by a commission headed by a retired Supreme Court judge, BN Srikrishna, and comprising six representatives of government and three representatives of industry. The bill closely followed the GDPR in important respects. However, a process of consultation and amendment within government followed, and by the time the bill was finally placed before parliament in December 2019, Mr Srikrishna was quoted as saying that its removal of judicial oversight for government access to citizens' personal data could 'turn India into an Orwellian state' (Mandavia 2019). Greenleaf (Greenleaf 2020) acknowledges that the freedom granted to the government by the bill represents a 'major exception' to its scope, and he also notes that provisions relating to the processing of foreign nationals' data would be an obstacle in adequacy discussions with the EU. But he argues that the bill remains broadly in line with the GDPR in key areas such as extraterritorial application, the creation of a powerful data protection authority, and the need for a lawful basis for all data processing.

The US remains a data protection outlier, with no national omnibus data protection framework in place. Data protection rules remain structured in line with the sectoral pattern we noted in relation to the 1970s, when data protection rules were first being codified globally. Sectors such as healthcare and financial services have their own laws, which are enforced by their own regulators. Arguably, this sectoral

approach to data protection is as important a feature of US data protection governance as the contrast mentioned above between the priority on fundamental rights in the EU and on consumer interests in the US (Schwartz 2019).

The absence of an omnibus data protection law at the federal level should not obscure the great amount of activity that has been under way in the US over recent years. As Chander et al (2019) note, multiple such federal proposals have been proposed in Congress. At least as significant is the fact that within a 12-month period 'nearly half of state legislatures have proposed or enacted broad privacy bills or have established privacy legislation task forces.' There is perhaps an echo here of developments in Hesse in 1970, where subnational legislative developments signalled the direction of travel that larger legislatures would soon follow. In the US, the most prominent state-level data protection initiative is the California Consumer Privacy Act (CCPA), which was agreed in June 2018 (a month after the GDPR took effect) and which entered into force in early 2020. An interesting debate has emerged about the relationship between the CCPA and the GDPR, which may have a significant bearing on the future of data protection global governance. For Schwartz (2019), the CCPA reflects 'the global success of EU data protection'. If this is true, then it becomes relatively easy to plot the development of an increasingly EU-aligned global governance landscape, with the US converging on EU norms and instruments and with China as the major outlier. However, Chander et al. (2019) reject this narrative. They see the CCPA as embodying 'a fundamentally different regime for data privacy' and point to five key substantive differences:

- The CCPA remains rooted in the American tradition: it treats data protection as a matter of consumer protection rather than fundamental rights.
- The CCPA covers a much narrower range of entities – businesses only, and only those meeting a number of criteria – than the GDPR
- There is no private right to initiate enforcement action under the CCPA, whereas the GDPR allows for this
- The CCPA creates limited but detailed requirements, whereas the GDPR issues broad standards and relies on various layers of guidance to flesh them out
- The GDPR is strengthened by the weight given to privacy and data protection in the treaties and by the CJEU, whereas the CCPA is constrained by 'increasingly deregulatory First Amendment doctrine'

Chander et al. suggest that ongoing governance developments at both state and federal level in the US owe more to this CCPA regime than to the GDPR. They conclude that far from being a reflection of a 'Brussels effect' that extends the EU's influence in the US, the CCPA embodies a distinct 'California effect' that is catalysing data protection law in the US and that could plausibly rival the EU's dominance in global data protection governance.

In China, the third of the technology superpowers, a very different culture of individual rights prevails, including in relation to privacy. The country's authoritarian one-party government makes extensive use of mass digital surveillance, in tandem with key actors in the private sector. Over the past 10 years, the country has put in place a series of measures that share many features with data protection regimes of

the sort we have discussed throughout this section. However, the practical weight of these measures needs to be considered against the backdrop of the wider rule of law and respect for fundamental rights.

The most important data protection measure introduced in China has been the Cybersecurity Law adopted in 2016 and enforced in 2017. Greenleaf and Livingston (Greenleaf and Livingston 2016) describe it as 'China's most comprehensive and broadly applicable set of data privacy principles to date'. They note that the law covers most (and perhaps all) of the private sector and strengthens protections in areas such as data correction rights, deletion, re-use and disclosure, breach notification to users and data localisation. But they also point to significant absences in comparison with typical data protection laws elsewhere. Of particular importance is the absence of user access rights, which Greenleaf and Livingston argue elsewhere (2017) means that China's data protection framework is missing one of the most fundamental elements. Other data protection gaps in the Cybersecurity Law include the absence of a data protection authority, requirements on data quality and special treatment for sensitive data.

Personal information is defined in the Cybersecurity Law in familiar terms of identifiability. It includes 'all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including, but not limited to, natural persons' full names, birth dates, identification numbers, personal biometric information, addresses, telephone numbers, and so forth' (Greenleaf and Livingston 2016). The principles that apply to this personal data are summarised in Article 41: 'Network operators collecting and using personal information shall abide by the principles of legality, propriety and necessity; make public rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtaining the consent of the person whose data is gathered.'

The Cybersecurity Law presupposes a policy of data localisation. It is explicitly stated that all data produced by 'critical information infrastructure' (CII) must be stored locally, unless export outside China is 'truly necessary'. CII is defined broadly as 'public communication and information services, power, traffic, water, finance, public service, e-governance [as well as] other critical information infrastructure that if it is destroyed, loses its ability to function or encounters data leaks, might seriously endanger national security, national welfare and the people's livelihood, or the public interest' (Greenleaf and Livingston 2016). Although this prohibition on data exports is not explicitly applied outside the CII category, other network operators are 'encouraged' to 'voluntarily participate'. In late 2017, China also introduced a recommended standard – 'Information Security Techniques - Personal Information Security Specification' – which aims to provide greater clarity on how privacy-related laws will be applied across both the private and public sectors. Greenleaf and Livingston (2017) describe this as an important step in the evolution of data protections in China.

1.1.4.4. Other developments

The third phase of global governance evolution also saw both the OECD and Council of Europe revisit the influential principles they had established in the early 1980s. The OECD's revised guidelines were

published in 2013 (OECD 2013). The basic principles remain unchanged, but they are elaborated upon differently in light of the profound changes in the data ecosystem and economy in the intervening decades. Four changes stand out:

- The **accountability** principle is expanded and has a section of its own in the new guidelines, reflecting the need for greater implementation of accountability within businesses (Kuschewsky 2014).
- Notification of **data breaches** becomes mandatory, reflecting the increasingly intertwined relationship between privacy issues and other concerns such as criminality and cybersecurity.
- On **cross-border data flows**, the revised guidelines emphasise the accountability of data controllers 'without regard to the location of the data'. They also follow the 1995 Directive in referring to risk as an important factor in weighing whether or how to transfer data to a third country.
- The revised guidelines also point to the importance of **non-regulatory elements** of the data protection ecosystem, such as privacy professionals and privacy-enhancing technologies.

The revised CoE Convention (designated Convention 108+) was yet another piece of data protection to be concluded in 2018. The protocol amending the convention was adopted in May 2018 and opened for signatures the following month. It is not expected to take effect before 2023. Greenleaf (Greenleaf 2018c) notes that Convention 108+ is closely modelled on the GDPR, incorporating its key innovations, albeit 'in less prescriptive form'. This leads him to suggest that 108+ may become a de facto global standard for data protection, because it captures the key elements of the EU's gold standard, while differing significantly from the EU in allowing third-country ratification. This process of CoE internationalisation is already evident with the original Convention 108, which continues to attract new ratifications. There are currently 55 in total: 47 European (which compares with the 27 Member States in the EU) and an additional eight outside Europe: Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay.

1.2. EU governance

In this section, we focus on the development of data-protection governance in the EU. To do this, we return to consider in greater detail two of the milestones discussed in the previous section: the 1995 Directive and the GDPR. As well as being crucial features of the global landscape, these instruments also represent the two key inflection points for data protection governance within the EU, when circumstances aligned to produce a significant shift in the bloc's data protection governance regime. Rather than rehearse the previous section's discussion of the main provisions of the directive and the GDPR, this section will focus on the dynamics between the various governance actors in this field, and in particular the EU institutions, the Member States, and the increasingly influential network of national data protection authorities. More specifically, we will consider three aspects of the directive and the GDPR: first, the background conditions that allowed or required these regulatory instruments to be introduced; second, the intra-EU dynamics during the two negotiation processes; and third, the concrete

results in terms of key features of the EU governance landscape. In the broadest terms, the story of EU data protection governance is one of gradual harmonisation, constitutionalisation and agencification at the EU level, albeit with a number of carve-outs being maintained at the national level. Our mapping of intra-EU dynamics in this section will prepare us for the discussion of EU actorness in the next chapter, particularly in relation to the authority, autonomy and cohesion dimensions.

1.2.1. A timeline of EU governance

Table 2 - Timeline of EU governance

MILESTONE 1: THE 1995 DIRECTIVE	1981	European Commission recommends that MSs ratify CoE Convention 108, raising the prospect of proposing an EU instrument if they fail to
	1983	German federal court decision on census data, with emphasis on connection between data protection and individual liberties
	1987	Council of Europe Recommendation R(87)15 on the use of personal data in the police sector
	1990	European Commission publishes its draft proposal for a Data Protection Directive
	1992	Revised draft of the directive
	1992	Maastricht Treaty
	1993	Single Market
	1993	European Commission publishes a white paper, on 'Growth, competitiveness and employment – the challenges and ways forward into the 21st century'
	1995	Adoption of the Data Protection Directive
	1998	The 1995 Directive enters into force
	2001	Regulation (EC No 45/2001) on data processing by EU institutions
	2002	Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector
	2003	Special Eurobarometer 196 on Data Protection
	2006	Data Retention Directive
MILESTONE 2: GDPR	2009	Lisbon Treaty comes into force, establishing data protection as a fundamental right and giving legal force to EU CFR
	2009	Amendment of 2002 directive
	2009	European Commission consultation on data protection (167 replies)

	2010	European Commission Communication: 'A comprehensive approach on personal data protection in the European Union'
	2011	European Commission consultation on data protection (288 replies)
	2011	Special Eurobarometer 359 on data protection and electronic identity
	2012	European Commission publishes GDPR draft proposal
	2013	European Commission Regulation 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC
	2014	Amended text of GDPR passed by European Parliament
	2014	Data Retention Directive ruled invalid
	2014	CJEU rules on right to be forgotten
	2015	European Council publishes its amended version of GDPR
	2015	EDPS commentary on GDPR
	2015	Special Eurobarometer 431 on data protection
	2016	Final text of GDPR adopted
	2016	Also adopted: Directive on data protection and law enforcement
	2017	European Commission proposes new regulations on ePrivacy and on data protection rules applicable to EU institutions
	2018	GDPR enters into force
AFTER GDPR	2018	Commission launches proceedings against 19 Member States for delays on 2016 directive transposition into national law
	2019	Schrems II hearing and advocate general opinion (supports SCCs)
	2019	Commission Communication 'Data protection rules as a trust-enabler in the EU and beyond – taking stock' (European Commission 2019)
	2019	City of Hamburg (Germany) Commissioner for Data Protection and Freedom of Information opens urgency procedure re Google Assistant
	2019	Special Eurobarometer 487a on General Data Protection Regulation
	2019	First large GDPR fine: French Data Protection Authority fined Google EUR 50 million for lack of transparency and valid consent surrounding use of data for ads personalisation
	2020	GDPR review

Source: Compiled by the authors.

1.2.2. Milestone 1: The 1995 Directive

1.2.2.1. Backdrop

What were the background conditions that led to the introduction of the 1995 Directive? In 1981, the European Commission recommended that Member States ratify the CoE Data Protection Convention. Repeatedly during the 1980s, it adopted a stance of 'passive resistance' to European Parliament calls

for EU-wide regulatory action (Simitis 1995). Yet by 1990, the Commission had published a draft directive (Schünemann and Windwehr 2020). What changed during this period that so fundamentally altered the Commission's stance on data protection? There are three main answers, relating to economic, political and institutional developments in the EU.

The 1980s were a pivotal decade for European economic integration, with the Single European Act (which took effect in 1987) promising an integrated market across the bloc by the start of 1993. The economic rationale for greater harmonisation of data protection laws is reflected in the fact that the first words of the directive root it in Article 100 of the Treaty Establishing the European Community, which relates to the steps needed to create the single market. One of the key roles of the Commission has always been to promote economic activity and integration. During the early 1980s, this led to its reticence about data protection regulations: the Commission wanted to support the development of economically significant new information technologies and saw data protection as a 'threat to the promotion of computer-based processing' (Simitis 1995). However, this zero-sum understanding of the relationship between data flows and data protection became less tenable as the 1980s proceeded. Data flows became increasingly important to economic activity at the same time as there was a major push to deliver increasing levels of cross-border economic activity in the EU. This led to a marked shift in the attitude of the Commission. Consistent data protection rules across the EU were now seen as necessary to enable free flows of information which in turn were viewed as vital to the completion of the single market (Pearce and Platten 1998). This reflects, at an EU level, the thinking that underpinned the OECD guidelines and the CoE Convention: data would not flow smoothly across borders if data protection standards differed.

Greater impetus was given to this approach to data protection during the negotiation period with the publication of a European Commission white paper on the economic challenges of the 21st century. It explicitly discussed the single market in relation to the growing importance of the information economy (Pearce and Platten 1998). This white paper led the European Council to mandate a high-level group (the Bangemann Group) on Europe's information infrastructure. This group reported in 1994 and highlighted the importance of robust data protection in order to ensure consumer trust in in the emerging 'information society' (Pearce and Platten 1998). On foot of this report, the European Council called for a swift resolution of negotiations on the data protection directive.

A second enabling factor for the 1995 Directive was political. The evolution of the EU in the 1980s and 1990s was political as well economic. As well as moving towards a single market and monetary union, the EU was also beginning to enshrine fundamental rights in its constitutional documents. The Maastricht Treaty introduced EU citizenship and stressed the EU's commitment to fundamental rights and the principles of democracy. But even in 1990, when publishing its draft proposal for a directive, the Commission stressed that fundamental rights were a core motivation, pointing back to this passage in the preamble of the Single European Act: 'DETERMINED to work together to promote democracy on the basis of the fundamental rights recognised in the constitutions and laws of the Member States, in

the Convention for the Protection of Human Rights and Fundamental Freedoms and the European Social Charter, notably freedom, equality and social justice.' For Simitis, this increasingly political character of the EU is what explains the shift in the Commission's attitude to data protection during the 1980s: 'the clearer the Member States emphasized the fundamental rights, the less the Commission could hold to its initial position. Instead, the Commission had to align itself with the view that any discussion about the processing of personal data is at the same time a debate on the essentials of a democratic society' (Simitis 1995).

A third factor that helps to explain the agreement of the 1995 Directive relates to the institutional consequences of the regulation that was taking place at the national level during the 1970s and 1980s. In particular, the establishment of independent data protection authorities (DPAs) created a new locus of regulatory influence in this field. The first European DPA to be created was in Sweden in 1976. By 1988 there were 11. Seven of these 11 were inside the EU; the remaining five Member States did not have a data protection law or a DPA in place: Belgium, Greece, Italy, Portugal and Spain (Newman 2008). This division within the EU between two groups of states with and without DPAs created an opportunity for regulatory leverage. In 1989 a meeting of DPAs resolved that progress towards the single market would require guarantees of data protection across the bloc. In July of that year, CNIL, the French DPA, threatened to block data transfers between the French and Italian offices of the carmaker Fiat, because of the absence of adequate data protection in the latter. For Newman, this positions the seven DPAs within the EU as the key governance actors ahead of the negotiation of the 1995 Directive:

> 'Fearing that market integration would threaten levels of protection across Europe and undermine their regulatory authority, national data privacy authorities created by earlier domestic legislation pushed for Pan-European rules. Collaborating with their peers, they employed extensive expertise to define a supranational agenda. Using domestically delegated power to ban the transfer of cross-border data flows, they blocked data transmissions to Member States with no or lax legislation. National data privacy agencies leveraged authority granted to them nationally to change the cost-benefit analysis of supranational policymakers' (Newman 2008)

Newman notes that other key actors were either silent (Member States) or hostile (industry) on the idea of EU-wide data protection rules[2]. This highlights important aspects of multi-level governance in the EU. Powers delegated to national actors can end up exerting significant supranational force because of the capacity of obstructions at the national level to hinder the smooth operation of the larger system. So even though they may have been created primarily as part of national data protection frameworks, the DPAs were able to function as 'de facto veto players' (Newman 2008).

[2] On hostility from business, see also Peace and Platten: 'Among the business community there was also growing unease about the potential financial and administrative costs of implementing the proposed directive. The major banks, insurance companies, travel agencies and credit reference agencies, all of which rely on the extensive use of personal data, were opposed to the proposed directive.'

1.2.2.2. Process and outcome

There were three main stages in the negotiation of the 1995 Directive. The Commission published its initial proposal in September 1990, at which time the intention was for the directive to take effect at the start of 1993 (Greenleaf 1995). In practice, the process took twice as long. By October 1992, the Commission published a revised draft of the directive, taking on board the views of the European Parliament, a working group of the Council of Ministers, the national DPAs and industry. This then led to 30 months of difficult negotiation between the members states, conducted in the working group mentioned above. A 'common position' was finally agreed at the Council of Ministers in February 1995 (albeit with the UK abstaining), and this version was adopted in July following minor final amendments by the Parliament.

Once the process had been initiated by the Commission, the Member States were the key actors in determining the shape of the final directive. According to Bendrath (2007): 'The ministers negotiated behind closed doors, and the citizens and parliamentarians only found out about the outcome later. The European Parliament, in particular, had no real impact on the 1995 Directive. It was mainly shaped by the struggle among influential governments in the European Council.' The initial Commission draft was strongly influenced by the approach to data protection in Germany (Pearce and Platten 1998). Subsequent changes were in large measure driven by Member States' efforts to ensure that the final directive incorporated elements from a wider range of national frameworks. As Simitis notes, Member States wanted a directive that was broadly in line with the provisions they already had in place: the challenge for the Commission was not to create innovative new data protection rules, it was to combine existing rules in a way that would keep Member States happy (Simitis 1995). This explains why Denmark, Ireland and the UK were the most reluctant among the Member States to sign up to the directive, because of the wider gap between their existing national regulatory approach and the new EU-wide proposals. However, it would be a mistake to think of each Member State as a monolithic actor in relation to the directive. Debates were also ongoing within countries. In the Netherlands, for example, 'reactions to the 1992 text ranged from outright hostility to cautious enthusiasm' (Pearce and Platten 1998). In the end, the report from the Bangemann Group on the role of data protection in opening a European 'information space' was a key development in terms of breaking the impasse among the Member States.

Although the process of national bargaining over the directive created a risk of a 'race to the bottom' in order to find a solution acceptable to all, the core provisions were not affected (Simitis 1995). The 1995 Directive enshrines substantive principles of data protection that are familiar from the OECD guidelines and the CoE Convention discussed in the previous chapter/section. Greenleaf (1995) highlights seven noteworthy aspects of the substantive principles of data protection in the directive:

- Data quality requirements, such as the need to ensure that data are accurate, up to date and not retained for longer than is needed
- A set of six lawful criteria that permit the processing of personal data

- The ‘finality principle’, which means that use and disclosure of personal information are limited to the original purposes for which the data were collected
- The requirement for data controllers to put appropriate security safeguards in place
- A system of notification, with exemptions for data processing operations that are unlikely to affect individuals’ rights or where an independent data protection officer is in place
- Special categories of personal information, notably sensitive data relating to factors such as health, ethnicity or political beliefs.
- Additional rights, including the right to be informed as to the purposes of data processing, and to obtain a copy of information held about oneself.

In terms of the governance architecture created by the directive, there are eight key points to note. The first is that as a directive rather than a regulation, the 1995 text had to be transposed into national law in each of the Member States, rather than being applied directly. This created scope for continuing variation in the way in which the principles are applied. Member States were given 3 years to implement the directive (with some exceptions, such as a 12-year transition for dealing with manual as opposed to computer data).

Second, the role of the Commission fell short of what it had initially hoped for, reflecting the driving role played by the Member States. The directive tasks the Commission with monitoring the implementation of the directive, but not with additional rulemaking powers. The Commission had sought such powers for itself in Article 33 of its 1992 (revised) draft, but this was removed during negotiations between the Member States in the Council of Ministers (Greenleaf 1995). As discussed in the previous chapter/section, another key role that the directive gives to the Commission is in assessing whether third country data protection frameworks meet the adequacy threshold required for Article 25 data transfers.

Third, the directive was potentially extraterritorial in scope. Article 4(1)(c) stipulates that a Member State must apply their data protection laws to data controllers based outside the EU if the controller is processing data using equipment that is located in the Member State (with an exception if the data is only in transit through the EU).

Fourth, the directive consolidated the network of DPAs discussed above. All Member States were now required to have an independent DPA, with a range of powers of investigation and intervention (Article 28). Moreover, Article 29 establishes a working party (hereafter WP29) composed of representatives of the Member States’ DPAs, a representative of the European Commission, and a representative of the authority responsible for data protection in the EU institutions. WP29 was given an important advisory role in the new data protection governance landscape, notably in relation to (i) consistency across the EU, (ii) assessments of the adequacy of third-country data protection rules, and (iii) assessments of sectoral codes of conduct. WP29 was required to publish an annual report on data protection in the EU and in third countries, while the Commission was required to publish an annual report detailing its

responses to WP29 recommendations. This new range of powers enjoyed by Europe's DPAs lends weight to Newman's view that they are crucial to understanding the genesis of the directive.

Fifth, the directive also establishes (Article 31) a committee comprising representatives of each Member State and chaired by a representative of the Commission. A key role of this committee is to take a final decision on proposals from the Commission on whether a third country meets the adequacy threshold for Article 25 data transfers, or whether the other justifications for data transfers listed in Article 26 apply.

Sixth, the directive introduces an element of risk-based regulation, by establishing (in Article 20) a system of 'prior checking' for data processing operations that can be expected to 'present specific risks to the rights and freedoms of data subjects'. This is a precursor to the data protection impact assessments (DPIAs) introduced in the GDPR.

Seventh, enforcement of the data protection rules derived from the directive remain at the national level. Individuals must be given the right to take enforcement actions, but where breaches are shown to have occurred, the sanctions are determined nationally. In practice, this leaves significant scope for the directive to operate differently in different Member States, creating incentives for data processing activities to be re-located within the EU to countries seen as having implemented the directive less strictly, such as Ireland.

Eighth, the directive introduces a system of certification which, in effect, creates a hybrid system of 'regulated self-regulation' (Bendrath 2007). The basic idea is that companies or business associations would submit their national data protection codes of conduct to the DPA for an assessment as to whether they comply with national law. EU-wide codes of conduct would be submitted to WP29 instead. The directive actively encourages the use of codes of conduct as a way of strengthening the implementation of national data protection laws.

1.2.3. Milestone 2: GDPR

The second EU governance milestone that we consider is the General Data Protection Regulation (GDPR), which was adopted in 2016 and took effect in 2018. In this section, we will mirror the approach we took towards the 1995 Directive. In the first subsection, we consider the drivers that led to the introduction of the GDPR. In the second subsection, we look at the dynamics of the negotiation process and the key features of the resulting governance landscape.

1.2.3.1. Backdrop

A variety of factors combined to create the conditions that led the EU to adopt the GDPR. Some of these have been discussed in the previous chapter, and so we will not dwell on them at length again here. In essence, as time passed the governance framework enshrined across the EU by the 1995 Directive became less and less fit for purpose. This is because developments inside and outside the EU were calling for an increasingly robust approach to data protection, and because problems with the 1995

governance arrangements were becoming increasingly clear. We can distinguish three key drivers: (i) another period of treaty change in the EU, which further prioritised data protection, (ii) the advent of the internet era and its transformation of the societal and economic role of personal data, and (iii) the persistence of fragmentation and ineffectiveness after the 1995 Directive. Let us look at each in turn.

We noted above that the increasingly political character of the EU from the mid-1980s was one of the factors that contributed to the drafting of the 1995 Directive. By the 2000s, this process had continued apace, and this led to the rights dimension of the EU's data protection framework becoming increasingly predominant. In 2005, proposals to create a European Constitution were rejected by voters in France and the Netherlands, but two years later the adoption of the Lisbon Treaty implemented many of the changes that the proposed constitution had contained. In terms of data protection governance within the EU, the Lisbon Treaty (which took effect in 2009) was important for two reasons. First, it enshrined data protection as a fundamental right within the EU's quasi-constitutional order. Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) states that 'Everyone has the right to the protection of personal data concerning them'. Second, the Lisbon Treaty incorporates the Charter of Fundamental Rights of the European Union (CFREU) into EU law, giving it the same legal force as the treaties themselves. This provided further constitutional underpinning for data protection in the EU, as Article 8 of the CFREU includes the following provisions: '1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.' This strengthening of the EU's legal duties to protect citizens' personal data in the early 2000s coincided with huge changes in the economic and societal role of such data. As discussed in the previous chapter on global governance, widespread use of the internet and electronic commerce shaped new economic activities and trading patterns both within and between states. This in turn created an ongoing pressure to adapt and update EU governance arrangements to ensure that they remained fit for purpose given changing conditions. (As noted before, this is in contrast to the situation in the US where the emphasis on self-regulation meant private-sector actors had much greater latitude to shape the societal and economic impact of new digital technologies.) A series of other EU data-related laws were passed between the directive and the GDPR, including a regulation on data processing by EU institutions (2001) and directives on electronic communications (2002) and data retention (2006).

Just as variance in data protection rules across Member States was one of the factors that led to the adoption of the 1995 Directive, so the pressure for greater uniformity in a new regulation was a response to continued regulatory fragmentation across the EU after the directive came into force. Some of this was inherent in the provisions of the directive: Simitis (1995) notes that the directive's recitals acknowledge that 'disparities' will be inevitable. Moreover, in 1999, a year after the directive took effect, seven of the EU's then-15 Member States had not introduced implementing legislation as they were required to do (Fromholz 2000). A further four years on, a European Commission evaluation of data

protection in the EU highlighted numerous problems. It pointed to ‘reasons for serious concern’ and ‘very patchy compliance’ and noted that the ‘risks of getting caught seem low’ (Bendrath 2007).

A further factor that contributed to the introduction of a new EU-wide data protection governance instrument was the role of public opinion. The increasing ubiquity of personal data flows in everyday life with the advent of the internet, smartphones and social media meant that data protection was becoming a more prominent political rather than technocratic issue. As noted in the previous section, this was particularly true when scandals such as the Snowden revelations erupted. In the years following the 1995 Directive, the European Commission conducted three special Eurobarometer surveys of public sentiment in relation to data protection. Their findings included the following:

- In 2003, 68 % of respondents were unaware of the existence of DPAs, one of the key citizen-facing elements of the directive’s governance architecture.
- In 2011, 90 % of respondents said it was important for the same data protection standard to apply across the EU.
- In 2015, 89 % of respondents said it was important for the same standards to apply to businesses regardless of where the businesses are located.
- Also in 2015, 81 % of respondents said they did not feel they had complete control of their personal data, and 67 % of that group said they were concerned by this lack of control.

1.2.3.2. Process and outcome

The legislative process that led to the adoption of the GDPR was intense, particularly from 2013 when the Snowden revelations pushed data protection concerns up the global policy agenda (Jančiūtė 2018). Between 2009 and 2011, the European Commission held two consultations on data protection (Hilden 2019). It also published the Communication ‘A comprehensive approach on personal data protection in the European Union’. In 2012, the formal legislative process got underway with the tabling of the Commission’s draft proposal for a new regulation. The process that followed involved three main stages as the co-legislators, the Council and Parliament, moved towards an agreed text. The Parliament adopted an amended version of the regulation in March 2014, following a range of inputs from various committees and notably the Committee on Civil Liberties, Justice and Home Affairs (LIBE), which, significantly, was the lead committee on this file (Coyne 2019). The Council moved more slowly (parliamentary minds had been focused by the fact that there were elections in 2014) and agreed a compromise text in mid-2015. The Council’s deliberations were not smooth, with reports of a ‘crisis’ in late-2013, leading to speculation that the reform process would collapse (Jančiūtė 2018). However, once the Council had agreed its version of the text, the next stage of the legislative process moved much more quickly. The trilogue process, involving the Commission, Council and Parliament, was completed in December 2015, allowing the final text of the GDPR to be approved in April 2016.

Broadly speaking, the Parliament and Council had quite different goals during the negotiation process. The Commission’s initial draft had emphasised a by-now-familiar synthesis of fundamental rights and economic development. The Parliament leaned towards ensuring the protection of fundamental rights.

In part this reflected the long-standing position of MEPs on this issue; as noted before, the Parliament had first called for EU-wide data protection laws as early as the 1970s. It also reflected more fortuitous developments, such as the choice of rapporteur to manage the passage of the GDPR through the Parliament's institutional machinery. This was Jan Philipp Albrecht, a Green politician with the Parliament's strongest record of voting in favour of privacy protections. Originally it looked like the rapporteur might have been Axel Voss, from the EPP, who by contrast had the Parliament's strongest record of voting for measures that weakened privacy protections (Jančiūtė 2018).

If the Parliament sought to ensure that the GDPR delivered strong data protection across the EU, the Member States in the Council sought to ensure that their room for discretion at the national level was not unduly restricted. Eighteen months after the Commission had published its draft text in 2012, eight Member States still preferred to replace the 1995 Directive with another directive, rather than with a directly binding regulation. (It is worth noting that the Commission had already moved data protection issues related to law enforcement into a proposal for a separate directive rather than include them in the draft GDPR[3].) Although a regulation was ultimately agreed upon, Member State reticence about harmonisation persisted throughout the negotiation process, leading to a 'directivised' regulation with a 'staggering' number of flexibility clauses (Jančiūtė 2018). Although corporate lobbying was more intense in the Parliament than in the Council (Hilden 2019), a number of Member States took a business-friendly approach to the negotiations, notably including Ireland where many multinational technology companies located their EU operations. Ireland held the rotating Council presidency towards the beginning of the legislative process, and Jančiūtė (2018: 136) notes that: 'the version of the first four chapters of the GDPR elaborated by the Irish Presidency promoted a more self-regulatory, risk-based approach as opposed to the more prescriptive framework featuring in the Commission and EP versions. Such a self-regulatory approach was largely in line with the industry demands expressed in some statements'. The economic backdrop was dire during much of the negotiation period, so arguments premised on maximising economic activity had strong supporters in the Parliament as well as among the Member States.

The CJEU also played an important role during the negotiation process, albeit in the background, handing down several major rulings. These rulings clarified the significance of the Lisbon Treaty changes that had put the full weight of EU law behind the principle that data protection is a fundamental right of all EU citizens. In the last chapter we discussed the 2015 Schrems ruling, which invalidated the Safe Harbor programme. Before that ruling, in 2014, the CJEU had also invalidated the entire 2006 Data Retention Directive (Lynskey 2014). In the same year, it had also ruled that Google must remove certain search results when asked to do so in order to respect citizens' 'right to be forgotten' (Lindsay 2014). These judgments were a wake-up call for the negotiating institutions. So too was the fallout from the Snowden revelations, which increased the salience of data protection issues generally and which are widely seen as having impressed on Member States the political imperative to introduce more robust

[3] See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0010

data protection measures. The European Council made a number of calls for timely data protection reforms during 2013 and 2014, and 16 national parliaments made a joint call for speedy reform in September 2014 (Barbière 2014).

The WP29 group of DPA representatives made an important intervention during the final trilogue stage of the legislative process. This phase moved swiftly, but one point of contention related to the processing of data for purposes incompatible with the original purpose for which the data had been collected. The Council wanted such 'incompatible purposes' processing to be permitted if it fell under the 'legitimate interest' of the data controller. This prompted a warning from WP29 that the prohibition on incompatible purposes should not be weakened in this way, arguing that it would result in a lower level of data protection than the 1995 Directive provided (WP29 2015). Their warning was heeded.

We now turn to consider the outcomes of the negotiation process. As in the section on the 1995 Directive, we look both at the substantive principles of data protection enshrined in the GDPR and at the changes that it made to the EU's data-protection governance architecture. On the first of these, the GDPR follows the 1995 Directive closely, setting down the following six broad principles (Hoofnagle, van der Sloot, and Borgesius 2019):

- Lawfulness, fairness, and transparency: this is an overarching obligation to comply with applicable laws and to act in good faith.
- Purpose limitation: data should only be collected for specified purposes and not subsequently used for incompatible purposes.
- Data minimisation: personal data should be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.
- Accuracy: data controllers must take all reasonable steps to ensure that personal data are accurate and up to date.
- Storage limitation: personal data should only be kept for as long as necessary, and time limits for erasing data should be set at the outset.
- Integrity and confidentiality: appropriate safeguards are required against loss, destruction, damage and unlawful processing or personal data.

The GDPR also imposes a range of obligations on data controllers, relating to matters such as record-keeping, having a data protection policy and, for governmental organisations and larger private companies, a requirement to appoint a data protection officer. Another important requirement of the GDPR is that data users build data protection into their services by design and by default (Jasmontaite et al. 2018).

In terms of the governance mechanisms required by the GDPR, we highlight eight important novel features (Albrecht 2016; Kalyanpur and Newman 2019):

- The first is the evolution from enshrining data protection rules in a directive to enshrining them in a regulation. This means that the principles listed above are binding across the EU, without

the need for any implementing national legislation. However, as mentioned earlier, the GDPR incorporates significant exceptions that give the Member States greater discretion to set their own rules in specific areas. Most notably, there is a wholesale exemption from the GDPR for data processing related to national security and policing, which are covered in a separate directive. (There is also a wholesale exemption for personal and household activities.) In addition, the GDPR contains numerous smaller provisions for Member State discretion. Out of a total of 99 articles, 37 include some scope for Member State flexibility[4].

- Second, whereas the 1995 Directive was rooted primarily in treaty provisions related to the creation of the single market, the GDPR starts with the fact that data protection is now a fundamental right in the EU treaties. The role of data protection in facilitating economically valuable flows of data is a secondary consideration. This is likely to have continuing jurisprudential significance given the willingness of the CJEU to take dramatic steps when data protection rights are threatened. In this regard, it is worth noting that the preamble to the GDPR calls for a balanced approach: 'The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.'

- Third, as discussed in the previous chapter, the GDPR extends the extraterritorial reach of the EU's data protection framework, primarily by including in its remit third-country data controllers who are providing goods or services to individuals based in the EU.

- Fourth, the GDPR introduces much higher sanctions for breaches of the rules. Crucially, these sanctions are uniform across the EU, ending the situation under the 1995 Directive whereby Member States could set their own penalties. In Articles 77 and 78 The GDPR provides a route for individuals to take a case through their national DPA and national court system and up to the CJEU if necessary. (This is not new; it is the process that a case like Schrems 1 went through before the CJEU invalidated the Safe Harbor programme.) The GDPR also introduces a provision allowing NGOs to represent data subjects in taking complaints to the authorities (Article 80).

- Fifth, DPAs are increasingly pivotal to the governance of data protection under the GDPR. The WP29 group becomes the European Data Protection Board (EDPB) and is given binding decision-making powers to maintain regulatory consistency across a decentralised system of supervision led by the national DPAs. This system operates as a so-called one-stop shop, the idea being that a data controller operating across numerous Member States would only have to deal with one DPA. This was part of the Commission's draft text from the outset, because it offered greater legal clarity and lower business compliance costs. This proposal raised concerns

[4] See more at https://dpnetwork.org.uk/gdpr-derogations-list/

that it would lead to forum shopping by large companies seeking to be supervised by the least strict DPAs. Ireland's DPA was cited as a potential weak link in the chain of DPAs because it had relatively few resources but was the lead DPA for many of the world's largest data-processing businesses (Jančiūtė 2018). At one point Germany proposed a centralised system with a single EU-wide super-agency. However, in the end the GDPR introduced a backstop for the one-stop shop instead, allowing for legally binding interventions if a lead DPA is seen by its counterparts to be undermining the consistent implementation of the GDPR (Articles 63-65). The Commission had sought this role of enforcing the new 'consistency mechanism', but it was granted instead to the new EDPB.

- Sixth, the GDPR introduces data protection impact assessments (DPIAs). Article 35 states that a DPIA is required: 'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons'. It goes on to clarify three categories of risk: (i) the use of automated processing to carry out systematic and extensive evaluations that lead to legal (or similarly significant) effects, (ii) large-scale processing of special categories of data, and (iii) systematically monitoring a publicly accessible area on a large scale.

- Seventh, the GDPR requires that a Data Protection Officer (DPO) be appointed by all public bodies and by any private-sector entities that are either processing data on a large scale or processing sensitive data. The role of the DPO is to be an independent expert, monitoring and advising on the organisation's fulfilment of its data protection obligations.

- Finally, the Committee established by Article 31 of the 1995 Directive remains in place in the GDPR (now Article 93), with the same role of deciding on Commission proposals in areas such as the adequacy of third-country data protection frameworks.

1.2.3.3. After GDPR

The EU's activity in the area of data protection governance has continued since the adoption of the GDPR. The regulation consolidated the EU's position as a leading global actor in this domain, and as we have seen, the GDPR has been an important influence on the wave of data protection laws that other countries have drafted in the years since. As we will discuss in more detail in the later chapter on EU effectiveness, the goal of being a global leader on data protection has become increasingly important to the EU. This was evident in a review published by the Commission to mark two years since the adoption of the GDPR (European Commission 2020c). However, this increased focus on projecting EU rules and values globally should not detract from the work that still needs to be done to ensure the smooth and consistent application of the GDPR within the EU. Compliance levels remain relatively low, and despite the steady progression from directive to regulation, the Commission's two-year review highlighted continuing problems relating to fragmentation across Member States, notably in relation to cross-border cases. It is also worth noting that the EU continues to work on an ePrivacy Regulation,

which would establish new requirements – aligned with the GDPR – for electronic communications, including messaging apps, direct marketing, rules for cookies, etc (Bensinger, Kociok, and Zollitsch 2021). In February 2021, the Council adopted a version of the draft regulation, and this now forms the basis of negotiations between Council, Commission and Parliament before it is finalised[5].

More broadly, the EU has been developing a wider data strategy, which seeks to boost the scale of the EU data economy without weakening the principles embodied by the GDPR (European Commission 2020a). This objective is also reflected in initiatives such as GAIA-X, which seeks to implement data protection by design across Europe, using a network of data infrastructure suppliers all following a shared standard[6].

As well as being a tacit response to criticisms that the GDPR has hampered data-intensive innovation and growth in the EU, the Commission's new data strategy reflects the increasing geopolitical significance of digital technologies. It is an explicit goal of the von der Leyen Commission to achieve 'technological sovereignty', in which the EU's capability to make its own choices and follow its own values is not restricted by over-reliance on other global actors. This highlights the increasing real-world relevance of the TRIGGER model of actorness, and in the next chapter we consider how that model applies to the data protection case study.

2. EU actorness in the data protection domain

2.1. Introduction

This chapter of the data protection deep dive presents an analysis and scoring of each dimension of the EU's actorness in the data protection domain. The primary focus of the analysis is on current conditions (and levels). However, one of the objectives of these deep dives is to trace the evolution of EU actorness over time and so an attempt has been made to provide an overview of how the dimensions of actorness have changed. In the main sections below, a series of three levels of actorness is allocated to each dimension, corresponding to three phases in the evolution of the data-protection governance landscape in the EU. These are: (i) the period prior to the 1995 Data Protection Directive (DPD)[7], (ii) the period between the DPD and the adoption of the GDPR in 2016[8], and (iii) the current (i.e., post-GDPR) period.

[5] See more at https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

[6] See more at https://www.gaia-x.eu/

[7] See 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, *OJ* 1995 L281/31

[8] See 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) [2016] *OJ* L119/1.

Given the prominence of the EU in the global evolution of data protection rules and norms, it is perhaps surprising that there has not already been a wider discussion of EU actorness in this area. Mărcuț (2020) assesses the EU's actorness in digital policy more broadly, but her analysis only touches briefly on data protection issues. Moreover, it relies on a model of actorness that focuses on three of the seven dimensions used in the TRIGGER model (authority, autonomy and recognition).

The analysis in this chapter draws heavily on the discussion in the last chapter of how the global and EU governance of data protection has evolved since the 1980s. Additional evidence and data are marshalled in support of the scoring exercise, but there are methodological considerations that should be acknowledged at the outset. Three stand out in particular. The first of these is the unavailability or inaccessibility of robust quantitative data capturing the various dimensions of actorness. This means that the analysis is largely qualitative in character and the levels are a matter of judgement, which can (and should) be contested. Second, where data have been available, they have tended to favour recent years, making comparisons over time difficult within each of the dimensions. And third, similar difficulties apply to comparisons of actorness levels across the four deep dives, owing to significant variation in the availability of data (which in turn reflects the substantive differences between the topics of the four deep dives). This may affect the comparability of levels across the deep dives, although the authors of the respective deep dives have worked together to benchmark and calibrate their work.

2.2. Summary

The table below provides an overview of the evolution of each of the seven dimensions of actorness in each of the three phases of data protection governance. In line with the qualitative approach to assessing actorness, this overview uses colour-coding rather than a numerical score to illustrate changes in actorness over time. There are five levels in this scheme: low, low/moderate, moderate, moderate/high and high. The darker the blue, the stronger we assess the EU to be on a given dimension of actorness.

Phase	Pre-directive	Directive to GDPR	Post-GDPR
Period	1980-1994	1995-2015	2016-2020
Authority			
Autonomy			
Cohesion			
Recognition			
Attractiveness			

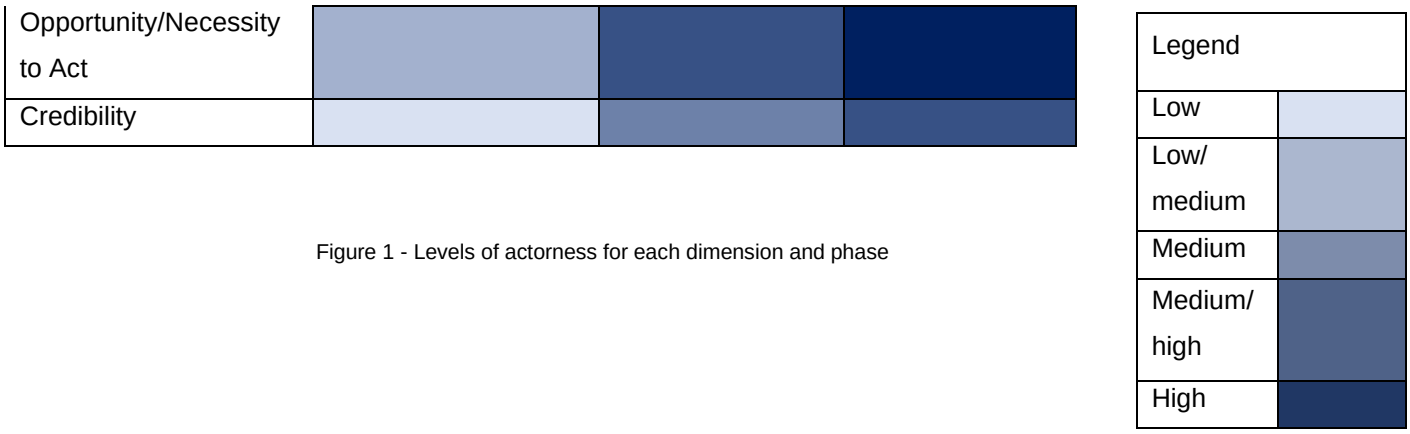


Figure 1 - Levels of actorness for each dimension and phase

While we are not combining the results of our analysis across the various dimensions to produce a composite measure of actorness, the results nevertheless point to a clear increase in the EU's actorness with respect to data protection. Across the seven dimensions, there is an average increase of almost three steps on our five-point scale between the first and third phases. The biggest change recorded on any of the dimensions is for recognition, which increases from 'low' in the first phase to 'high' in the latest phase. This contributes to a more general trend that sees greater increases on the three external dimensions (recognition, attractiveness and opportunity/necessity to act) compared to the three internal dimensions (authority, autonomy and cohesion). Assessing possible causal relationships between the various dimensions of actorness is beyond the scope of this report, but one possibility is that improvements on the internal dimensions of actorness lead either directly or indirectly to (even greater) improvements on the external recognition and attractiveness dimensions. However, these changes have taken place against the backdrop of dramatic changes in the external policy context – reflected in the opportunity/necessity to act dimension – with the rise of the internet and the data economy creating an increasing impetus for the regulation of global data flows and greater protection for personal data in particular.

2.3. Dimension 1: Authority

Authority is defined as follows: 'This dimension refers to the legal competences that the EU has in a specific policy area. These competences are laid out in the Treaties of the European Union, but may also be complemented by issue specific agreements.' The authority dimension is primarily about the formal powers of the EU institutions (vis-à-vis the Member States), and the TRIGGER definition goes beyond the treaties to include EU legislation, as well as the policy cycle (that is, who is formally responsible for what at different stages of the policy cycle). An assessment of 'high' for authority would be appropriate in an area where the Member States have transferred all or nearly all formal authority to the EU. A level of 'low' would be appropriate where the Member States retain all or nearly all formal legal authority.

2.3.1. Analysis

After decades of evolving EU governance in this area, data protection is now firmly anchored in the treaties and in EU legislation. This creates a baseline of robust EU authority but needs to be qualified with reference to a significant number of exceptions that exist.

Data protection is rooted in Article 16 of the Treaty on the Functioning of the European Union (TFEU)[9]. This appears in Title II which contains 'provisions of general application,' implying that the protection of personal data is far-reaching, extending across both the public and private sectors. Article 16(1) states that 'Everyone has the right to the protection of personal data concerning them.' Article 16(2) goes on to mandate the EU to 'provide for data protection in all areas of European Union law' (Hijmans 2010).

This broad treaty basis for EU authority in relation to data protection is subject to a number of caveats, but these are minor in the overall scheme of things. First, Article 16 TFEU notes explicitly that its provisions do not apply to the EU's Common Foreign and Security Policy (CFSP), as laid down in Article 39 of the Treaty on European Union (TEU)[10]. Second, declarations 20 and 21 to the TFEU note that special treatment of personal data may be required in the areas of national security and policing. Third, the protocols to the TFEU contain derogations related to Article 16 for Ireland and the United Kingdom (Protocol 21) and for Denmark (Protocol 22).

The EU's strong authority is also reflected in a pair of legislative instruments that were agreed in May 2016 and have been implemented since May 2018: the GDPR and the Data Protection Law Enforcement Directive (LED)[11]. Whereas the GDPR directly imposes EU-wide authority on the Member States, the LED continues to rely on implementing measures being introduced by the Member States. Thus, the EU does not enjoy uniform authority across all aspects of this policy domain.

Although we are primarily concerned here with assessing the EU's authority vis-à-vis the Member States, it is worth noting that the GDPR (like the DPD before it) allows the EU to wield significant influence over international actors. The clearest example is the extraterritorial reach of the GDPR via Article 3 (Kuner 2015). Another is the fact that the European Commission takes the leading role in assessing whether data protection in third countries reaches the EU's standard of adequacy (Article 45) (Drechsler 2019). In the absence of formal global governance institutions relating to data protection

[9] See Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1 [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016E%2FTXT]

[10] See Consolidated version of the Treaty on European Union (TEU) [2016] OJ C202/1 [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016E%2FTXT]

[11] See 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 [2016] OJ L119/89.

(equivalent to the WTO in the trade field, for example), provisions such as these give the EU a significant degree of external authority.

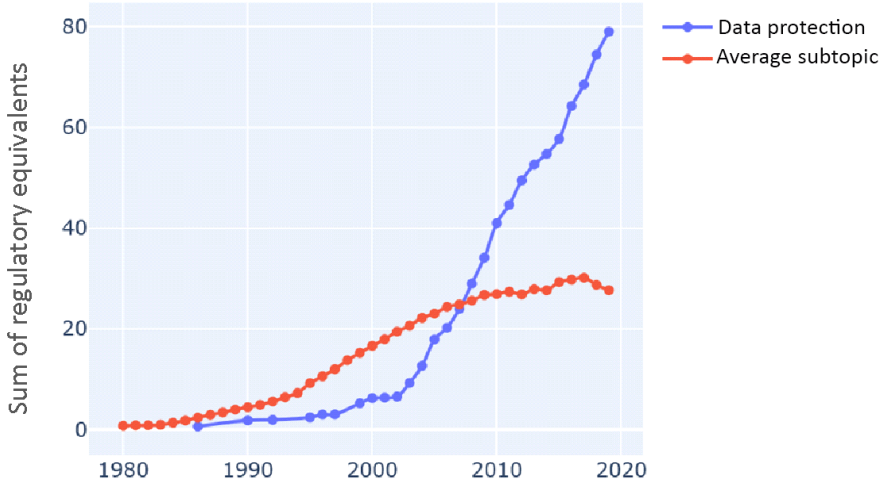
While the freedom that Member States enjoy when implementing directives should not be overstated, the direct applicability of the GDPR marks an increase in EU authority relative to the 1995 Directive. The GDPR's horizontal direct effect also widens the potential exposure of private actors for data protection infringements. The territorial, material and personal scope of the GDPR is extremely broad. However, it is worth noting that the EU's increased authority is subject to a number of exceptions. The preamble of the GDPR notes that it does not apply to national security, law enforcement, CFSP, or to data processing within households. The substantive articles of the regulation also allow for national rules in a range of areas. These relate, inter alia, to children (Article 8), sensitive data (Article 9), the right to be forgotten (Article 17) and 'public interest' data transfers to third countries (Article 49). Article 23 contains a list of rights and freedoms which may justify restrictions of GDPR protections. Finally, Chapter IX (Articles 85-91) provides a further list of areas in which national rules are permissible or required.

Although the adoption of key legislative instruments like the GDPR has played a particularly important role in shaping the EU's data protection authority, it is also important to note the catalysing role that the CJEU has played at various points. In a number of high-profile data-protection decisions it has demonstrated a willingness to interpret its treaty-based authority broadly, and it has put rights protection increasingly at the centre of the EU's data protection framework, even when it is potentially disruptive to do so, both in terms of inter-institutional dynamics within the EU, as well as in terms of political and economic relations between EU Member States and third countries. Important cases include Google Spain (2014) and Breyer (2016), but the most significant have perhaps been the CJEU's decisions striking down the Safe Harbor agreement and its successor, Privacy Shield. Notably, these two decisions were primarily a rejection of decisions that had previously been made by the European Commission. This intra-EU dynamic highlights the extent to which authority with respect to data protection is now located and contested at the EU rather than the Member State level.

It is also instructive to look at a wider survey of the body of EU law, beyond the milestone pieces of legislation. This approach assesses authority on the basis of the accumulation of all the legal instruments that the EU has passed on a given topic, with different categories of EU law coded in terms of 'regulatory equivalents' to reflect the greater or lesser impact that different types of instrument can have[12]. As the chart below illustrates, by 2019 there were almost three times as many regulatory equivalents in the area of data protection (78.99) as in the average policy area (27.64)[13].

[12] Regulations are scored as 1 'Regulatory Equivalent', while Directives are scored as 0.5, Decisions as 0.1 and International Agreements as 1. If a legal act is an amendment to an existing act, then its score is reduced to 20%.

[13] For the CEPS-developed application used to conduct this analysis, see more at https://trigger.eui.eu/ceps-eurlex-dataset-analysis/all/countryNotes



Source: CEPS EurLex web application

Figure 2 - The EU's accumulated legal authority

In terms of the evolution of authority over time, there has been a clear trend towards higher levels of EU authority in the area of data protection. This is most clearly illustrated in the changing nature of the legal regime for data protection across the EU, which as discussed in the previous chapter has progressed through three clear phases: initially ad hoc national measures, followed by national implementation of the common principles agreed in the DPD, followed by the directly applicable GDPR. This increase in the EU's legislative authority was influenced by the evolution of the treaties towards a greater focus on the EU as a political (rather than solely economic) community underpinned by fundamental rights. The Lisbon Treaty made the commitment to data protection explicit, but as was noted in the previous chapter, the political dimension of the Maastricht Treaty was an important enabler of Commission action that led to the DPD, in addition to the economic dimension related to the smooth functioning of the internal market. Finally, external developments also contributed to the EU's increasing authority in relation to data protection. The growth of the internet marked a profound economic and societal development and has challenged policymakers for decades. In the EU, the growing importance of the information economy meant that cross-border flows of personal data became an increasingly unavoidable aspect of regulating the internal market and upholding the rights of citizens (Pearce and Platten 1998). However, the EU does not enjoy the same level of authority along all stages of the policy cycle. This is particularly true of enforcement, which takes place primarily at the Member State level, through the national data protection authorities (DPAs). This is not unique to the data protection domain: in almost all policy areas enforcement takes place at the national level. However, in the data protection domain the system of enforcement is a source of ongoing fragmentation – and occasional dispute – and therefore can be seen as a limit on the *effective* authority of the EU, notwithstanding the role of bodies such as the Article 29 Working Party and the European Data Protection Board in maximising consistency in this area (Hijmans 2016).

Under the 'one-stop shop' system introduced in the GDPR, data processors with operations in multiple Member States only need to deal with the DPA in their primary location (Giurgiu and Larsen 2016). If

that DPA is (or is perceived to be) a weak link in the system, then it hampers the EU's formal authority from being enforced across the whole system and not just in the territory of the DPA in question. The possible reasons why an individual DPA might represent a weak link could include a lack of resources (which are allocated by national governments and can differ significantly between countries), as well as more substantive questions of political economy, relating for example to how a DPA believes it should balance data protection and national economic considerations (Kuner et al. 2012).

When the current system was being negotiated, the European Commission sought for itself a role that would help ensure consistency in the decentralised system of DPAs, with the power to temporarily suspend DPA decisions. Instead, control of this 'consistency mechanism' was granted in the GDPR to the new European Data Protection Board (EDPB) (Jančiūtė 2018). This EDPB role, as well as the guidelines, recommendations and best practices that the EDPB produces, aims, in effect, to limit the scope of DPAs to erode EU authority at the enforcement stage. And in the final instance, the CJEU can ensure that rules are applied consistently across the EU, as any complaints about DPAs can ultimately be referred to it.

2.3.2. Levels

Table 3 - Levels of authority

Phase	Level	Note
Pre-directive	Low	For most of this period, the EU plays a weak, inchoate role. As a legal framework for data protection begins to take shape, it is European countries rather than supranational institutions that take the initiative (including Sweden, Germany, Austria, France and others). Formal legislative authority rests at the national rather than the supranational level. Moreover, as discussed in the previous chapter, insofar as there is international coordination or influence, for much of this period it is provided by the Council of Europe and the OECD rather than the EU.
Directive to GDPR	Moderate	There is a step change in the level of EU authority in 1995 with the advent of the DPD. This phase also sees a twofold strengthening of the treaty basis for EU authority in this area: (i) internal market provisions develop more traction in relation to data protection as data become more commercially and economically more important, and (ii) data protection is established as a fundamental right in the treaties and the Charter of Fundamental Rights. This period also saw the introduction of the ePrivacy Directive (ePD), which was adopted in 1997 (and subsequently amended in 2002 and

		2009) in order to apply the principles of the DPD in the telecommunications sector.
Post-GDPR	Moderate/ High	There is a further increase in authority in 2018 with the coming into force of the GDPR. The position is one of strong authority, with a clear treaty mandate shaping a large body of EU legislation including the landmark GDPR. However, the level does not increase to the highest level. This reflects a number of significant constraints on the EU's authority in this area. There are many areas (notably relating to policing and security) in which Member States have retained the freedom to deviate from EU-wide rules. Moreover, the EU's effective authority is limited by the fact that enforcement takes place predominantly at the Member State level, through the DPAs. Mechanisms designed to ensure consistency of enforcement have yet to remedy fragmentation in this area (European Commission 2020c).

2.4. Dimension 2: Autonomy

Autonomy is defined in D3.1 as being complementary to authority. It 'refers to the resources and capabilities to act' and thus captures the potential gap that might exist between an actor's legal right to act and its ability to follow through on that legal right. This is not solely a matter of material resources. Autonomy also includes capabilities such as knowledge, institutional expertise, policymaking, idea-generation, networking, innovation and agenda-setting. In some cases, autonomy may best be assessed in terms of the presence or absence of resource deficiencies that could prevent the EU from acting to the full extent of its formal authority. It is possible that autonomy might enable an actor to exert power and influence despite the weakness or absence of formal authority. One example here in the data protection domain might be the early role played by the European Parliament and European Commission in catalysing an EU-wide approach to data protection, which then resulted in increased authority being vested in the EU institutions. A level of 'high' for autonomy would be appropriate in an area where the EU enjoys levels of relevant resources (money, staff, skills, connections, ideas, etc) that allow it to 'punch above its weight' in terms of formal authority. A level of 'low' for authority would be appropriate where the EU enjoys little or no relevant resources and so struggles to deliver on its formal levels of authority.

2.4.1. Analysis

The EU enjoys strong political leeway and agenda-setting freedom in the field of data protection. In part this mirrors the strong authority discussed in the previous section: as well as establishing the EU as a formal locus of authority, the GDPR also confers great agenda-setting power on the EU institutions.

Related to this, the autonomy of EU institutions is strengthened by the accumulated knowledge, expertise and networks (for example, between Commission officials, national DPAs and corporate privacy officers) that have been developed during the decades-long process of shaping how data protection is understood and implemented across the EU[14]. However, the inter-institutional dynamics do not all point in the direction of strong autonomy at the EU level. As noted above, the fragmentation of enforcement practices across the Member States is an important constraint on the EU institutions. Turning to the external impact of EU autonomy, there may be a connection here with the recognition dimension of actorness: the high levels of recognition that the EU enjoys among both state and non-state actors contributes to its ability to influence discussions about the global governance landscape for data protection (Greenleaf 2012). Within the Commission, data protection falls under the responsibility of two units in the Directorate-General for Justice and Consumers (DG JUST). The first of these units is 'Data Protection'; the second unit reflects the increasingly global reach of the EU's data protection rules: 'International data flows and protection'. Although staffing levels are relatively modest in these units (see below), they enjoy significant autonomy, particularly in the agenda-setting sense. This points to a potentially important relationship between the authority and autonomy dimensions. It suggests that an actor's ability to leverage even meagre levels of available resources is higher when the actor enjoys high levels of formal authority (as well as the external recognition this may bring).

In terms of the institutional arrangements created by the DPD and the GDPR, the decentralised system of national data protection authorities (DPAs) represents a potential constraint on EU autonomy (Schütz 2012). This is because of the significant powers enjoyed by the DPAs, such as on guidance and enforcement of rules, independent of both the EU and its Member States. While the overall trajectory of data protection governance in the EU has been from the national to the supranational, as noted in the previous section it remains possible for a national DPA to weaken the overall integrity and consistency of the EU-wide data protection regime.

In the EU's 2014-20 budget, data protection fell under the Rights, Equality and Citizenship (REC) programme in DG JUST. This programme was allocated EUR 439 million, out of a total Security and Citizenship budget of EUR 18 billion (and a total EU budget of EUR 1.1 trillion)[15]. An initial TRIGGER assessment of the number of people working in the EU on areas related to data protection points to very low staffing levels[16]. In the Commission, for example, the personnel database lists just 27 people with the phrase 'data protection' or the word 'privacy' in their job title or the name of their unit. This compares with much higher figures for the other three topic areas being covered in WP7: 467 Commission employees for sustainability, 259 for climate-related issues and 298 for the EU-Africa partnership. Notwithstanding questions about the accuracy of these budget and staffing data, a general pattern of relatively low levels of EU resourcing in the field of data protection would be consistent with the EU's developing role as a 'regulatory superpower' in this area. Whereas policy areas such as climate change,

[14] For a list of key communications and similar documents, see the timeline in chapter 1, section 1.1.2.

[15] See more at https://ec.europa.eu/justice/grants1/programmes-2014-2020/rec/index_en.htm

[16] This is a dataset scraped from the EU's official who-is-who.

sustainable development or the EU-Africa partnership involve major spending programmes, the EU's role on data protection is more one of shaping agendas and codifying rules, relying on others to a significant extent for enforcement and monitoring of compliance.

As the discussion so far suggests, the autonomy of the EU has increased over time. In part, this follows the trajectory of authority, with the introduction of the DPD and then the GDPR anchoring data protection at the EU level and therefore increasing the EU's scope to set the agenda. This has been a self-reinforcing process, with the EU developing cumulative knowledge and expertise through successive multi-year legislative and institutional cycles. In addition, the baseline level for autonomy in the first measurement phase (before the DPD) is slightly higher than for Authority. This reflects a point made in the definition of autonomy above. It is a sign of higher autonomy when an actor is able to exert influence despite the absence or weakness of formal authority. This is a good description of the early role taken by the EU institutions in the 1980s (initially the Parliament, but then with the Commission gradually taking on a much more significant role) in creating the conditions for the formalisation of EU authority in this policy area.

2.4.2. Levels

Table 4 - Levels of autonomy

Phase	Level	Note
Pre-directive	Low/Moderate	As discussed in the previous section, the EU had weak authority at this time. By definition, the ability of EU institutions to 'bootstrap' a role for themselves in this policy area reflects the exercise of autonomy rather than authority. As discussed in the chapter on the evolution of EU governance, the European Commission was instrumental in this process, working to catalyse and then consolidate support for a supranational approach to data protection.
Directive to GDPR	Moderate	The level across this time period increases by one step to 'moderate'. This is primarily a reflection of the EU's increasing agenda-setting power in this domain, as its leadership position on data protection governance is bolstered first by the introduction of the DPD and then the adoption of the Lisbon Treaty. Ownership of large swathes of data protection policy was now situated firmly at the EU level, which as noted above allowed the EU to leverage the relatively modest resources devoted to data protection, both within the EU and externally.

Post-GDPR	Moderate	The level for autonomy does not change in any of the post-GDPR years, remaining at 'moderate'. While the EU's agenda-setting power has been further strengthened since the introduction of the GDPR,its own resources in this area remain low, and this is an important aspect of the autonomy definition. In addition, the EU institutions remain reliant on others for enforcement and monitoring.

2.5. Dimension 3: Cohesion

Cohesion is defined in D3.1 as 'a consistent line of argument, meaning that the involved nation states are 'speaking with one voice' and share the same policy preferences in a specific policy area.' It is a measure of shared values, norms, principles and interests. Although the primary focus of this actorness dimension is on cohesion between the Member States and EU supranational institutions, it also concerns intra-EU cohesion among the institutions. A level of 'high' for cohesion would entail high levels of EU-MS and intra-EU alignment on all key aspects of a policy area. A level of 'low' would be appropriate in a policy area characterised by competing visions, narratives, values, preferences, interests, etc.

2.5.1. Analysis

There is a high degree of cohesion around most aspects of data protection in the EU. Clearly, important fundamentals are shared across the 27 Member States. Data protection is expressly laid down in the treaties as a fundamental right and a general principle of EU law. Important parts of this principle have been operationalised in a binding EU-wide regulation. The core principles that underpin the governance of data protection in the EU are uncontested. They stretch back to the early 1980s and are aligned with international norms developed by the Council of Europe and the OECD.

Despite this bedrock of shared fundamentals, there are various divergences over aspects of data protection. Not all of these should be seen as detrimental to cohesion. For example, the separate legislative treatment of data protection in the field of law enforcement (that is, in a directive requiring national implementing measures – the LED – rather than in the GDPR) is foreseen in the treaties, and so arguably counts as an expression of cohesion: it reflects a shared view as to the need for special provisions in that area. The specific treaty derogations enjoyed by Ireland, the UK and Denmark (see the Authority section, above) are a clearer instance of certain Member States delineating the limits of their willingness to rely on shared treaty provisions and legal instruments. More generally, as discussed in the chapter on EU governance, Ireland has been seen as comparatively soft on data protection because of its economic interest in continuing to host many of the European operations of some of the world's largest data processors (Jančiūtė 2018). Fragmentation of enforcement at the Member State level has been mentioned already in the authority and autonomy sections, but it can also be seen as a potential indicator of lower cohesion.

It should also be noted that the existence of a strong degree of cohesion in the fundamentals of data protection does not imply homogeneity in this area. As the previous chapter noted, the negotiations leading up to the adoption of both the DPD and the GDPR were characterised by significant differences between EU institutions (notably the Parliament and Commission), and between the supranational institutions and the Member States in the Council. Differences have also been evident within individual EU institutions, such as between individuals from different political groupings in the Parliament. As discussed in the previous chapter, one factor that helped with passage of the GDPR through the Parliament was the choice as rapporteur of Jan Philipp Albrecht, a Green MEP with a strong record of voting for privacy protections, rather than Axel Voss, from the EPP, who had a strong record of opposing such measures. Different Member States have also taken different positions during negotiations in the Council, with Ireland and the UK adopting a more business-friendly approach when the GDPR was being negotiated.

EU cohesion on data protection has deepened significantly over the period under analysis. The starting point of our analysis in the 1980s was characterised by weak cohesion in this nascent policy area. However, as national laws were introduced they already shared some common features and principles, in line with an emerging international consensus on what the core of data protection entailed[17]. Nevertheless, there were still significant differences between national priorities and legal/commercial cultures across the EU, and as noted in the previous chapter, reconciling these national differences was one of the key challenges for the Commission in drafting the DPD. It is also worth recalling that during the 1980s, there were significant intra-EU differences, with the Parliament and the Commission taking different approaches to data protection, largely on the basis of the perceived tension between data protection and the promotion of economically significant new information technologies (Simitis 1995). From the early 1990s, the changing approach of the Commission (that is, an increasing focus on the normative dimension of data protection in addition to its economic significance) represented an increase in intra-EU cohesion in and of itself and was also a catalyst for a period of deepening cohesion among Member States. Key milestones over the next two decades included national laws being at least partially harmonised via the DPD and data protection being anchored in the treaties in 2009. The evolution from the DPD to the directly applicable GDPR provides further evidence of deepening cohesion, despite the extensive national carve-outs that it contains. Moreover, negotiations leading up to the GDPR's adoption also bolstered cohesion, even if the reasons for this were at times external and fortuitous, as with the galvanising effect of the Snowden revelations on Member States attitudes towards the need for stronger protections (Barbière 2014).

2.5.2. Levels

Table 5 - Levels of cohesion

[17] For more details of the early evolution of data protection rules in the EU, see the previous chapter.

Phase	Level	Note
Pre-directive	Low/Moderate	The first phase is one of relatively weak cohesion, as is natural given how new of a policy issue data protection was at that time. However, as a growing number of national rules are put in place, there are broad 'family resemblances'. The biggest divergence among the Member States is not between competing visions of data protection, but between the countries that have or do not have data protection rules in place. Overcoming this divergence provides the impetus that leads to the introduction of the 1995 Directive.
Directive to GDPR	Moderate	There is a significant strengthening of cohesion during this period. This averages out at a 'moderate' level across the whole period, but two separate developments indicating higher cohesion set the scene for a further increased level in the post-GDPR period. The first change during this period is the agreement of shared rules (albeit nationally implemented) in the directive. The second is the Member States' agreement to explicitly include data protection as a fundamental right in the Lisbon Treaty.
Post-GDPR	Moderate/ High	With the agreement of the GDPR (and the directive on law enforcement), there is another increase in the cohesion level, reflecting a further ratcheting upwards of the Member States' alignment on data protection. This takes the cohesion level to 'moderate/high' in line with the equivalent post-GDPR level for authority. One way of thinking about this is to note that there is a strong degree of cohesion even about how authority should be divided between the Member States and the EU institutions. (In short, all the Member States agree that more national flexibility is needed in areas like national security and law enforcement. It is not that Member States have insisted on a patchwork of different national carve-outs.)

2.6. Dimension 4: Recognition

Recognition is defined in terms of the EU being 'recognised as an actor and legitimate negotiation partner by other actors in the international system.' This is a relative rather than an absolute concept, with the EU's recognition being considered in comparison in the context of how strong or weak is the recognition of other actors. It is also positive rather than normative: this dimension of actorness assesses only the relative strength/intensity of recognition, and is not affected by whether the EU is viewed favourably or unfavourably. (That normative aspect of external perceptions is captured in the

attractiveness dimension.) Another important feature of the definition relates to the EU's formal legal standing as a party to international organisations, conventions, etc. A maximum level for recognition indicates that the EU is widely viewed as one of the most powerful actors in the global governance of a given policy area. A level of 'low' indicates that the EU is viewed as having little or no power or legal standing.

2.6.1. Analysis

In an area such as trade policy, one way of gauging the recognition of the EU is through the legal quality of its participation and its independent standing in an international organisation like the WTO. There is no comparable multilateral governance body for data protection, although global interaction and collaboration are increasing in forums such as the Global Privacy Assembly (in which the European Commission and EDPB are observers). There is ample evidence of the EU being recognised externally as a powerful actor in the global governance of data protection. This reflects the explicitly international nature of the EU data protection regime. First, it is extraterritorial in scope, which means that the combined authority, autonomy and cohesion that the EU has accumulated over many years has direct relevance for many affected data processors in other countries. Second, EU institutions are at the heart of the system of adequacy decisions and related mechanisms that have shaped cross-border data transfers between the EU and third countries since the DPD.

A possible counter-argument here is that these formal considerations overlook the reality of international diplomacy, which is still likely to see third countries use well-oiled bilateral relationships with Member States in order to raise any data protection issues that have arisen (Hilden 2019). While this is possible, it is limited by the increasingly clear position of the CJEU as the final arbiter on matters of data protection, a role that it has played independently and expansively: for example in its much broader interpretation than the Commission of what the term 'adequate' requires in a third-country's data protection regime (Drechsler 2019).

Another potential rival for the EU institutions as a perceived interlocutor for external actors is the system of national data protection authorities (DPAs). The DPAs play an extensive enforcement role, creating potential incentives for data processors (or their home-country governments) to seek to cultivate a lenient relationship with a DPA or to 'forum shop' across the EU to exploit any differences in enforcement standards between different DPAs. Even in the absence of any such gaming of the DPA system, the central role played by the DPAs in the day-to-day operation of the EU data protection regime potentially detracts from the recognition enjoyed by the EU institutions. In addition to their enforcement role, the DPAs also play a role in third-country data transfers involving standard contractual clauses (GDPR Article 46) and binding corporate rules (Article 47).

Beyond these institutional considerations, it is difficult to identify indicators that will accurately reflect the level of recognition of the EU as a global governance actor. One potential proxy that has been explored by the TRIGGER project is a data mining exercise on a corpus of international media articles about data

protection. According to a preliminary analysis of these data, the EU is the most frequently referenced public-sector entity over the 2010-20 period; the only group to be referred to more frequently in these articles is the 'US tech giants' category. However, without deeper qualitative assessment of the media sources and the individual mentions of different actors, these data should not be over-interpreted. A related proxy is the prominence of the EU in academic discussion of data protection over the past decade. A search of the titles of data protection articles indexed by Google Scholar reveals a greater focus on the European Union than in the US or China. Since 2010, there have been 803 articles with the phrases 'data protection' and either EU or European Union in the title[18]. The corresponding figures for the US and China are 105[19] and 30[20]. Unlike in the media mining exercise, the US tech giants do not feature prominently in the results of the Google Scholar search, returning just 32 articles since 2010[21].

2.6.2. Levels

Table 6 - Levels of recognition

Phase	Level	Note
Pre-directive	Low	There is weak recognition for the EU in the first phase. In part, this reflects the fact that data protection was still an emerging policy area, with limited arrangements for global governance. It also reflects the fact that before the introduction of the Directive other actors were seen as being in the lead on data protection. Insofar as there were international actors shaping the international governance of data protection, it was the Council of Europe and the OECD rather than the EU.
Directive to GDPR	Moderate	The recognition of the EU as a global governance actor increased by two steps in this period with the introduction of the DPD and with the general increase in the relevance of data governance to international commerce and economics. While the primary focus of the directive was the harmonisation of Member State rules affecting the flow of data within the EU, it was also extraterritorial in scope, tying market access to third-country data protection adequacy.
Post-GDPR	High	The introduction of the GDPR consolidated the EU's position as a regulatory superpower in the area of data protection, establishing a framework of rules that few third-country actors (private sector or public sector) can afford to ignore.

[18] Search string: allintitle:'data protection' ('european union' OR EU).

[19] Search string: allintitle:'data protection' ('united states' OR US).

[20] Search string: allintitle:'data protection' china.

[21] Search string: allintitle:'data protection' (facebook OR google OR amazon OR alphabet OR apple).

Notwithstanding the important role played by the DPAs – particularly in Ireland, where many of the largest third-country data processors have their EU operations – the European Commission and the CJEU are the key institutions in terms of projecting the EU's data protection rules globally.

2.7. Dimension 5: Attractiveness

Attractiveness is defined in D3.1 in the following terms: 'It describes how much other actors perceive cooperation with the EU as something worth striving for. It is defined by both, the economic attractiveness of the EU, but also the values and norms or the EU's soft powers.' It therefore contains two key elements, one instrumental (the material benefits of aligning with EU governance in a policy area) and the other normative (the EU as a source of governance best practice to be emulated). The material benefits are defined primarily in terms of the economic benefits of alignment with the EU, either in terms of market access or investment flows. As with the recognition dimension above, attractiveness is a relative concept: how attractive is the EU in this policy area compared with other key actors. A level of 'high' for attractiveness is warranted where there is a high degree of policy emulation or influence and/or relevant investment to or from the EU. By contrast, a level of 'low' indicates that there is active reluctance to align with EU governance and/or little or no economic advantage in doing so.

2.7.1. Analysis

There is unambiguous evidence of third countries emulating or being influenced by EU approaches to the governance of data protection, particularly since the introduction of the GDPR (Greenleaf 2012; 2021). But because the EU was a relatively early and strong mover in this policy area, and with an explicitly normative approach, there can be a tendency to jump too quickly from an assessment that the EU is widely recognised as a global governance actor on data protection, to an assessment that it is seen globally as an attractive model to be emulated. For example, while the US and China might recognise the EU as a powerful global governance actor, there are significant limits to how attractive the EU's governance model is to them. Notwithstanding the gradual evolution of a body of data protection rules in China, there is no sense in which it is emulating the EU's individual rights-based approach, or seeking to attain the EU's standard of adequacy (Sacks, Shi, and Webster 2019). The US is much closer to the EU's legal and political culture than is China, and current moves to strengthen US data protection rules have undoubtedly been influenced by the EU example, but there remain significant normative divergences which limit the extent of policy emulation between the two. This was discussed in the chapter on the evolution of data protection global governance; it continues to shape differing approaches to the digital economy. As the two largest consumer markets in the world, there are deep trade and investment connections between the US and the EU, and policymakers on both sides have consistently sought to avoid blocking these flows. However, it is noteworthy that (i) the US has only been willing to sign up to an amended or tailored version of the adequacy regime, with Safe Harbor and then the Privacy

Shield, and (ii) that these agreements have subsequently been deemed invalid by the CJEU, precisely because of their failure to emulate the full protections required in the EU. This points to a tension between the instrumental and normative aspects of the attractiveness dimension with respect to the EU-US relationship. Aspects of the data protection regime in both the DPD and the GDPR have also been viewed with hostility by some US scholars. The extraterritorial reach of both instruments in particular has been seen by some as an 'aggressive' attempt to foist EU norms on non-EU countries (Salbu 2002). Given the undisputed status of the US and China as technological superpowers, and the share of global economic and data-related activity they account for, their reluctance to emulate the EU should inform our overall assessment of the EU's attractiveness.

The clearest evidence of the normative attractiveness of the EU's data protection governance would be when another country replicates some or all of the EU regime in its own domestic rules. Perhaps the best example of this is Brazil, which published a data protection law in 2018 that closely mirrors the key provisions of the GDPR (Perrone and Strassburger 2018). This law took effect in August 2020. Another example is Thailand's 2019 Personal Data Protection Act (Greenleaf and Suriyawongkul 2019). An example like India is more complicated, as discussed in the previous chapter, with a law that follows the GDPR in important respects, but which has also been amended to remove judicial oversight for government access to citizens' personal data. It is not just countries that can be seen emulating the EU's approach to data protection. Corporations have been doing so too, including Microsoft, which applies core provisions of the GDPR globally (Brill 2018). This is the 'Brussels effect' in action (Bradford 2012; 2020). There are commercial reasons for a multinational company to standardise its rules globally in this way, but that does not mean that the normative factors highlighted by Microsoft should be disregarded.

It is important to note that when looking at whether policy emulation has occurred between countries, establishing the causality is not simple. There may be independent factors or pathways that lead to the similarity. In the case of data protection, it is worth recalling that some of the core principles underpinning the EU's approach to data protection were first codified by the Council of Europe and the OECD. The EU's data protection framework builds on a foundation that was developed internationally. There is a danger of blurring the lines between the recognition and attractiveness dimensions of actorness, and of jumping from the fact that the EU is a recognised leader in data protection governance to the conclusion that it also motivates the actions of others in this area. For example, while the growing debate about state-level and federal data protection rules in the US is clearly informed by developments in the EU, Chander et al. (2019) caution against over-simplifying the extent to which the US is emulating the EU. They point instead to the roots of a statute such as the California Consumer Privacy Act (CCPA) in American legal and commercial culture, and they stress the role of 'networked norm entrepreneurs' in driving the process forward, as opposed to the more top-down process they see in the EU.

Turning to the instrumental attractiveness of the EU's data protection governance regime, we see that it relates primarily to market access rather than investment. Indeed, the EU's strict data protection rules

are frequently cited as an obstacle to investment in various emerging technologies that rely on data processing. Third countries have a clear incentive to meet EU standards in order to allow cross-border data flows in and out of the EU's market of 500 million consumers with GDP per capita of around EUR 25 000[22]. At present, the EU recognises 13 countries as providing adequate levels of data protection under the terms of the GDPR, and talks are ongoing with South Korea (European Commission n.d.). However, these country-level adequacy decisions are only one element in the panoply of methods by which third-country data protection standards can be validated. In addition to the troubled attempts to craft standalone agreements with the US, covering around 5 000 entities (Privacy Shield Framework 2020), the EU also allows for enterprise-level alignment with GDPR principles, via standardised contractual clauses (SCCs) that are used by thousands of businesses, and binding corporate rules (BCRs).

2.7.2. Levels

Table 7 - Levels of attractiveness

Phase	Level	Note
Pre-directive	Low	Assessment of the attractiveness dimension is complicated by the range of contributory factors. As well as having to consider the normative and instrumental implications of the EU's governance framework per se, it is also necessary to consider wider economic developments: the greater the size of the data-related EU market, the greater the attractiveness of securing or maintaining access to it. In the first period, as with the recognition dimension, the level for attractiveness is 'low'. In instrumental terms, the economic value of the 'information society' remains potential rather than actual at this stage. And in normative terms, the EU is not yet a leader. As noted above, the Council of Europe and OECD were the early pioneers in terms of framing principles for widespread international adoption.
Directive to GDPR	Moderate	The level rises by two steps to 'moderate' during this period. This increase reflects two things. The first of these is the huge growth in data-driven economic activity during this period, and the corresponding increase in the potential value of cross-border data transfers with the EU. The second relates to the introduction and evolution of adequacy and related

[22] See more at https://ec.europa.eu/trade/policy/eu-position-in-world-trade/

		provisions that tie third-country market access to having EU-compliant data protection provisions in place.
Post-GDPR	Moderate/ High	There is a further increase in the level for attractiveness in this period, reflecting the same twin processes as in the previous period: growth in the economic value of cross-border data flows, and the GDPR's consolidation of the conditionality mechanisms tying market access to data protection.

2.8. Dimension 6: Opportunity or Necessity to Act

This dimension of actorness differs from the others in that it incorporates into the actorness concept factors that may be beyond the control of the EU, namely the state of the external governance environment. This is perhaps counter-intuitive, given that the concept of actorness seeks to capture the ability of the EU to exert agency, influence and control. However, the level of agency, influence and control that the EU can exert in a given policy area is constrained by external circumstances: if there are no opportunities for the EU to act, then its ability to act is necessarily constrained, regardless of how strongly it may score on the other dimensions of actorness. As the definition in D3.1 puts it: 'developments and constellations in the international arena [are] one factor that also determines the degree to which the EU can be an actor.' This dimension is therefore concerned with the existence of windows of opportunity that create an opening for the EU to act. It also covers external threats or crises that make it necessary for the EU to act. The scoring also takes into consideration the nature of the EU's response – proactive or reactive – to such developments in the external governance environment. A maximum level on this dimension is warranted where (i) there is ample opportunity/necessity for the EU (and other actors) to act, and (ii) the EU is proactive in exploiting such openings in order to shape the global governance landscape. A level of 'low' would be appropriate in circumstances in which there are no such openings for the EU to act.

2.8.1. Analysis

The EU has been an active and assertive governance actor in the data protection domain from the outset, and developments have provided it with plenty of opportunities to act. The external policy environment has been characterised less by isolated windows of opportunity than by multiple global and regional trends which have combined to provide an ongoing opportunity for the EU. These trends include: (i) digitalisation and the increasing volume and significance of personal data, (ii) the increasing size of the data-related economy, and (iii) developments in the EU – notably its increasingly political character since the 1990s – that brought data protection more firmly within its ambit.

In terms of the EU's response to these developments in the external policy arena, there is an important element of path dependency to highlight. The Commission moved quite early (1990) to propose the internalisation and harmonisation of an emerging core of data protection principles around which other

actors were already beginning to align – notably the Council of Europe and OECD, but also those Member States that had already introduced national data protection legislation. This early move positioned the EU institutions rather than the Member States as the natural locus for further policy moves in this area. This set the scene for a subsequent ratcheting up of policy in this area in response to technological and economic developments. The clearest instance of this subsequent ratcheting is the move from directive to regulation with the introduction of the GDPR.

Another point to note about the EU's approach is the early and assertive manner in which it sought to project its system of data protection governance externally. It incorporated explicit extraterritorial provisions into its core data protection instruments, leveraging its market size and power to incentivise the adoption of its approach in third countries. In the absence of a formal multilateral framework for data protection, this commitment to extraterritoriality also gave the EU an 'early mover advantage' in terms of being a key influence on the evolution of global norms and patterns of cooperation in this area.

Risks related to surveillance and manipulation have been a repeated driver of data protection governance changes. The chapter on the evolution of global governance noted that the first data protection law, in 1970 in the region of Hesse, rested on fears that new government databanks would facilitate government surveillance and the manipulation of individual behaviour. Similar fears remain a commonplace feature in discussion of data protection governance, and the 2013 Snowden revelations are a specific example of surveillance risks contributing to the policy development process in the EU. It would go too far to say that the Snowden episode created a 'necessity' to act, but it certainly added impetus to GDPR negotiations at an important stage (Butler and Hidvegi 2015).

Not all windows of opportunity are external. Arguably, the Lisbon Treaty can be seen as an internal window of opportunity, which was leveraged to deepen the EU's commitment to data protection. From the perspective of the EU institutions, the new prominence of data protection in the treaties following Lisbon shifts the dynamic to one of 'necessity to act' rather than 'opportunity to act'. The Schrems decisions are an example of this process in action, with the Commission twice developing bilateral workarounds in response to the fact that the US does not meet the adequacy threshold, and the CJEU twice deeming those workarounds insufficient. The fact that data protection is embedded in the treaties as a fundamental right means that the EU crosses the 'necessity to act' threshold more easily than would otherwise be the case.

2.8.2. Levels

Table 8 - Levels of opportunity or necessity to act

Phase	Level	Note
Pre-directive	Low/Moderate	The level on this dimension is 'low/moderate' over the pre-directive period, but that masks some evolution during that timeframe. The most important influences on the level during

		this phase were external: the changing role of data and the emergence of a patchwork of national responses across the EU created an opportunity for the EU institutions to take a coordinating role. This window of opportunity was strengthened by internal developments in the EU: as noted previously, the increasingly political character of the EU allowed (or required) the Commission to point to political as well as economic reasons for putting consistent data protection rules in place.
Directive to GDPR	Moderate/High	The level on this dimension of actorness continues to increase during this phase. Again, this largely reflects the continuing (and accelerating) evolution of the societal and economic role of data in the years following the introduction of the directive. As in the first phase, internal considerations also play a role: the incorporation of data protection into the Lisbon Treaty strengthens the responsibility of the EU institutions to act externally in order to protect the fundamental data protection rights of EU citizens. This phase also sees external factors push the EU towards action, such as the Snowden revelations in 2013, which galvanised progress towards the GDPR:
Post-GDPR	High	The EU is at the maximum level throughout the post-GDPR period. This reflects (i) the pivotal and deepening role of data in almost all aspects of contemporary life, which makes it essential that there is ongoing vigilance and action to ensure that governance frameworks evolve, and (ii) how well positioned the EU institutions are to take the lead in this area, following decades of accumulated authority, experience, reputation, etc, during the preceding two periods.

2.9. Dimension 7: Credibility

In the TRIGGER project, credibility is defined primarily in terms of whether other global governance actors (typically states, but also including other important actors such as tech giant corporations) have good reason to believe that the EU will act consistently and follow through on what it commits to do[23]. It is therefore closely related to the EU's record of goal attainment or effectiveness, which is the subject of the next chapter. In addition, the credibility dimension also presupposes a degree of ambition: it would not indicate significant credibility if a trivial commitment were upheld. Unlike the other dimensions of

[23] Thus defined, the credibility dimension of actorness is closely related to considerations of trust: is the EU trusted (to act consistently, in good faith, etc) in the area of data protection?

actorness, the credibility dimension is cross-cutting in the sense that it has both internal and external aspects. In other words, we are interested in the credibility of the EU institutions in the eyes of both Member States (internal) and global actors (external). A level of 'high' indicates that there are very strong reasons to expect the EU to deliver on its commitments. A level of 'low' indicates that there is little or no reason to expect the EU to follow through in this way.

2.9.1. Analysis

There is some overlap between this dimension of actorness and two that have already been discussed: authority and recognition. The recognition dimension is related to the EU's credibility with external actors – the EU would not be recognised as a key interlocutor if it did not have a track record of behaving in a consistent and reliable manner, following through on commitments it has made. Similarly, a high level of authority is also likely to contribute to the EU's credibility with external actors, in the sense that it has the formal powers required to make commitments and to stick to them. A strong level on the authority dimension also provides prima facie evidence that the Member States view the EU institutions as a credible and trustworthy custodian of a given policy area (Hoffman 2002). Authority demonstrates willingness by Member States to cede control, which they would be unlikely to do if they did not expect the EU to act responsibly, predictably and according to shared norms and values[24]. (In this sense, there is also some overlap between the internal aspect of credibility and the cohesion dimension.)

We point to three factors that have contributed to a high level of EU credibility on data protection. The first is consistency over time. Data protection has been a focus of EU policymaking for almost four decades, and although there have been huge changes over that time, the current governance regime is still recognisably rooted in the values and objectives that characterised the EU's early work in this area during the 1980s. For the most part, the evolution of the EU's approach to governance has involved the introduction of new measures to advance existing principles more effectively, rather than the introduction of new principles. An exception to this might be changes in the weight attached to economic and fundamental rights considerations as the basis for data protection rules. However, as discussed in the previous chapter, this reflects deeper changes in the constitutional status of the EU rather than inconsistency on data protection.

A second and related source of credibility relates to the twin objective of harmonising data protection rules within the EU and projecting them externally. Each stage in the evolution of the EU's governance of data protection has reviewed progress on these objectives and tailored the regime in response. This provides a very clear signal (both to internal and external actors) that the EU views this as a core concern and will continue to iterate its regulatory approach in order to deliver success. This is most clearly evident in relation to harmonisation, where, as the last chapter outlined, there has been a series of step changes:

[24] In practice, matters might be more complicated than this suggests. There may be reasons why a Member State might cede authority to the EU despite concerns about its credibility. These reasons could include a weak negotiating position on the issue in question, or a strategic decision to cede authority in a low-priority area in order to preserve it in a higher-priority area.

first, the relatively ad hoc national arrangements in the 1980s; second, the national implementation of the EU-wide DPD from the mid-1990s; and third, the directly applicable GDPR. This process continues. In its two-year review of the application of the GDPR, the Commission continues to highlight areas of possible fragmentation in the system that may need attention, such as the resourcing of national DPAs (European Commission 2020c). The international reach of the EU's data protection principles has already been discussed in the attractiveness section, but it is also worth noting that this process of internationalisation can also increase credibility. An important example here is the cooperation between the EU and the Council of Europe on the revision of Convention 108, which brings important GDPR principles into a framework with which non-EU and non-European countries can formally affiliate (Greenleaf 2018c).

A third important source of EU credibility on data protection is the strong line that the CJEU has taken in milestone decisions. These include the invalidation of the Data Retention Directive in 2014, the clarification of the right to be forgotten, also in 2014, and the two Schrems judgments in 2015 and 2020 (Tzanou 2020; Granger and Irion 2014; Lynskey 2014; Lindsay 2014). The CJEU has interpreted data protection broadly and has repeatedly demonstrated its willingness to hand down decisions that are potentially highly disruptive both for other EU institutions and for external actors. This gives a very clear signal that the constitutional protection that data protection principles enjoy is not just formal but substantive, and will be pursued to its logical conclusions rather than being fudged. Paradoxically, this strong signalling of credibility by the CJEU may raise credibility issues elsewhere in the EU's treatment of data protection. For example, the US has now twice agreed a data protection agreement with the Commission, and it has twice seen its agreement overturned by the CJEU. This may undermine the Commission's credibility as a negotiator with the US, if it is perceived as being unable to gauge reliably the constitutional limits within which it has to operate.

Another potential counter-argument to consider on credibility relates to the EU's objectives around being an engine of innovation and economic growth. In an important sense, these objectives are separate from the EU's constitutional commitments to data protection as a fundamental right. Nevertheless, it is now frequently suggested that the extent of the EU's commitment to data protection has become an obstacle to its development in data-heavy activities that account for an increasing share of economic activity. In other words, the EU's credibility on data protection may come, to a certain extent, at the expense of its credibility as an economic actor. The potential trade-off between these two aspects of the EU's credibility is interesting given that the initial phase of the EU's involvement in data protection, as discussed in the last chapter, saw strong data protection both as an end in itself (as an individual right) and as a means to other ends (increased cross-border economic activity). With this in mind, it is striking that recent proposals from the Commission target the development of policies, and even technological infrastructures, that will allow the EU to increase its relative share of the global data-driven economy without compromising on its approach to data protection (European Commission 2020a; 2020b). (Another noteworthy initiative in this regard is GAIA-X, which envisages GDPR compliance by design, a development that would avoid or minimise the need for enhanced international regulatory cooperation

to enforce GDPR.) The EU's ability to balance the twin goals of data protection and economic dynamism is likely to be an important test of the EU's credibility in the years ahead, particularly given current patterns of heightened geopolitical and geoeconomic uncertainty.

2.9.2. Levels

Table 9 - Levels of credibility

Phase	Level	Note
Pre-directive	Low	The EU has a level of 'low' for this period, reflecting the fact that it did not have clear ambitions in the data protection area, let alone a track record of credibly delivering on them. Moreover, in the earliest years of this phase, the EU's approach to data protection was characterised by inter-institutional tension rather than consistency, with the European Commission rebuffing calls from the European Parliament for legislative action. However, the EU's credibility begins to increase later in this phase, as the Commission's proposal for directive initiates a decades-long process of building and strengthening the EU's role in the governance of data protection across the bloc and in its third-country relationships.
Directive to GDPR	Moderate	The credibility level increases during this phase, in line with significant changes in the legal/constitutional framework. First, in 1995 the EU delivered on its ambitions to improve the harmonisation of national laws with the introduction of a directive. Second, with the advent of the Lisbon Treaty and the elevation of data protection to a fundamental right and general principle of EU law, the CJEU becomes a powerful guarantor of the integrity of the EU's data protection rules.
Post-GDPR	Moderate/ High	The EU's 'moderate/high' level during this period reflects the continuity of the EU's approach to data protection: the predictable, rules-based and clearly signalled application of the same core principles that informed the drafting of the directive more than 25 years ago. One question that arises here (and that will recur in the later chapter on future opportunities and challenges) is whether the credibility of the EU's approach to data protection governance is undermined by what some view as its adverse economic impact (particularly in terms of hampering the development of data-

intensive sectors in Europe). Our assessment assumes that – thus far at least – any such economic considerations have not eroded the EU's credibility in this policy area.

3. EU effectiveness in the data protection domain

3.1 Introduction

The previous chapter assessed the actorness of the EU in the domain of data protection. In this chapter, we turn to consider how effective the EU has been in this area. We define effectiveness in terms of goal attainment and, in line with the overarching focus of the TRIGGER project, we are primarily concerned with those goals that relate to the EU's influence over or impact on global governance. Assessing effectiveness requires an argument in two main stages. First, the EU's goals must be identified. Second, the extent to which the EU has attained these goals must be assessed. The second of these steps is fraught with difficulties which will be beyond the scope of a chapter such as this to resolve fully. Smith (2010) captures these challenges succinctly: 'Measuring 'effectiveness' is inherently a difficult task – how can we attribute 'success' to the EU, rather than, say, to domestic actors or other international actors or beneficial international developments or just plain luck?' In other words, it is not sufficient to assess whether a given EU goal has been attained. Determining how effective the EU has been means also assessing the extent to which the goal's attainment can be attributed to the actions of the EU.

This chapter proceeds as follows. In section 3.2, we identify the EU's main goals in the data protection domain. These meso-level goals should be in line with the macro-goals of the EU, which have been discussed in the introductory chapter to this deliverable. They are also expected to determine the content of the EU's micro-level goals, i.e., the more granular objectives that the EU adopts in specific contexts with a view to helping to attain its meso-level goals. In section 3.3, we provide an overview of the main methods and instruments with which the EU has sought to attain its data protection goals. By contrast with some other domains where international negotiations shape the global governance landscape, in the case of data protection the EU has mainly used its own legal instruments to shape the behaviour of other global governance actors. In the remainder of the chapter, our focus shifts to goal attainment. In section 3.4, we consider two case studies and assess the extent to which the EU has been able to achieve its aims in each. These case studies on their own will not be sufficient to make generalisable conclusions about the external effectiveness of the EU in relation to data protection, and so in section 3.5 we conclude with a wider discussion of the EU's effectiveness.

3.2 EU data protection goals

This section provides an overview of the EU's key meso-level goals in the data protection domain. It begins with an outline of six key goals which have played an important role in the EU's approach to data protection for much or all of the period under review, from 1980. These goals have been identified through a review of key primary sources, including (i) the core legal instruments (the DPD and the GDPR), (ii) the EU treaties, (iii) Commission proposals, Communications and impact assessments, and (iv) CJEU judgments. The initial overview of the six key goals is followed by a discussion of the way in which these goals, and their prioritisation by the EU, have evolved over time.

3.2.1 Summary of key goals

There has been a significant degree of continuity in the six goals listed below. Most have been a feature of the EU's approach to data protection since before the DPD was enacted in 1995. The first two have been particularly foundational; they stretch back to the earliest intra-EU debates about data protection (Simitis 1995). The balance between them continues to evolve, but it is now clear (not least from various CJEU judgments) that the goal of protecting individuals' fundamental rights is now the foremost goal of the EU's data protection framework. The first goal, relating to the smooth functioning of the internal market, clearly focuses primarily on internal rather than external developments. Nevertheless, we retain it here because it has shaped the evolution of the other goals, and because the economic logic that ties data protection to cross-border data flows and economic activity within the EU is the same that was later applied to cross-border data flows between the EU and third countries.

1. **Contribute to the smooth functioning of the internal market.** As economic activity increasingly entails the exchange of data, data protection standards become an increasingly important factor in facilitating cross-border economic activity. Within an individual state applying common rules across its territory, data protection is no constraint on economic activity, regardless of the absolute level of protection: the same data protection standards apply on both sides of any economic transaction. However, when transactions cross international borders, then differences in data protection standards can be a drag on economic activity, in particular due to reluctance on the part of higher-protection states to transfer data to trading partners that cannot guarantee to match the same level of protection. The agreement of common data protection standards in both territories removes this problem. Freeing up cross-border economic activity in the EU in this way has been a key goal of EU data protection policy from the outset.

How should goal attainment be recognised/assessed? Goal attainment here would entail data protection not being cited (for example, by companies or Member State governments) as an obstacle to the smooth functioning of the internal market. However, given our primary focus on global governance and external actors, this goal is not at the forefront of our concerns.

2. **Protect individuals' fundamental rights.** The rationale for EU rules on data protection has never been solely economic. From early on, there has also been a political or normative motivation too, related to the upholding of individual rights that citizens enjoy with respect to their personal data. As was noted in the chapter on EU and global governance, this rights-based motivation has strengthened over time, and it is now the dominant goal of EU policy in this area, both internally and externally. Moreover, it also applies as a general principle of EU law, since the introduction of Article 16 of the Lisbon Treaty. In other words, as well as being a meso-goal in this specific domain, upholding EU citizens' data-protection rights is now also a macro-goal of the EU.

How should goal attainment be recognised/assessed? As we will see in section 3.5, this is a difficult goal to assess given how wide-ranging and open to interpretation it is. Examples of ways that effectiveness could be measured here include: changes in the behaviour of data subjects and processors; survey data; as well as evidence relating to successful enforcement action when rights are breached. In addition, because the CJEU is the ultimate guarantor of the rights contained in the EU treaties, its judgments (such as the Schrems judgments on EU-US data transfers, or the Google Spain decision on the right to be forgotten) play an important role in determining whether this goal of upholding citizens' fundamental rights has been upheld.

3. **Harmonise data protection across the EU.** The need for a strong degree of harmonisation is implicit in each of the first two goals. However, harmonisation warrants inclusion as a goal in its own right because it has been repeatedly returned to by the EU as a reason for changes to many aspects of data protection rules and, in particular, the way they are implemented. This includes EU efforts to ensure a harmonised approach towards influencing the behaviour of external actors.

How should goal attainment be recognised/assessed? Goal attainment here would entail the existence of a harmonised system of data protection (the same rules, applied in the same way) across all the EU Member States. Given our global governance focus, we are concerned in particular with harmonisation of those aspects of the system that relate to the behaviour of external actors.

4. **Facilitate external data transfers in order to boost trade.** This fourth goal effectively extends the economic logic of the first goal to the international sphere: there will be greater cross-border economic activity if data protection standards can be harmonised internationally. As we have seen in the governance chapter, this goal of aligning on data protection in order to reduce obstacles to trade shaped much of the early multilateral work in this domain; it underpinned the efforts of both the OECD and the Council of Europe in the 1980s. Arguably, one reason why the EU has been able to position itself as a global leader in data protection has been the fact that its supranational scale gave it a head start in developing a framework for dealing with cross-border data flows and economic activity. But it is worth noting that the goal of boosting trade is widely shared, and so we should be careful not to assume that any trade gains due to harmonised data protection should be attributed to the effectiveness of the EU rather than its trading partners.

How should goal attainment be recognised/assessed? Attainment of this goal would entail (i) the creation of regulatory and/or other mechanisms that facilitate cross-border transfers, and (ii) the agreement of external actors to use these mechanisms.

5. **Boost EU activity and innovation in the data economy.** This goal is distinct from the preceding, trade-related, goal and focuses on the relationship between data protection to the vibrancy of the data economy across the EU. Given that it is often argued that the EU's prioritisation of data protection hinders the development of data-intensive sectors, a modest formulation of this goal might focus on ensuring that the EU's data protection regime does not slow economic activity and innovation (relative to a counterfactual baseline). However, the EU has also put forward the more ambitious goal of using data protection as a means of increasing economic activity and innovation relative to the baseline. Given the focus of the TRIGGER project on matters of global governance, this goal is not directly relevant to our assessment of (external) effectiveness. However, it could be of indirect interest if, for example, levels of economic activity were found to determine levels of influence over other global governance actors.

How should goal attainment be recognised/assessed? Goal attainment here would be reflected in increasing levels of economic activity and innovation (measured, for example, by gross value added, employment, patents, etc) that can at least partially be attributed to the effects of the EU's data protection regime. Given the global focus of this project, goal attainment here should be assessed in relative rather than absolute terms. A modest increase in the size of the EU's data economy would not represent goal attainment if other global players recorded greater increases over the same time period.

6. **Position the EU as a driving force in global data protection standards.** The last of the six goals we are highlighting reflects the increasing confidence of the EU in projecting itself as a global leader in the governance of data protection. In the other five goals, achieving influence over other global governance actors has had instrumental value as a means to other ends, such as protecting fundamental rights or benefiting the EU economy. With this sixth goal, influence is at least partially an end in itself. (Arguably, something like this is already incorporated in the TRIGGER actorness model, via the recognition and attractiveness dimensions.) There is also a significant degree of potential overlap between this goal and the other five. If the EU were able to influence other global governance actors to behave in the ways required to achieve the other five goals, then, by definition, it would be acting as a driving force. One way of distinguishing this goal from the others is to focus on the EU's ability to influence the data protection standards that other actors adopt in non-EU contexts – for example, the data protection rules that a third-country government applies to its own citizens or that a company adopts in non-EU markets.

How should goal attainment be recognised/assessed? Attainment of this goal would entail other global governance actors adopting or applying EU data protection rules and standards elsewhere than the EU, as discussed above.

3.2.2 Evolution of goals over time

One of the earliest and clearest statements of EU goals in the area of data protection is in the Commission's 1981 Communication recommending that Member States ratify the Council of Europe's Convention 108. It contains a clear statement of three of the goals outlined above. Article 2 highlights individual rights: 'Data-protection is a necessary part of the protection of the individual. It is quite fundamental.' Article 3 focuses on the internal market: 'Approximation of data-protection is desirable so that there can be free movement of data and information across frontiers and in order to prevent unequal conditions of competition and the consequent distortion of competition in the common market.' And Article 4 points to potential economic gains: 'An approximated and assured level of data protection in the Member States will help to break down the reserve which exists in regard to data processing and to the data-processing industry.'

In 1990, when the Commission published its initial draft of the Data Protection Directive (DPD) and an accompanying communication, there were five key goals (European Commission 1990). In addition to the three included in the 1981 Communication, the 1990 Communication highlights the importance of harmonisation and the need to facilitate external transfers. Harmonisation is raised in the context of the 'diversity of national approaches' that has arisen since the 1970s, which the Commission sees as 'an obstacle to the completion of the internal market.' It continues with a passage that ties individual rights to the goal of facilitating data-driven economic (and other) activity: 'If the fundamental rights of data subjects, in particular their right to privacy, are not safeguarded at Community level, the cross-border flow of data might be impeded just when it is becoming essential to the activities of business enterprises and research bodies.' This economic rationale is stated more directly in paragraph 10 which says, 'A Community approach to the protection of individuals in relation to the processing of data is also essential to the development of the data-processing industry.'

On external transfers, the 1990 Communication highlights the twin goal of ensuring 'the protection of data subjects and the cross-border flow of personal data.' Interestingly, at this early stage, the Commission seems to view EU accession to the Council of Europe convention as being the key step for achieving this twin goal (see paragraphs 14 and 19), despite the fact that the accompanying draft directive includes Chapter VIII on the transfer of data to third countries, which introduces adequacy and related provisions that quickly became a cornerstone of the EU's efforts to shape the behaviour of external actors. In 1995, the recitals in the final text of the DPD make explicit the relationship between these cross-border transfers and the goal of expanding international trade (see recital 56).

The 1995 Directive also sees the EU's broad meso-level goals begin to be translated into more concrete institutional provisions, such as requirements relating to data subjects' consent or the lawful processing

of personal data. While these clearly entail the EU using legislative instruments to achieve its data-protection goals (see section 3.3 for a fuller list of methods used), they can also be thought of as micro-level goals that are designed to make progress on higher meso-level goals. So, for example, one of the EU's micro-goals is to ensure that personal data are (broadly speaking) only processed with the consent of the data subject. But this goal is not an end in itself. Rather, it operationalises the meso-level goal of protecting the individual's fundamental rights relating to their personal data. The idea is that success – in our terms, effectiveness – on the (micro) consent goal will contribute to success on the (meso) fundamental rights goal.

There was a significant evolution in the EU's data protection goals in the early years of the 2000s. The Charter of Fundamental Rights of the European Union formally declared data protection to be a fundamental right in 2000 (see Article 8). Agreed in 2007, the Treaty of Lisbon made the Charter legally binding, and it also brought data protection into the EU treaties themselves. It did so in such a way as to shift the balance of the EU's goals in this area decisively towards fundamental rights having priority over other data protection goals. Article 16.1 states simply: 'Everyone has the right to the protection of personal data concerning them.' This made achievement of the rights-related goal a general principle of EU law.

The next milestone in the evolution of the EU's goals is the 2010 Communication which began the legislative process that would result in the GDPR six years later (European Commission 2010). Reflecting major technological and economics changes since 1995, this 2010 document marks an inflection point in terms of the centrality of global considerations in the EU's data protection regime. 'Addressing globalisation and improving international data transfers' is one of the issues highlighted in a review of how the DPD has been functioning. When the Communication reflects on the implications of the Lisbon Treaty, it states explicitly that citizens' fundamental data protection rights have implications that stretch into the global governance arena, outside the borders of the EU. It says that, 'The above challenges require the EU to develop a comprehensive and coherent approach guaranteeing that the fundamental right to data protection for individuals is fully respected *within the EU and beyond*' (ibid. p. 4) In the same vein, the Communication is very direct in asserting the sixth goal described in section 3.2.1. It notes that an instrument like the GDPR will be 'the best way of endorsing and promoting EU data protection standards globally.' Under a heading about the 'global dimension' of data protection, the Communication highlights two objectives: (i) clarifying and simplifying the rules for international data transfers that were introduced in the DPD, and (ii) promoting universal data protection principles by working through a range of international channels (bilateral, multilateral, standards bodies, etc). The Communication also calls for the role of the DPAs to be strengthened, particularly in the area of dealing with multinationals that have operations in multiple Member States.

In 2012, the Commission followed up on the 2010 Communication by publishing its proposed text for the GDPR, as well as an impact assessment (European Commission 2012b). In terms of the EU's goals, the proposed text does not contain much new. However, it does restate prominently the goal from 1981

and 1990 of using data protection to encourage economic activity, with the difference that in 2012 the concept of trust is introduced as part of the explanation of how this would work: consumer trust is needed to underpin innovation in new data-reliant products and services, and high levels of data protection are the way to build that trust (ibid. p.18). The impact assessment lists three policy objectives for the proposed GDPR, none of which is directly or primarily related with global governance considerations: (i) enhancing the internal market dimension of data protection, (ii) increasing the effectiveness of the fundamental right to data protection, and (iii) establishing a comprehensive and coherent EU data protection framework. However, earlier in the document, when the overarching policy problems are being outlined, two of the factors mentioned have potential relevance to global governance goals. The first of these relates to data transfers with third countries, which is considered here as part of a harmonisation problem: the impact assessment notes that national fragmentation under the DPD means that in some cases a transfer might be deemed legal in one Member State but not in another (European Commission 2012a, p.16). The second factor relates to inconsistent enforcement, due in particular to wide variation in the national funding allocated to DPAs (ibid. p.19). This is not an external issue per se, but as noted above it has a direct bearing on the treatment of multinationals with operations in multiple states.

Between the 2012 GDPR proposal and the agreement of the final text of the regulation in 2016, the key developments were at the CJEU, which confirmed that the inclusion of data protection in the treaties as a fundamental right meant that rights protection now took precedence over other EU goals in this area. The court's 2014 Google Spain ruling on the right to be forgotten emphasised the primacy of the fundamental rights aspect of data protection, explicitly noting that the individual's privacy rights override the economic interests of the data controller. A year later, the Schrems I decision on EU-US data transfers was more directly related to external, global governance considerations. While the court notes that two of the EU's data protection goals are particularly relevant for international transfers (the individual's fundamental right to data protection, and the encouragement of international trade), in paragraph 48 of the judgment it states in effect that the goal of boosting trade must be subordinated to the goal of upholding fundamental rights, reaffirming recital 57 of the DPD which says that transfers to third countries are prohibited where adequate levels of data protection are not ensured.

When the full text of the GDPR was agreed in 2016, it consolidated the evolution of the goals as discussed above. This is particularly clear in the recitals. The primacy of the fundamental rights goal is reflected in recital 1. The need for greater harmonisation is reflected in recitals 3 and 10, and then given institutional expression in aspects of the new DPA regime, including the 'one-stop shop' and 'consistency mechanism', which form one of our case studies in section 3.4, below. Recital 6 covers the goal of facilitating international transfers with third countries. The role of data protection in securing the internal market is highlighted in recital 13. The goal of expanding trade is included in recital 101.

One notable development in the years since the GDPR was adopted has been a growing focus on the goal of positioning the EU as a global leader on data protection standards. This is particularly clear in

the Commission's 2017 Communication on exchanging and protecting personal data in a globalised world (European Commission 2017). This reiterates relevant provisions or objectives of the GDPR, such as harmonisation of rules and enforcement, or clarification of the system for third-country transfers. It also highlights the role that adequacy agreements can play in easing trade negotiations or 'amplifying the benefits' of existing trade agreements. But of particular interest is the emphasis the document places on bilateral and multilateral dialogue as a means of promoting international convergence on data protection standards that are broadly aligned with the EU. The 2017 Communication lists numerous countries and organisations, but it gives pride of place to the Council of Europe's Convention 108, on the basis that it is 'the only binding multilateral instrument in the area of data protection' and that after revisions then under way, it 'will reflect the same principles as those enshrined in the new EU data protection rules.' (The revised Council of Europe Convention is the subject of the second case study in section 3.4.) Two years later, in an update on the GDPR one year after it came into force, the Commission again reiterated the goal of intensifying international cooperation on data protection, and moots the creation by like-minded countries of a 'multinational framework' for data protection, building on the CoE Convention (European Commission 2019). In 2020, the Commission published another review of the GDPR (European Commission 2020b). It restates the main goals of the GDPR as discussed above, and it displays significant confidence that progress is already being made on the goal of positioning the EU as a global leader. The 2020 review also reframes the rationale of the GDPR in more ambitious and all-encompassing terms than earlier documents: 'The ultimate objective of the GDPR is to change the culture and behaviour of all actors involved for the benefit of the individuals.'

3.3 How has the EU sought to attain these goals?

In section 3.4 of this chapter, we will examine two case studies of the EU in action in the field of data protection policy, with a view to establishing what its specific goals were, how it went about achieving them, and how effective it was. First, we here take a step back to provide a broader overview of the main methods or channels that the EU has used to advance its data protection global governance goals, from the following list of modes of global engagement:

- **Unilateral rule-setting.** The EU adopts policies and strategies and requires other global governance actors to comply with them (typically as the price for market access).
- **Example-setting.** This category reflects the exercise of soft power rather than the harder market or regulatory power of the previous category. It again involves the EU adopting its own policies and strategies, but other actors decide on uptake.
- **Participation with international governmental organisations.** The EU works with international organisations in a variety of ways: as exclusive representative of the Member States, as a special observer (e.g. in the UN), and sometimes through specific EU institutions, such as agencies.

- **Participation in European regional organisations.** The EU works with a patchwork of regional organisations – such as the CEPT, the Council of Europe or the OSCE – that have broader membership than the EU.
- **Cooperation with other regional organisations and institutions.** Examples include other regional blocs (e.g. ASEAN, MERCOSUR, ECOWAS, EAC and COMESA), multilateral development banks (as counterparts to the EIB), and other central banks (as counterparts to the ECB).
- **Participation with standardisation bodies.** The EU interacts with many of the private regulatory bodies (such as the IEC and the ISO) and transnational private regulatory initiatives (including the Global Reporting Initiative, and the Forest and Marine Stewardship Councils) that now shape global rules.
- **Participation in plurilateral and minilateral organisations.** Examples include standard-setting and policy debate within the OECD, as well as EU membership of the G7 and involvement with ad hoc groups, such as the GPAI for artificial intelligence.
- **Rulemaking through bilateral negotiations.** The exclusive competence to negotiate trade agreements provides important global governance leverage for the EU, but it also uses bilateral ad hoc mechanisms, such as the adequacy regime in data protection.
- **Other forms of international regulatory cooperation.** The EU is also involved in a dense network of international regulatory cooperation relationships, as defined by the OECD in its taxonomy.

In the field of data protection, four of these nine strategies have been used. First, as noted above, the system of adequacy decisions that has been at the heart of the EU data protection regime since the DPD in 1995 is an example of relying on bilateral negotiations. Second, unilateral rule-setting is explicit in a number of areas, such as the extraterritoriality provisions in both the DPD and GDPR. More broadly, the EU requires 'essentially equivalent' data protection to be in place before third-country data transfers can take place, but it is agnostic on the method used to achieve this equivalence: it could be through country-level bilateral adequacy negotiations, or through enterprise-level use of standard contractual clauses (SCCs). Third, there is evidence of example setting and soft power in the voluntary adoption of EU rules and practices, either by private-sector actors (such as Microsoft's extension of GDPR principles across its global operations) or by third countries (such as the influence of the GDPR on the growing number of data protection laws that have been drafted in recent years). Finally, engagement with European regional organisations – the Council of Europe in particular – has been an important aspect of the EU's approach to data protection global governance. As discussed in the chapter on the evolution of EU and global governance, the CoE was an important influence on the initial development of its core data protection principles. More recently, however, the EU has used the revision of Convention 108 as a means of extending the reach of key rules and principles contained in the GDPR. It is worth noting that Convention 108+ has plurilateral as well as regional characteristics, by virtue of the fact that it is open to signatories outside of Europe.

3.4 Two case studies

In this section we discuss two case studies that show the EU in action as it seeks to influence other actors in the data protection domain. The objective here is to show how the meso-level goals discussed in section 3.2 and the strategic preferences highlighted in section 3.3 can be operationalised in concrete global governance settings.

It is clear from the earlier chapter on the history of EU and global governance that there are numerous points of engagement between the EU and other global governance actors which could serve as case studies. Obviously, therefore, the two we have chosen are designed to be illustrative rather than comprehensive. The first of our case studies is the Privacy Shield framework, which is a key example of bilateral negotiations, affecting the EU's most important bilateral economic relationship. The second case study is the Council of Europe's revision of Convention 108, which forms an important plank in the EU's efforts to propagate its approach to data protection globally. After discussing these case studies, we will turn to a wider discussion of the EU's effectiveness in section 3.5.

3.4.1 Case study 1: Privacy Shield

The European Commission's goal in its negotiations with the US on the Privacy Shield framework was relatively straightforward and reflected the circumstances that had led to the need for negotiations. In October 2015, the CJEU had struck down the Safe Harbor framework that had underpinned EU-US data transfers since 2000, on the basis that it failed to provide sufficiently robust data protection standards in the US. The Commission's immediate micro-level goal in the Privacy Shield negotiations was therefore clear: to agree on a revised framework for EU-US data transfers which would meet the threshold set down by the CJEU, namely that data transferred outside the EU be subject to protections 'essentially equivalent' to those applying within the EU. This goal is directly related to the meso goals discussed in section 3.2. However, the ultimate objective of the micro-level Privacy Shield goal is not to achieve one of the meso goals, but to find a durable balance between two of them: upholding the fundamental rights of EU citizens and facilitating increased trade. Although it lasted for 15 years, Safe Harbor failed to achieve this balance in a manner consistent with the EU treaties. Moreover, in its Safe Harbor judgment, the CJEU clarified that the weighing of these goals was not a matter of Commission discretion. The protection of rights takes precedence over the promotion of trade, and so any successor agreement to Safe Harbor would have to deliver a sufficient increase in data protection standards on the US side to satisfy the CJEU.

The underlying structure of the negotiations over both Safe Harbor and Privacy Shield reflects the significant divergences between the EU and the US approaches to data protection, as well as the fact that neither party enjoyed the negotiating power to insist that the other bend to its will. Both Safe Harbor

and Privacy Shield embody a hybrid approach where the Commission's assessment of adequacy focuses not on the US domestic framework, but on a separate negotiated framework to which US companies can voluntarily sign up. The need for such a *sui generis* bilateral agreement on data protection stems from the twin facts that (i) the US's domestic data protection framework would not meet the EU's adequacy standard, and (ii) unlike some smaller economies, the US would not tailor its domestic regulatory framework as the price of guaranteeing EU-US data transfers. In other words, while the idea of 'market power Europe' has considerable salience in the field of data protection, it bumps up against important limits in negotiations with a counterparty as large and powerful as the US (Terpan 2018).

While the US begins from a position of strength, being able to insist on an adequacy workaround, Farrell (Farrell 2002) points out that in relation to the Safe Harbor process, once negotiations begin the EU enjoys certain structural advantages. Farrell distinguishes between three negotiating arenas in the transatlantic process: talks between Commission negotiators and their US interlocutors (Arena 1), internal debates in the US between different data protection actors (Arena 2) and similar intra-EU debates with relevant actors including other EU institutions (Arena 3). For the Commission, Safe Harbor negotiations entailed shuttling between the first and third arenas, with the result, according to Farrell, that 'the obduracy of actors with veto power within the European Union strengthened [the Commission's] bargaining hand with the Americans.' By the time we reached the Privacy Shield negotiations, this multi-arena dynamic had been intensified by the CJEU's decision in the Schrems I case to strike down Safe Harbor. To use Farrell's terms, the CJEU was an obdurate EU actor that had exercised its veto power. The onus was therefore now squarely on the US to provide additional assurances if it wished to maintain an adequacy workaround with the EU. This meant that the EU went into the Privacy Shield negotiations with its negotiating hand 'immeasurably strengthened' (Schwartz and Peifer 2017). In the words of one of the Commission negotiators: 'There was clearly a pre- and post- Schrems judgment. I felt as a negotiator, that there was much more solidarity and cohesion amongst the EU after the Schrems judgment. That's not because people all of a sudden fell in love with data protection. But it was objectivised in a certain sense. There were requirements, criteria to meet' (Farrell and Newman 2019).

Given this new focus and unity of purpose that the Schrems judgment had created on the Commission side, it is unsurprising that US negotiators were unsuccessful in their early attempts to persuade the EU that the CJEU had been misguided in Schrems and that the US did in fact provide equivalent levels of data protection to the EU. Substantive negotiations therefore ensued, and a first iteration of the Privacy Shield framework was announced quite swiftly in February 2016. The key changes with respect to the predecessor agreement all represented US concessions, including:

- a strengthened monitoring and enforcement system, with clear sanctions for non-compliance;
- authority for EU DPAs to follow up on unresolved complaints with US authorities;
- a dispute settlement mechanism;
- a new ombudsman, to whom EU citizens could complain if they felt US intelligence services had compromised their privacy.

For many actors on the European side, and notably the DPAs and the European Parliament, these concessions did not go far enough (Farrell and Newman 2019). Criticism of the draft crystallised in April 2016, when the Article 29 Working Party (WP29, which is made up of the national DPAs) published a highly critical assessment of the new framework. This assessment stated that despite 'the improvements offered by the Privacy Shield, the WP29 considers that some key data protection principles as outlined in European law are not reflected in the draft adequacy decision and the annexes, or have been inadequately substituted by alternative notions' (Article 29 Data Protection Working Party 2016). The deficiencies related, inter alia, to data retention, purpose limitation, onward transfers of data from the US, the complexity of redress provisions, and continuing concerns about national security derogations. US negotiators were reluctant to reopen and revise the draft in response to these criticisms (Weiss and Archick 2016). However, pressure from EU actors in Arena 3 was further ratcheted up in May 2016, with a European Parliament resolution dismissing the draft framework as insufficient, and a statement from the European Data Protection Supervisor that it was 'not robust enough to withstand future legal scrutiny before the Court' (Farrell and Newman 2019). This led to a number of further changes in the agreement before it was finalised, including a concession from the US that the ombudsman role would be filled by a senior official from the State Department and not from the intelligence services. These final changes were sufficient to conclude negotiations and on 12 July 2016, the Commission adopted the Privacy Shield framework and it entered into force with immediate effect (European Commission 2016).

We turn now to the question of how effective the EU was in its negotiation of the Privacy Shield. On the face of it, the EU had a successful negotiation, with input from a range of actors on the EU side combining to secure a range of data protection concessions from the US relative to the Safe Harbor *status quo ante*. Ultimately, however, the negotiation must be seen as a failure on the terms set out above, where we stated that the goal was to agree a revised framework that would meet the threshold set down by the CJEU in the Schrems I judgment. It was certainly the hope of the Commission that it had done enough to meet this threshold, but that is not for the Commission to determine. It is a call that only the CJEU can make decisively. It did so in July 2020, in the Schrems II case, where it struck down the Privacy Shield framework. In essence, the CJEU ruled that the Commission had departed too far from upholding the second meso-goal of protecting citizens' fundamental rights. The Commission therefore had not been effective. It had not achieved its goal of reaching an agreement with the US that balanced the goals of protecting rights and promoting trade in a way that would satisfy the CJEU.

Moreover, this failure to achieve the Privacy Shield micro-goal has potential lasting implications for the EU's future pursuit of the two meso goals of protecting individual rights and expanding international trade. In twice striking down data protection arrangements underpinning the deep economic interlinkages between the EU and the US, first Safe Harbor and then Privacy Shield, the CJEU has left no room for ambiguity as to the relative importance of these two meso goals. Citizens' fundamental rights, as set down in the treaties, enjoy clear priority and cannot be traded off against trade or economic gains.

3.4.2 Case study 2: Council of Europe modernisation of Convention 108

Our second case study is the revision process that led to the Council of Europe's adoption of a modernised revision of Convention 108 (hereafter C108+) in 2018. Building on decades of interaction between the CoE and the EU on data protection, the EU was active in this revision process. For example, in the Ad Hoc Committee on Data Protection (CAHDATA) that was responsible for finalising C108+, the list of participants included three representatives from the Commission and one each from the Council, the Parliament, the EDPS and the EU Delegation to the CoE (Council of Europe Ad Hoc Committee on Data Protection 2016a). This is in addition to the Member States' CoE representatives, many of whom were the same individuals handling negotiations on the GDPR in Brussels, which were taking place at the same time.

One of the EU's goals in relation to C108+ was to ensure its alignment with the new GDPR framework that was being put in place at the same time. This clearly falls under the remit of the sixth meso-goal discussed earlier, of positioning the EU as a driving force in the global evolution of data protection governance. In its 2017 Communication on 'Exchanging and Protecting Personal Data in a Globalised World' the Commission noted that C108+ 'will reflect the same principles as those enshrined in the new EU data protection rules and thus contribute to the convergence towards a set of high data protection standards' (European Commission 2017). Perhaps the clearest evidence of the EU's goal of alignment is in a pre-final version of C108+ from 2016, which includes a number of reservations – issues that remain to be finalised – accompanied by the following annotation: 'Reservation of the European Union in order to ensure consistency with the European Union reform' (Council of Europe Ad Hoc Committee on Data Protection 2016b; Greenleaf 2016).

Was the goal of alignment between C108+ and GDPR achieved? While there are clear differences between the two, there is broad consensus that C108+ captures many key GDPR principles. Graham Greenleaf, who has done more than most to track the evolution of data protection rules across the world, has referred to C108+ as 'GDPR Lite' and as a mid-point between the original C108 and the GDPR (Greenleaf 2016; 2021). Elsewhere, Greenleaf provides a useful summary of the points of commonality and difference between the two frameworks (Greenleaf 2018b). He first lists 13 new elements in C108+ that correspond to important elements of the GDPR:

1. Proportionality required in all aspects of processing
2. Stronger consent requirements ('unambiguous' etc)
3. Greater transparency of processing
4. Some Mandatory Data Protection Impact Assessments (DPIAs)
5. Limits on automated decision-making, including the right to know processing logic (was also in EU Directive)
6. Data protection by design and by default
7. Biometric and genetic data require extra protection
8. Right to object to processing on legitimate grounds (also in directive)
9. Direct liability for processors as well as controllers

10. Data breach notification to DPA required for serious breaches
11. DPAs to make decisions and issue administrative sanctions/remedies
12. Demonstrable accountability required of data controllers
13. Parties must allow and assist evaluation of effectiveness.

And he then lists nine new principles in the GDPR which are not explicitly included in C108+, although he concedes that they may be implied by C108+:

1. Obligations to apply extra-territorially, if goods or services offered, or behaviour monitored locally
2. Local representation required of such foreign controllers or processors
3. Right to portability of data-subject-generated content
4. Right to erasure/de-linking (right 'to be forgotten')
5. Mandatory Data Protection Officers (DPOs) for sensitive processing
6. Data breach notification (DBN) to data subjects (if high risk)
7. Representative actions before DPAs/courts by public interest privacy groups
8. Maximum administrative fines based on global annual turnover
9. Requirement to cooperate in resolving complaints with international elements, with any other DPA (as distinct from 108+ members).

Greenleaf was writing in 2018 and he noted that it was too early to gauge definitively the significance of the gaps between C108+ and the GDPR. This remains the case. Broadly speaking, however, it is reasonable to conclude that the EU's goal of aligning C108+ with the GDPR has been achieved to a significant degree. As Greenleaf notes, C108+ 'includes the most important GDPR innovations'. Given that recital 105 of the GDPR already singles out third countries' compliance with the original C108 as something to be 'taken into account' when an adequacy decision is being made, it is likely that compliance with C108+ will come close to meeting the EU's adequacy requirements (Greenleaf 2018a, 5). However, the strong line taken by the CJEU on the need for adequacy to be underpinned by 'essentially equivalent' protections suggests that C108+ compliance on its own may not suffice.

What can we say about the EU's effectiveness in the C108+ process? It is important to note at this point that the goal of aligning C108+ and GDPR was not unique to the EU. It was also shared by the Council of Europe, which synchronised the revision of C108 with the EU's legislative process precisely to ensure 'consistency between both frameworks' (De Terwangne 2021). The fact that the goal of C108+/GDPR alignment was mutual highlights the causal complications that bedevil assessments of effectiveness, as mentioned in the introduction to this chapter. It is not enough to show that a goal has been achieved. Demonstrating effectiveness also means attributing responsibility for goal-achievement. In the context of C108+, even if we conclude that the EU's goal of alignment has been achieved, the default assumption must be that this is as much a reflection of CoE effectiveness as EU effectiveness.

A similar point can be made about the way in which this case study relates to the six data EU protection meso goals discussed in section 3.2. On the one hand, the EU micro-goal of C108+ alignment contributes clearly to the sixth meso-goal, by amplifying and extending the reach of the EU's data protection principles. A crucial difference between C108+ and the GDPR is that non-EU states can accede to the former, giving it potentially global reach (Mantelero 2021). On the other hand, it is reductive in this context to refer too narrowly to EU data protection principles being amplified, as if these principles represent a concession that the EU is seeking to win from the CoE. As we discussed in the chapter on the evolution of EU and global data protection governance, the histories of the CoE and EU in this field are deeply intertwined, and the CoE was an important early inspiration for many of the key principles that have become central in the EU's data protection framework (Bygrave 2020). In important respects, 'EU data protection principles' already have key 'CoE data protection principles' baked in. Against this backdrop of decades-long cooperation and consensus between the EU and CoE, it would be churlish to claim that C108+ exclusively spotlights the EU as a global leader. Perhaps better here to suggest that C108+ reflects what Bygrave describes as a process of global data protection governance being 'Europeanised' by both the CoE and the EU (Bygrave 2020).

The alignment of C108+ and GDPR is a win-win outcome for the EU and CoE, and there may be lessons here for the way we think about the actorness and effectiveness concepts more broadly. In the absence of shared global norms or institutions for data protection governance, it is easy to see actorness and effectiveness in zero-sum terms. Given current geopolitical and geoeconomic trends, this is particularly true when it comes to comparing the actorness and effectiveness of the EU, the US and China. What the C108+ process highlights is the possibility of alternative positive-sum dynamics: when actors' goals are shared, their effectiveness is mutually reinforcing. The metaphor is no longer one of a bicycle race between two competitors seeking relative advantage, but one of two partners on a tandem sharing the work of moving forward.

3.5 Discussion

The case studies in the preceding section provide two snapshots of EU effectiveness in concrete negotiation contexts. They present a mixed picture of EU effectiveness: failure to secure a durable underpinning for EU-US transfers, but success – shared with the Council of Europe – in amplifying key elements of the GDPR framework via C108+. However, the two case studies cannot be taken as representative of the EU's overall effectiveness in achieving its data protection goals. For that reason, in this final section of the chapter we return to the EU's six meso goals for data protection, with a view to providing a high-level assessment of how effective the EU has been at achieving each of them.

3.5.1 Contribute to the smooth functioning of the internal market

This goal is not a priority for our purposes, given that it focuses on intra-EU considerations rather than the external, global governance considerations that we wish to assess. That said, it should be noted that

the EU's early experience at dealing with cross-border data flows within the EU was a very important factor in positioning it to be a regulatory front-runner when global cross-border data flows became increasingly economically significant. We therefore note in passing our assessment that the EU has displayed a high level of effectiveness in ensuring that data protection considerations do not inhibit the functioning of the internal market. From a position in the 1980s where the existence of two groups of Member States, with and without national data protection laws, threatened to undermine cross-border data flows, the EU has stewarded this policy domain so that the shared provisions of the GDPR apply directly across the bloc, without the need for implementing national legislation. In other words, the goal has been achieved, and the EU has been instrumental in its being achieved. This is our definition of effectiveness. The Commission's review of the GDPR after two years in force summarises the situation fairly: 'By creating a harmonised framework for the protection of personal data, the GDPR ensures that all actors in the internal market are bound by the same rules and benefit from the same opportunities' (European Commission 2020c). It is also worth noting that other relevant provisions are evolving in the same way, such as the ePrivacy directive which is in line to be replaced by a regulation. However, there are potential caveats here. This internal market goal should be considered alongside the harmonisation goal below, because continuing problems with the fragmentation of implementation across Member States have the potential to become a source of tension or friction within the internal market.

3.5.2 Protect individuals' fundamental rights

This is perhaps the most important of the six meso goals, given its explicit inclusion in the treaties and the fact that the CJEU has repeatedly attached the highest priority to it. While it has strong internal dimensions, its relevance to the EU's external influence and effectiveness should not be overlooked. Protecting citizens' data protection rights is neutral as to whether those rights are threatened by EU or non-EU actors, and the commercial dominance of some non-EU data processors means that they have significant potential to affect EU citizens' rights. We saw this dynamic clearly in the second case study above, where the CJEU was concerned with the protections being offered to EU citizens against possible infringements by US-based data processors.

This is a difficult goal to assess. We will consider a number of different possible sources of evidence. The first of these is GDPR compliance and enforcement, where the record is, at best, mixed. On the third anniversary of the GDPR taking force, the IAPP's summary of its impact noted that '47 % of companies now self-report as fully compliant with GDPR' (International Association of Privacy Professionals (IAPP) 2021). After three years, it is striking that more than half of companies do not self-report full compliance. Across the EU there have been around 700 enforcement actions since the GDPR came into force, with a total of EUR 280 million in fines and eight individual fines in excess of EUR 10 million[25]. Most of these fines relate to breaches of core principles, which does not suggest that the fundamental principles of data protection are being internalised by all actors. It is also important to note that there are stark national differences in the distribution of these enforcement actions across the

[25] See www.enforcementtracker.com

EU. For example, 230 relate to Spain, compared to 30 in Germany and just 7 in Ireland. This kind of discrepancy highlights an issue that we have noted repeatedly in this deep dive: the relative autonomy of the national DPAs is a source of potential weakness as far as the uniform implementation of data protection across the EU is concerned. Moreover, the fact that Ireland has recorded so few enforcement actions is of particular interest to this project, given our focus on the EU's engagement with, and influence over, external actors. The Irish DPA is responsible for regulating the EU operations of many of the foreign-owned technology giants. So, the low number of enforcement actions in Ireland suggests that enforcement may be at its weakest precisely at the point where the EU interacts most intensively with key external actors.

A second potential indicator of fundamental rights being protected is individuals' awareness of their data protection rights. This point features prominently in the Commission's two-year review of the GDPR, which cites survey evidence showing, among other things, that 69 % of the population is aware of the GDPR and 71 % is aware of their national DPA (European Commission 2020c). Unfortunately, the details of whether and how these rights are being exercised are fuzzier. The Commission notes that 'organisations have put in place a variety of measures to facilitate the exercise of data subjects' rights' but it also lists seven areas where improvements are needed to ensure that individuals can exercise their rights. The Commission does not make clear what proportion of organisations are actively enabling individuals to exercise their rights, nor what proportion of organisations fall under one of the seven areas where progress is required. A Dutch study of perceptions and attitudes towards the GDPR enrichens the picture considerably (Strycharz, Ausloos, and Helberger 2020). The authors note that their respondents' awareness of the GDPR is not matched by 'knowledge and understanding of the actual provisions'. This calls into question the extent to which awareness of the GDPR can be taken as a proxy for awareness of – let alone the exercising of – the rights it confers on individuals. In addition, the research points to significant public scepticism about the impetus for the GDPR, with almost a quarter of respondents saying that it had been imposed from above without public participation. Respondents also highlighted a range of frustrations with the GDPR, including minorities reporting that it had negatively affected their personal lives (13 %) or professional lives (14 %).

A third means of assessing the impact on individual rights is to look at whether online behaviour changed following the introduction of the GDPR. Empirical research suggests that user behaviour has changed. For example, one study focusing on the online travel sector points to a 12.5 % drop in the number of consumers across the sector 'as a result of the new opt-in requirement of GDPR' (Aridor, Che, and Salz 2020). We can assume that this reflects individuals' responses to the 'massive compliance and consent activities' by data processors that the GDPR triggered (Sørensen and Kosta 2019). Such changes in the behaviour of both processors and users represent prima facie evidence in support of a key philosophical underpinning of the EU's data protection regime, namely that users' consent should determine whether and how personal data are processed. However, against this should be set a growing body of research that critiques the EU's emphasis on consent as a primary means of achieving the key goal of protecting individuals' rights. We can distinguish two important categories of criticism here. One

focuses on the volume and opacity of the consent notices with which users are now routinely confronted. It argues that what results is often not informed consent but unreflective box-ticking, or what Utz et al (2019) describe as the 'habit to click any interaction element that causes the notice to go away instead of actively engaging with it and making an informed choice'. Solove (2012) refers to this as the 'consent dilemma,' while Richards and Hartzog (2015) suggest that, 'Consent via the fine print of a legal agreement no one reads is disloyal and illegitimate'. The second strand of criticism of the consent framework highlights the manner in which some data processors manipulate users in order to secure their consent. A study by the Norwegian Consumer Council, entitled Deceived by Design, highlights companies use of 'dark patterns' including default settings and other features that steer users to give their consent to privacy intrusions (Norwegian Consumer Council 2018). Another study concludes that 'dark patterns and implied consent are ubiquitous' and highlights how simple design changes can have a dramatic effect on user consent (Nouwens et al. 2020). For example, removing the 'reject all' button from the first page a user encounters on a website causes consent to increase by 22-23 percentage points.

It is beyond the scope of this chapter to weigh all the diverse and contested evidence relating to the effect of EU law on individuals' fundamental rights and come to a precise assessment of the EU's effectiveness in achieving its goals in this area. That would require a much more detailed analysis than is possible here. For the moment, an assessment of 'partly effective' will have to suffice. While the EU has raised individuals' awareness of their data protection rights and created a legal framework designed to ensure that data processors uphold those rights, compliance with this framework is weak and a potentially significant proportion of data processors may be actively gaming the system. Given the quasi-constitutional status of data protection rights across the EU, this should be of significant concern.

3.5.3 Harmonise data protection across the EU

Effectiveness on this meso-goal would entail the same data protection rules being applied in the same way across all EU Member States. On the face of it, this is very much an internal goal rather than one concerned with external influence and global governance. However, in practice this goal is increasingly intertwined with external considerations: as we shall see, one of the key areas where divergence and dissent has been growing is precisely in relation to the regulation of external actors.

Overall, there is a strong case to be made for the EU being highly effective in terms of achieving consensus and harmonisation. As we have noted in previous chapters, since the 1980s there has been a steady evolution towards increased harmonisation, particularly with the progression from patchy national frameworks to the DPD and then the GDPR. One useful way of approaching the question of EU effectiveness is to consider the counterfactual: what would the position be in the absence of any EU action? On some of the meso goals, it is possible that significant progress would have been made in the counterfactual scenario. On harmonisation, however, it is surely the case that progress would have been much weaker without the EU institutions exerting the centripetal force necessary to pull up to 28 countries into a high degree of alignment.

Notwithstanding this baseline of high EU effectiveness at delivering harmonisation, fragmentation remains. We have noted it repeatedly in previous chapters. This is particularly true of the role played by the national DPAs, which allows significant divergences to emerge in the way the EU's common rules are enforced. This problem is exacerbated by the one-stop shop approach to cross-border cases, leading to potential tensions between DPAs if they disagree over how a case should be handled. Importantly for our concern with the EU's engagement with external actors, one of the most likely triggers for such tensions between DPAs is the regulation of foreign-owned data processors with operations in the EU, more often than not by Ireland's DPA, which has come under repeated criticism for its light-touch approach. This criticism erupted publicly in early 2021, when Germany's Federal Commissioner for Data Protection and Freedom of Information called out the Irish DPA for its 'extremely slow case handling, which falls significantly behind the case handling progress of most EU and especially German supervisors' (Espinoza 2021). Further evidence of these tensions emerged when Hamburg's supervisory authority for data protection triggered the 'urgency procedures' of GDPR Article 66, adopting its own provisional measures towards Facebook because, in its view, the Irish DPA had failed to respond adequately to changes in the terms of service and privacy policy of WhatsApp, which is owned by Facebook (European Data Protection Board 2021). While a subsequent binding decision by the EDPB concluded that 'the conditions to demonstrate the existence of an infringement and an urgency are not met', this incident points to a potentially destabilising breakdown of trust in parts of the EU's decentralised architecture of data protection enforcement. Another example of this fraying of harmonisation is the leaking in April 2021 of a draft European Parliament resolution highly critical of the Irish DPA (Tene 2021).

On digital policy more broadly, the European Commission has sought to emphasise the need for collective EU action to vouchsafe Europe's digital sovereignty (European Commission 2020a). Among many other things, this is likely to entail Commission vigilance in relation to fragmentation in the data protection domain. With this in mind, in the Commission's two-year review of the implementation of the GDPR, it is noteworthy how much attention is given to ongoing harmonisation problems. On cross-border cases in particular, the review notes the need for a more 'efficient and harmonised' system, and acknowledges that numerous stakeholders have raised fragmentation as a concern (European Commission 2020c). However, in addition to efforts to ensure a common EU approach to digital policy, there are also counter-currents which seek to re-assert national prerogatives. For example, in negotiations over the forthcoming Digital Services Act, France has expressed its unhappiness with the one-stop shop approach to digital regulation across the EU and has called for each Member State to have the right to regulate technology companies within its territory (Espinoza and Abboud 2021).

3.5.4 Facilitate external data transfers in order to boost trade

Gauging the EU's effectiveness on this goal is problematic, because the goal itself is problematic. Its logic seems to be that the EU's data protection framework provides a set of criteria that give third countries clarity on the data protection standards that must be upheld in order to trade with the EU.

However, in this scenario it is not the EU rules that facilitate trade, but the third countries' compliance with those rules. That being so, this goal is perhaps subordinate to the sixth goal, below, which focuses on the extent to which the EU can project its rules internationally.

On the face of it, this fourth goal runs counter to economic logic, which suggests that imposing regulatory thresholds at the border will inhibit rather than boost trade. This is confirmed by economic analysis of the trade effects of data protection rules. For example, Ferracane and Van der Marel (2019) note that, 'more restrictive data policies, in particular with respect to the cross-border movement of data, result in lower imports in data-intense services for countries imposing them'. Similarly, the language used by Pasadilla et al. (2020) suggests how far they are from agreeing that the GDPR boosts trade: 'While the GDPR does not expressly prohibit cross-border data flows, the compliance cost can become prohibitive for many small businesses'. More generally, Greenleaf (Greenleaf 2018a) notes a pattern of emerging tension between the obligations contained in free trade agreements and in international data protection agreements.

There is an interesting relationship between this meso-goal and the attractiveness dimension of actorness as defined and discussed in the last chapter. One of the core elements of the attractiveness dimension is the idea that economic incentives (such as the prospect of trade with the EU's huge market) are one of the ways in which the EU is able to influence external actors to align with its rules. The causal chain here is intuitive: the prospect of increased trade leads to compliance with EU rules. By contrast, this fourth meso-goal turns things around very counter-intuitively, suggesting that EU rules lead to increased trade. On these terms, it is difficult to conclude that the EU has been effective. Moreover, the EU's failure thus far to agree a durable basis for data transfers with the US highlight the fact that there is no guarantee that prospective trading partners will sign up to all aspects of the EU's data protection framework.

3.5.5 Boost EU activity and innovation in the data economy

As with the previous trade-related goal, this fifth goal is also challenging. Widespread anecdotal evidence highlights concerns in data-intensive sectors – such as machine learning – that the EU's high data protection standards are more likely to inhibit rather than promote economic activity. Countering such concerns is an important element of the EU's evolving data strategy, which seeks to use innovations such as sectoral 'data spaces' to provide the private sector with the scale of data it requires without compromising on data protection (European Commission 2020a). Until these developments bear fruit, however, it seems optimistic to expect the EU's data protection framework to boost economic activity. When assessing the fundamental rights goal, we considered evidence pointing to a decline in the volume of consumers remaining active after the GDPR introduced data protection opt-ins. We interpreted this as a positive sign of individuals using the GDPR to exercise their data protection rights. In economic terms, however, it suggests reduced rather than increased activity. As it happens, the economic picture in that specific study is more nuanced than this, with the authors noting that, 'the average value of the remaining consumers to advertisers has increased, offsetting most of the losses

from consumers that opt out' (Aridor, Che, and Salz 2020). However, a range of other research points to negative commercial outcomes for businesses as result of GDPR compliance. Ferracane et al.(2020) point to 'a negative and significant impact on the performance of downstream firms in sectors reliant on electronic data.' Goldberg et al. (2019) point to a 0.6 % decline in weekly revenues. Koski and Valmari helpfully place things in an international context, allowing for some visibility of the relative economic impact of differences in data protection standards. They looked at the performance of European and US businesses in the first year after the GDPR took effect, and concluded that, 'the costs of the GDPR during the first year of its implementation were substantial, at least for some European companies. The profit margins of the data-intensive firms increased, on average, by approximately 1.7 to 3.4 percentage points less than the profit margins of their US counterparts' (Koski and Valmari 2020).

The conclusion here is that the EU has not been effective at turning its data protection strength into economic advantage. However, it is important to note that there are legal constraints on how far the EU can go in pursuit of the goal of increased economic activity. The CJEU has repeatedly highlighted the primary importance of protecting individuals' data protection rights, and has ruled out compromising these rights for economic gain. The challenge is therefore to see whether new approaches, such as the data spaces mentioned earlier, can spur economic activity while staying within the data protection limits set by the GDPR. It will be some time before it is possible to assess the EU's effectiveness on this challenge.

3.5.6 Position the EU as a driving force in global data protection standards

This goal is perhaps the most significant for the purposes of our study, given that it relates directly to the EU's ability to influence evolution of the global governance landscape, the core focus of the TRIGGER project. Unsurprisingly, therefore, this goal overlaps substantially with aspects of the actorness model that we have discussed and assessed in the previous chapter. In particular, strong ratings on the recognition and attractiveness dimensions of actorness would appear to be necessary (but not sufficient) conditions of effectiveness at shaping global data protection standards. It appears clear that the EU meets these necessary conditions, given our assessment that the EU rates 'high' or 'moderate/high' on these two dimensions in the GDPR era.

It is useful again to consider the counterfactual as a way of clarifying the extent of the EU's effectiveness here. There has been a dramatic evolution of the data protection global governance landscape in recent years. Would this evolution have looked different if the EU were not actively trying to influence global developments? The data-driven evolution of the global economy would probably have spurred significant regulatory activity. And there is a recognisable set of core international principles (dating back to the work of the Council of Europe and the OECD in the 1980s) that would probably have informed much of this regulatory activity even without the EU's involvement. But the detailed data protection framework that the EU has honed over the past three decades provides a template that has been hugely influential on other global governance actors. Graham Greenleaf's most recent overview points to data protection laws being enacted in 145 countries (up from 76 in 2011), and he notes that each new law

coming through is ‘almost always’ influenced by the GDPR (Greenleaf 2021). He distinguishes two different modes of influence, with some countries emulating what they see as the EU’s best practice, while others ‘claim ambitions to enact new or stronger laws so as to be able to consider applying for ‘adequate’ status under the GDPR.

It is worth reiterating that there are counterarguments here. Researchers in the US, in particular, caution against assuming that a flurry of data protection activity in that country can be attributed to the influence of the GDPR (Chander, Kaminski, and McGeveran 2019; Mercer 2020). Similarly, we have noted in the previous chapter that the EU’s prioritisation of fundamental individual rights has little resonance with China’s political and legal culture, even if there are points of similarity between the GDPR and the data protection framework that is gradually taking shape in China. But these caveats do not change the fact that the EU has positioned itself as an unavoidable reference point in the global governance landscape for data protection. In other words, every other actor’s data protection framework is inevitably assessed in terms of how far it aligns with or diverges from the EU’s. That is a position of remarkable global governance status and influence, and so our assessment is that the EU has been highly effective on this goal.

3.6 Conclusion

This chapter presents a mixed picture of the EU’s effectiveness in the data protection domain. Crucially, in terms of direct external influence and impact on global governance – in other words, what we have described in this chapter as the sixth meso-goal – we have seen that the EU is highly effective. That is an important conclusion given the overall focus of the TRIGGER project. The fact that it correlates with the high levels of actorness discussed in the previous chapter suggests that there is fruitful research to be done on whether there are causal connections between particular dimensions of actorness and EU effectiveness in different contexts.

However, against this picture of strong overall external effectiveness, this chapter has also raised a number of caveats which highlight the need for more careful assessment. For example, neither of our two case studies provides an unalloyed argument for EU effectiveness. The Commission failed in its Privacy Shield negotiations, and our discussion of Convention 108+ noted that alignment with the GDPR reflected the effectiveness of the Council of Europe as well as of the EU. Moreover, in our discussion of EU effectiveness on six meso goals, we showed how global governance factors – particularly ongoing debates about how to regulate non-EU tech giants – weaken the EU’s effectiveness in a number of areas, from achieving harmonisation to the central goal of protecting rights that have been enshrined in the EU treaties.

It is beyond the scope of this chapter to pursue the many threads of further investigation that are suggested here. In particular, it would be instructive to see a wider range of case studies examined, to provide a much broader sample than is offered by the two that we have looked at. Similarly, there are

aspects of the assessment of meso-goal effectiveness that warrant more detailed attention. The fundamental rights goal is particularly important in this respect. It would be beneficial not just to have a better set of indicators for measuring overall performance on this goal, but also to be able to distinguish between the role played by potential rights infringements by external rather than internal actors. This would give us a clearer sense of the link between the EU's global governance influence and its ability to uphold citizens' data protection rights.

In general, we would expect meso goals to remain stable over the medium term. This is particularly true in the case of data protection, which is now a relatively mature policy domain for the EU, with clear roots in the treaties. However, the EU's external micro-goals will evolve continually because of ongoing changes in the global environment, both in terms of ongoing changes in the economic and societal role played by data, and because of the evolving stances on data protection that are being adopted by other global governance actors, both governments and companies. In the next chapter, we will highlight four broad issues (comprising both opportunities and challenges) that are going to shape the outlook for the EU in this policy domain.

4. Conclusion: opportunities and challenges

In the preceding chapters of this deep dive on data protection, we have explored the role of the EU in the evolving global governance landscape. In the first chapter, we provided a narrative overview of how data protection governance has developed since the 1980s, both within the EU and globally. One of the key insights here was that the EU's supranational structure meant it was well placed to play an influential role in the development of global data protection norms and rules. Experience gained dealing with intra-EU cross-border data flows could be applied externally as global cross-border data flows became a driving force of the global economy.

In the second chapter, we assessed the 'actorness' of the EU, using the TRIGGER project's seven-dimension model of actorness to illuminate the ways in which the EU has been able to influence the global governance landscape. Our analysis points to a steady increase in EU actorness since the 1980s. To a large extent this reflects the deepening of data protection's legal roots in the EU, as captured by the authority dimension of actorness. From an initial position of patchy ad hoc national measures, there has been a clear progression from, first, the 1995 Data Protection Directive to, second, the inclusion of data protection in the treaties as a fundamental right of EU citizens, and third, the enactment of the GDPR in 2018. This progression of EU authority in the data protection domain has been accompanied by strong performances on most of the other actorness dimensions, including those measuring internal cohesion as well as external recognition and attractiveness.

In the third chapter, we turned to consider the EU's effectiveness – in other words, its ability to leverage its actorness to achieve its (global) data protection goals. Our analysis presented a mixed picture on effectiveness, depending on which goals you consider. For example, we considered two case studies where the EU has been involved in negotiations with other global governance actors: Privacy Shield negotiations with the US and C108+ negotiations with the Council of Europe. We concluded that the EU failed in the first of these, because it could not find an arrangement that met the requirements of the CJEU. We suggested that the EU had been more effective with C108+, but we noted the importance of the fact that the Council of Europe shared the EU's goal of aligning C108+ and the GDPR – in effect, the EU was pushing at an open door. We also provided a broad assessment of the EU's effectiveness on six overarching goals that have characterised its long-term approach to data protection. We noted a strong degree of EU success at projecting its norms and rules internationally, but we also highlighted important questions about how effectively the EU fulfils one of its core goals, of protecting citizens' fundamental rights.

In this concluding chapter, we build on the preceding chapters to highlight a number of factors that we believe are likely to determine the EU's actorness and effectiveness in the data protection domain in the future. Our primary interest remains in the EU's ability to influence the global governance landscape. A number of these challenges for the EU are primarily domestic (i.e., within the EU) rather than global, but

they remain relevant for us given the structure of the TRIGGER model of actorness, in which internal dimensions (authority, autonomy and cohesion) are understood to affect the EU's global influence.

In total we list four broad areas where we suggest the EU should focus if it wishes to maximise its actorness and effectiveness in the data protection domain. These four strategic priorities present the EU with both opportunities and challenges. They are: data protection fundamentals, the need to reduce fragmentation, challenges relating to innovation and growth, and the prospect of further increases in the EU's international influence.

Fundamentals: consent and citizen's rights

In the preceding chapter, we highlighted concerns that have been raised about the robustness of the consent principle that underpins much of the EU's approach to data protection. If users are just ticking boxes to make consent notices disappear (Utz et al. 2019; Solove 2012), and if data processors are using manipulative design to 'nudge' users into giving consent (Norwegian Consumer Council 2018), then that is a substantive challenge to the foundations of the EU's approach to citizens' fundamental data protection rights. This issue is acknowledged in the staff working document that accompanies the Commission's review of the GDPR after two years in force. However, it is only mentioned in passing, and there is little sense of the serious implications of claims that a cornerstone of the GDPR approach to data protection has been hollowed out (European Commission 2020c). This question warrants serious research by the EU, as well as proposals for remedial steps if it is found that the current system is leading to behaviours (by both citizens and data processors) that undermine the idea that flows of personal data are underpinned by meaningful consent. The alternative is an erosion of confidence in the EU's approach if the perception takes root that the GDPR is a box-ticking exercise that can be easily gamed by unscrupulous data processors.

Admittedly, the so-called 'privacy paradox' – whereby many users claim that data protection is important to them, while simultaneously clicking 'accept all' on consent notices with little apparent regard for protecting their personal data – is a knotty problem. But we should not rush to assume that users' actions are a truer reflection of their preferences than their statements. Bietti (2020) notes that user choices about data consent are made in the context of power relationships between users and data processors, and that these power relationships are particularly asymmetrical in the internet platform economy. In a similar vein, Richards and Hartzog (2015) argue that the choice users are faced with is often illusory: 'Users given a blunt choice between protecting their data and participating in modern society really have no choice at all.' And they go on to suggest the privacy paradox can also be seen as reflecting the durability of user concerns about data protection: 'If our revealed preferences show that we don't care about privacy, why do so many of us remain anxious about our personal data?' This is a good question, and one which suggests that the current consent regime may not represent a durable equilibrium. Again, this is an argument for the EU to carry out detailed research into how well the consent regime as

currently implemented allows users to exercise their fundamental rights and exert meaningful control over their personal data.

Given the foundational importance of consent in the EU's data protection framework, any fraying of the consent regime may have implications for the EU's global governance role. For example, in terms of actorness, an erosion of confidence in the consent regime could adversely affect the EU's performance on the credibility dimension. It might also lead to a reduced rating on the attractiveness dimension in the eyes of some global actors, although, as we have noted previously, not all global actors view data protection primarily through a rights-based prism. And in terms of effectiveness, we discussed in the preceding chapter how problems with consent can weaken the EU on the goal of upholding citizens' fundamental rights.

It is beyond the scope of this chapter to suggest what steps the EU could take to bolster its consent regime. There are no easy solutions. Richards and Hartzog (2015) suggest that data protection regulators could learn from fiduciary law, the central goal of which is 'to protect against the exploitation of a vulnerability created by trust in another . . . by imposing duties such as care, loyalty, and confidentiality'. An analogous approach in the data protection domain might see data processors under a legal obligation not to 'self-deal' with users' personal information in ways that adversely affect the users and betray their trust. The EU would also do well to pay close attention to changes in the way data protection has been affecting competitive dynamics in the private sector. An example here is Apple's recent introduction of a default setting that will greatly limit Facebook's access to large flows of user data. The EU may be able to use private-sector innovation of this kind to prompt new ways of thinking about how best to ensure the implementation of a feasible and effective consent regime.

Fragmentation: enforcement and compliance

As noted in the chapter on effectiveness, it is estimated by IAPP that just over half of companies internationally are not fully compliant with the GDPR. In the EU, 43 % of respondents to an IAPP-EY survey said they were only 'moderately compliant', even when GDPR compliance was their primary responsibility. It is now more than 3 years since the GDPR became applicable, and 5 years since it was agreed. These are significant levels of non-compliance for a high-profile piece of legislation that affects most individuals and organisations. Among other things, high levels of non-compliance highlight the perennial importance of ensuring that the rationale for, and the requirements of, regulations are communicated clearly to private sector actors. There is an opportunity here for improved GDPR guidance, including greater harmonisation between EDPB and national guidance, as the Commission has noted.

The fragmentation of GDPR enforcement is an issue that has been mentioned a number of times in the previous chapters, as it bears directly on the EU's actorness via the cohesion dimension. The decentralised system of national DPAs is a core feature of the EU's data protection framework. The rules that apply across the EU have been largely unified with the shift from the DPD to the GDPR, but

how these rules are enforced remains subject to variation at the national level. As we have seen, this has particular relevance for the way in which external technology giants are regulated, owing to the fact that many of these companies have their EU headquarters in Ireland. This means that Ireland's DPA is the lead regulator for all of their EU operations – under the GDPR's one-stop shop approach to regulation, data processors are regulated by the DPA of their home Member State rather than by the DPAs of every Member State in which they operate. This is a recipe for regulatory tensions if DPAs differ in their views of how the GDPR should be implemented. This was a concern among many Member States when the GDPR was negotiated and it is precisely what has come to pass, with Ireland's DPA being criticised for being too lax towards the companies it is responsible for.

There is an important institutional challenge here for the EU, because the ratcheting up of inter-DPA tensions will be disruptive if it is not halted. The Commission can argue that it foresaw these kinds of problems. In the negotiations over the final text of the GDPR, the Commission had proposed that it would have the power to intervene to ensure consistency across the DPAs (Jančiūtė 2018). Instead, the EDPB was given this role, and provisions were included in the GDPR that anticipate potential divergences among DPAs, such as the consistency mechanism (Article 63) and the urgency procedure (Article 66). On the face of it, these are not currently working as well as they should. A more assertive role by the EDPB might help to impose more alignment across the system of national DPAs, and it is notable that in its two-year review of the GDPR, one of the Commission's key recommendations is that the EDPB and the DPAs work together more closely to ensure more harmonious implementation of the GDPR (European Commission 2020b). If the EDPB does not lead this process of alignment, greater use of Article 66 might be another way of achieving it, albeit more confrontationally. The urgency procedure in Article 66 allows a DPA to override the one-stop-shop approach, by introducing temporary measures on its own territory and requesting a binding decision from the EDPB on whatever disagreements exist between the DPAs in question. In theory therefore, DPAs could force the pace of greater alignment. A still more radical proposal might be to consider more substantive changes to the one-stop-shop system to reflect the fact that some cross-border cases are more significant than others. Given the increasingly systemic societal role that major technology companies play in all Member States, it may not make sense to delegate their regulation to the DPA of one Member State. When a data processor crosses a certain threshold (such as revenue, profit or the number of EU customers/users a company has outside its home Member State) there may be an argument for the lead DPA to have to share regulation with a panel of additional DPAs.

Fragmentation is an ongoing challenge for the EU, but we should not lose sight of the fact that the overall trajectory in the decades since the 1980s has been towards much greater harmonisation of data protection across the EU. The fragmentation that remains should also be kept in perspective: harmonisation is a challenge in most areas of EU law. Nevertheless, enforcement is a crucial element of any regulatory framework, and if current signs of fragmentation across Member States in the data protection domain were to worsen, then this would be likely to affect the EU's global governance standing. In terms of actorness, increased fragmentation relating to enforcement could hit the EU's

performance on the cohesion and credibility dimensions. It is also self-evident that the EU's data protection effectiveness will be hampered if rules are not being properly enforced to any significant degree. One additional aspect of the GDPR enforcement regime which may push towards higher levels of enforcement is the ability of non-governmental organisations (NGOs) to act on behalf of citizens in lodging complaints with the relevant DPA. After the success of the Schrems cases in overturning the EU's agreements with the US, it is to be expected that data protection NGOs will push for stronger enforcement of the GDPR.

Economics: innovation and growth

A third broad challenge that the EU faces relates to the impact of data protection on the bloc's economy. In the chapter on actorness, we suggested that one of the future tests of the EU's credibility will be its ability to marry data protection and economic dynamism. The EU enjoys strong levels of actorness in the data protection domain; it is not hubris to refer to it as a regulatory superpower. But the EU cannot be described as a technological superpower in terms of driving the development of key data-intensive technologies or of building up a share of the global digital economy that is commensurate with the EU's size. It is frequently asserted that these two facts are linked and that the GDPR dampens digital innovation and growth in the EU. This is a question that deserves rigorous research by the EU, including quantitative assessment of the impacts of the GDPR as well as consultation with a wide range of affected stakeholders. More evidence is needed. If there is a trade-off between the GDPR and innovation, then it is important to understand it so that good decisions can be made about it. A clear-eyed assessment of the data is imperative. It may not be possible to 'have it all' when shaping the EU's digital economy. Indeed, it appears highly plausible that pursuing a values-driven and strong-regulation approach to data would constrain aggregate growth to at least some extent. This is a point that TRIGGER researchers have already made in the context of the EU's values-driven approach to artificial intelligence and machine learning, where it has been noted that, 'prioritising values in this way will likely mean ceding a lot of digital economic activity to more commercially assertive players' (Collins and Florin 2021). This also applies to data protection. But it should not necessarily be interpreted as a criticism. Rather, it is a call for policy decisions on trade-offs like these to be as transparent and as well-informed as possible.

In terms of actorness, a potential trade-off between values and economics is relevant for the attractiveness dimension in particular. The attractiveness dimension comprises two distinct components, with instrumental attractiveness referring to the economic advantages of aligning with the EU, while normative attractiveness refers more to values-based reasons for following the EU's lead in this policy domain. What is suggested by the discussion of the relationship between values-driven regulation and economic vibrancy is that in the field of data protection there is a potential tension between the two attractiveness components. Gains on one side of the attractiveness equation may be offset by losses on the other.

One area where the relationship between data protection and growth is going to be a particular challenge is in emerging data-intensive sectors of the economy, including machine learning. We have seen in the

effectiveness chapter that one of the EU's goals with its data protection framework is to boost innovation. In its two-year review of the GDPR, the Commission states quite unambiguously at one point that 'the GDPR fosters competition and innovation' by allowing data to flow freely, but this seems, at the very least, to be an over-simplification of the case (European Commission 2020c). For example, one of the key premises of the Commission's recent data strategy is that current data flows in the EU are *not* conducive to the growth of key data-intensive sectors that underpin a growing share of economic activity. In its Communication launching the data strategy, the Commission states that, 'Currently there is not enough data available for innovative re-use, including for the development of artificial intelligence' (European Commission 2020a). The Commission's response in the data strategy is an ambitious piece of industrial strategy, which seeks to put in place an EU-wide data ecosystem of sectoral 'data spaces' that will be grounded in GDPR principles but that will also provide companies with access to much greater volumes of data than are currently available in the EU. In an important nod to the increasing geopolitical and geoeconomic significance of technology governance, the Commission explicitly contrasts this EU approach with the way the US and China have developed their data ecosystems: 'In the US, the organisation of the data space is left to the private sector, with considerable concentration effects. China has a combination of government surveillance with a strong control of Big Tech companies over massive amounts of data without sufficient safeguards for individuals. In order to release Europe's potential we have to find our European way, balancing the flow and wide use of data, while preserving high privacy, security, safety and ethical standards' (European Commission 2020a). It is implicit in the Commission's data strategy that the GDPR on its own is not enough to achieve this desired balance.

The EU will have to be realistic about what is involved in developing a vibrant data-intensive technological ecosystem. The data strategy appears to envisage the EU adopting something of a midway point between the approaches of the US and China: involving greater public sector involvement than the former but without the authoritarianism of the latter. But it remains to be seen whether this is a viable route to a healthy and self-sustaining ecosystem. The EU risks adopting a quite mechanistic approach to this, assuming that a top-down decision to create a set of 'data spaces' will lead to all the other elements of the data-intensive innovation ecosystem flourishing. This looks like a simple solution being sought for a complex challenge involving a much wider constellation of factors that both shape and are shaped by Europe's overall political economy, including taxes, financing, labour markets, and so on.

The Commission's data strategy also highlights an important point about the development of technologies that can help to embed data protection. Data protection is not only a matter of regulation and other forms of governance. It can also be facilitated by technological solutions. This adds another dimension to the question of the relationship between data protection and innovation. As well as asking whether strong data protection helps or hinders the overall innovation ecosystem, it is also worth considering how much innovation might be prompted by the requirements of data protection itself. The EU's data strategy focuses on innovation on the macro scale required to develop a European data

infrastructure, through data spaces and other initiatives, such as GAIA-X. But data protection may also prompt innovation at the enterprise and consumer level, through the development of so-called privacy-enhancing technologies (PETs), such as homomorphic encryption, differential privacy or federated learning. One possible economic opportunity for the EU is to leverage its strong global reputation for data protection into a badge of commercial excellence for PETs that meet EU data protection standards and/or are developed in the EU. A similar argument has already been made in the TRIGGER project in relation to machine learning, where it was suggested that the US and China are likely to remain the leading technology powers, but that the EU could pursue a 'niche leadership' strategy in those commercial domains where its values-driven approach is particularly salient (Collins et al. 2020). The EU is already a regulatory superpower for data protection. Is there an opportunity to leverage this into commercial openings for innovative EU firms producing privacy-enhancing technology? Strong data protection requirements in the EU create a domestic market for such innovations, and the evidence points to a strong increase in the market for privacy technology since 2017[26]. The growing global influence of the GDPR may also create an international market for this technology too. This could be an area for the EU to prioritise in its significant research and development spending.

The vibrancy of the EU's innovation ecosystem is primarily of interest for internal reasons, related to the performance of the economy and the wellbeing of EU citizens. Innovation is a driver of productivity, which in turn underpins the long-term trends of economic growth and living standards. However, there is also the potential for a direct spillover to the external domain and to the EU's actorness, not just in the data protection domain but more broadly too. Economic factors are built into the TRIGGER actorness model, through the attractiveness dimension, so if the EU economy were to decline relative to its major peers, then we would expect EU attractiveness and actorness to suffer too. Moreover, the current geopolitical backdrop is challenging. Relationships between the EU, the US and China are evolving, and not least in relation to the growing geopolitical significance of leadership in the emerging technologies that will serve as the backbone of a growing share of future economic activity. The way the latest European Commission has badged itself a 'geopolitical Commission' highlights the extent to which these international factors now frame strategic thinking at the highest levels of the EU. They may also begin to weigh on EU decisions about whether and how to balance data protection and economic growth.

Influence: the continuing internationalisation of EU data protection

The final opportunity that we highlight here is one that we have been discussing throughout this deep dive on data protection: the EU's desire to influence the evolving governance of data protection around the world. This goes to the heart of the whole TRIGGER project: how can the EU be an effective global actor? Notwithstanding the various reservations outlined so far in this conclusion, the EU has made solid progress on many of the 'domestic' aspects of data protection governance. Over the decades it has built and consolidated a system of rights and duties which, though far from perfect, are at the heart of the regulatory architecture of the EU and its 27 Member States. There will be a lot of refinement and trouble-

[26] See https://iapp.org/resources/article/privacy-tech-vendor-report/

shooting to do, some of it touching on fundamental issues, but the GDPR marked an important milestone for data protection within the EU, and 3 years after it entered into force, the EU now has an opportunity to devote increasing energy to building on the position of global influence it has already carved out for itself.

One very concrete challenge in the short term will be establishing a stable data transfer arrangement with the US in the wake of the Safe Harbor and Privacy Shield decisions, in which the CJEU struck down the Commission's attempts to find a workaround for the fact that US data protection standards do not meet the EU's adequacy threshold. This question brings into stark relief the tension between two of the EU's six meso goals, as outlined in the previous chapter, namely the goals of protecting fundamental rights and of boosting external trade. The CJEU has said that the treaties leave no room for ambiguity here: fundamental rights take precedence and cannot be compromised for a potential boost to trade volumes. Against that, the EU's economic relationship with the US is of great importance for many businesses and workers. If data protection differences were to become a source of real friction in that relationship, it could undermine support for the EU's approach. If jobs began to be lost, it is not certain that all EU citizens would line up behind the CJEU's interpretation of the need for 'essentially equivalent' protections in third countries. Recall the research cited in the previous chapter which found that around 1 in 8 individuals already believe that the GDPR has adversely affected their professional lives (Strycharz, Ausloos, and Helberger 2020). It would be a significant failure for the EU's data protection diplomacy if a way is not found to square the circle of EU-US data transfers.

It is to be welcomed that the EU's decisions about data transfers with the US will require it to think about the relationship between its various goals in this domain, such as the potential trade-off between rights and innovation. The data protection domain is too young for policy stances to become too rigidified too quickly. The world of digital technology is evolving rapidly. The global economy is evolving too. To use the language of our actorness model, these developments are likely to create new opportunities (or necessities) for the EU to refine and project its approach to data protection. The EU has previously been adept at seizing such opportunities – from the 1990s in particular, a sparse global regulatory landscape allowed it to internationalise key aspects of the approach it had developed to deal with intra-EU cross-border flows. Maintaining the global leadership position it has established will require the EU to be vigilant and proactive. It should be willing to tweak its approach to international data protection if emerging evidence begins to point either to potential problems or to potential opportunities. There are already signs of interesting developments in this field. One such development that we discussed in the previous chapter is the EU's close involvement with the Council of Europe's C108+, which arguably represents a second pillar in the internationalisation of EU data protection values. C108+ probably falls short of the EU's adequacy threshold, but the EU nevertheless strongly supports the convention and wants countries around the world to sign up to it. This may lead to questions for the EU in the future about what it sees as the most efficient and effective way of influencing data protection standards in third countries. Would the EU prefer to work closely with countries to get them to 'essential equivalence'

and an adequacy agreement? Or would it prefer to prioritise a greater number of countries signing up for C108+, which is less onerous than the GDPR but which still captures most of its key principles?

The EU would also do well to spell out its reasons for wanting to increase its influence over data protection standards in other countries. This is not just a philosophical question. Different reasons are likely to lead to different policy preferences, and different priorities when external goals come into conflict. One reason for wanting strong data protection overseas relates to fundamental rights at home – in other words, ensuring that EU citizens' personal data will be safe if processed in third countries. A second reason could be more altruistic: the EU might want to see the citizens of other countries given some of the same fundamental rights that EU citizens enjoy. Economic factors are a third potential reason: as we saw in the effectiveness chapter, strong data protection standards in the EU are likely to hamper rather than boost trade unless similar protections can be enforced in the EU's trading partners. A fourth potential reason for wanting data protection influence is geopolitical. The EU derives soft power from being a regulatory superpower. This regulatory power is particularly welcome in a technological domain, given that the US and China are otherwise so dominant in this area.

There is a wider point here that perhaps applies to the TRIGGER project as a whole. We have been taking it for granted that more influence is better than less influence, and more actorness better than less actorness. But that might not always be the case. Creating and maintaining global influence is not cost-free. It takes time and resources. For example, if your ultimate goal is to protect EU citizens' fundamental rights, then depending on the circumstances it might make more sense in terms of cost-benefit analysis to devote any additional resources to securing improvements within the EU rather than influencing the actions of third countries. Only with a clear sense of why you want to influence global governance can you take robust decisions about how to go about it and how much effort and investment to devote to it. With the EU now a dominant fixture in the global governance landscape for data protection, developing this kind of clarity about goals and priorities will be crucial to maximising the EU's success in the post-GDPR era.

Bibliography

Albrecht, Jan Philipp. 2016. 'How the GDPR Will Change the World.' *Eur. Data Prot. L. Rev.* 2: 287.

Aridor, Guy, Yeon-Koo Che, and Tobias Salz. 2020. 'The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR.' *NBER Working Paper 26900*. http://www.nber.org/papers/w26900.

Article 29 Data Protection Working Party. 2016. 'Opinion 01/2016 on the EU–U.S. Privacy Shield Draft Adequacy Decision.' https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=55929.

Barbière, Cécile. 2014. 'National Parliaments Raise the Pressure on Data Protection.' *Www.Euractiv.Com* (blog). 22 September 2014. https://www.euractiv.com/section/digital/news/national-parliaments-raise-the-pressure-on-data-protection/.

Bendrath, Ralf. 2007. 'The Return of the State in Cyberspace: The Hybrid Regulation of Global Data Protection.' *Dunn M., Krishna-Hensel SF et V. Mauer,(Dir.), The Resurgence of the State: Trends and Processes in Cyberspace Governance, Aldershot: Ashgate*, 111-51.

Bensinger, Viola, Carsten Kociok, and Viola Zollitsch. 2021. 'E-Privacy Regulation: EU Council Finally Adopts Its Position, and Trilogue Begins.' Data Privacy Dish. 1 April 2021. https://www.gtlaw-dataprivacydish.com/2021/04/e-privacy-regulation-eu-council-finally-adopts-its-position-and-trilogue-begins/.

Bietti, Elettra. 2020. 'Consent as a Free Pass: Platform Power and the Limits of the Informational Turn.' *Pace Law Review*, 310.

Birnhack, Michael D. 2008. 'The EU Data Protection Directive: An Engine of a Global Regime.' *Computer Law & Security Review* 24 (6): 508–20. https://doi.org/10.1016/j.clsr.2008.09.001.

Bradford, Anu. 2012. 'The Brussels Effect.' *Nw. UL Rev.* 107: 1.

– – – . 2020. *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, USA.

Brill, Julie. 2018. 'Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data.' Microsoft on the Issues. 21 May 2018. https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

Butler, Alan, and Fanny Hidvegi. 2015. 'From Snowden to Schrems: How the Surveillance Debate Has Impacted US-EU Relations and the Future of International Data Protection.' *Whitehead J. Dipl. & Int'l Rel.* 17: 55.

Bygrave, Lee A. 2020. 'The 'Strasbourg Effect' on Data Protection in Light of the 'Brussels Effect': Logic, Mechanics and Prospects.' *Computer Law & Security Review* 40: 105460.

Chander, Anupam, Margot E. Kaminski, and William McGeveran. 2019. 'Catalyzing Privacy Law.' *Minnesota Law Review* 105: 1733-1802.

Cody, Jonathan P. 1998. 'Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation.' *Cath. UL Rev.* 48: 1183.

Collins, Aengus, and Marie-Valentine Florin. 2021. ‘Governance and Technologies: Interrelations and Opportunities (D4.6).’

Collins, Aengus, Marie-Valentine Florin, Anca Rusu, Anshuman Saxena, and Gianluigi Viscusi. 2020. ‘Review of Current Governance Regimes and EU Initiatives Concerning AI (D4.3).’ https://trigger-project.eu/wp-content/uploads/2020/10/D4.3.-Review-of-current-governance-regimes-and-EU-initiatives-concerning-AI-working-paper.pdf.

Council of Europe. 1981. ‘Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.’ https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434.

Council of Europe Ad Hoc Committee on Data Protection. 2016a. ‘Abridged Report [CAHDATA(2016)RAPAbr].’ https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b7e90.

– – – . 2016b. ‘Consolidated Version of the Modernisation Proposals of Convention 108 with Reservations [CAHDATA(2016)01].’ https://www.privacyandpersonality.org/wp-content/uploads/2016/05/OG_Ref_1_20_May_2016.pdf.

Coyne, Hallie. 2019. ‘The Untold Story of Edward Snowden’s Impact on the GDPR.’ *The Cyber Defense Review* 4 (2): 65–80.

De Terwangne, Cecile. 2021. ‘Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data.’ *Computer Law & Security Review* 40: 105497.

Determann, Lothar, and Chetan Gupta. 2018. ‘Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law.’ *UC Berkeley Public Law Research Paper*.

Drechsler, Laura. 2019. ‘What Is Equivalent? A Probe into GDPR Adequacy Based on EU Fundamental Rights.’ *A Probe into GDPR Adequacy Based on EU Fundamental Rights (February 21, 2019). Jusletter IT* 21.

Espinoza, Javier. 2021. ‘Fight Breaks out between Ireland and Germany over Big Tech Regulation.’ *Financial Times*, March 17, 2021. https://www.ft.com/content/37705bcf-c5b6-4ef0-adb8-35a8680dbaec.

Espinoza, Javier, and Leila Abboud. 2021. ‘France Pushes for Big Changes to Proposed EU Tech Regulation.’ *Financial Times*, February 15, 2021. https://www.ft.com/content/5e41d0cf-a83c-4817-997e-a353858137ab.

European Commission. 1990. ‘Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security.’ http://aei.pitt.edu/3768/1/3768.pdf.

– – – . 2010. ‘Communication from the Commission, ‘A Comprehensive Approach on Personal Data Protection in the European Union’, COM(2010)609.’ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0609.

– – – . 2012a. ‘Commission Staff Working Paper: Impact Assessment.’ https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072.

– – – . 2012b. ‘Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation).’ https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

– – – . 2016. ‘European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows.’ https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461.

– – – . 2017. ‘Communication from the Commission to the European Parliament and the Council, ‘Exchanging and Protecting Personal Data in a Globalised World’, COM(2017)7.’ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN.

– – – . 2019. ‘Communication from the Commission to the European Parliament and the Council, ‘Data Protection Rules as a Trust-Enabler in the EU and beyond – Taking Stock’, COM(2019)374.’ https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2019:374:FIN.

– – – . 2020a. ‘Communication: A European Strategy for Data.’ https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN.

– – – . 2020b. ‘Communication from the Commission to the European Parliament and the Council, ‘Data Protection as a Pillar of Citizens’ Empowerment and the EU’s Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation’, COM(2020)264.’ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264.

– – – . 2020c. ‘Staff Working Document Accompanying the Commission Communication "Two Years of Application of the General Data Protection Regulation."' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0115.

– – – . n.d. ‘Adequacy Decisions.’ Text. European Commission -– European Commission. Accessed 9 November 2020. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

European Data Protection Board. 2021. ‘EDPB Adopts Urgent Binding Decision: Irish SA Not to Take Final Measures but to Carry out Statutory Investigation.’ 2021. https://edpb.europa.eu/news/news/2021/edpb-adopts-urgent-binding-decision-irish-sa-not-take-final-measures-carry-out_en.

Farrell, Henry. 2002. ‘Negotiating Privacy in the Age of the Internet. Analyzing the EU-US ‘Safe Harbor’ Negotiations.’ In *Common Goods: Reinventing European and International Governance*, edited by Adrienne Hèritier. Rowman and Littlefield.

Farrell, Henry, and Abraham L. Newman. 2019. *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security*. Princeton University Press.

Ferracane, Martina Francesca, Janez Kren, and Erik van der Marel. 2020. ‘Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?’ *Review of International Economics* 28 (3): 676-722.

Ferracane, Martina, and Erik van der Marel. 2019. ‘Do Data Policy Restrictions Inhibit Trade in Services?’ *Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS* 29.

Fromholz, Julia M. 2000. 'The European Union Data Privacy Directive.' *Berk. Tech. LJ* 15: 461.

Giurgiu, Andra, and Tine A. Larsen. 2016. 'Roles and Powers of National Data Protection Authorities.' *Eur. Data Prot. L. Rev.* 2: 342.

Goldberg, Samuel, Garrett Johnson, and Scott Shriver. 2019. 'Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic & e-Commerce Outcomes.' http://dx.doi.org/10.2139/ssrn.3421731.

Granger, Marie-Pierre, and Kristina Irion. 2014. 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU Legislator and Teaching a Lesson in Privacy and Data Protection.' *European Law Review* 39 (6): 835-50.

Greenleaf, Graham. 1995. 'The European Privacy Directive – Completed.' *Privacy Law & Policy Reporter*. http://www.austlii.edu.au/au/journals/PLPR/1995/52.html#fn5.

– – – . 2012. 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108.' *International Data Privacy Law* 2 (2): 68-92.

– – – . 2016. 'Renewing Convention 108: The CoE's' GDPR Lite' Initiatives.' *Privacy Laws & Business International Report* 142: 14-17.

– – – . 2018a. 'Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108.' *Privacy Laws & Business International Report* 156: 22-24.

– – – . 2018b. 'Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018.' *UNSW Law Research Paper*, no. 18-56.

– – – . 2018c. ''Modernised' Data Protection Convention 108 and the GDPR.' In *Data Protection Convention*, 108:22-23.

– – – . 2019a. 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills.'

– – – . 2019b. 'Global Data Privacy Laws 2019: New Eras for International Standards.'

– – – . 2020. 'India's Data Privacy Bill: Progressive Principles, Uncertain Enforceability.'

– – – . 2021. 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance.' *Privacy Laws & Business International Report* 169: 3-5.

Greenleaf, Graham, and Scott Livingston. 2016. 'China's New Cybersecurity Law–Also a Data Privacy Law?'

– – – . 2017. 'China's Personal Information Standard: The Long March to a Privacy Law.'

Greenleaf, Graham, and Arthit Suriyawongkul. 2019. 'Thailand–Asia's Strong New Data Protection Law.' *Available at SSRN*.

Greer, Damon. 2011. 'Safe Harbor – a Framework That Works.' *International Data Privacy Law* 1 (3): 143-48.

Hijmans, Hielke. 2010. 'Recent Developments in Data Protection at European Union Level.' In *ERA Forum*, 11:219-31. Springer.

– – – . 2016. 'The DPAs and Their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European.' *Eur. Data Prot. L. Rev.* 2: 362.

Hilden, Jockum. 2019. ‘The Politics of Datafication: The Influence of Lobbyists on the EU’s Data Protection Reform and Its Consequences for the Legitimacy of the General Data Protection Regulation.’

Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. 2019. ‘The European Union General Data Protection Regulation: What It Is and What It Means.’ *Information & Communications Technology Law* 28 (1): 65-98.

Houser, Kimberly A., and W. Gregory Voss. 2018. ‘GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy.’ *Rich. JL & Tech.* 25: 1.

International Association of Privacy Professionals (IAPP). 2021. ‘GDPR at Three.’ https://iapp.org/media/pdf/resource_center/GDPR-at-Three-Infographic_v3.pdf.

Jančiūtė, L. 2018. ‘EU Politics and the Making of the General Data Protection Regulation: Consociationalism, Policy Networks and Institutionalism in the Process of Balancing Actor Interests.’ PhD Thesis, University of Westminster.

Jasmontaite, Lina, Irene Kamara, Gabriela Zanfir-Fortuna, and Stefano Leucci. 2018. ‘Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR.’ *Eur. Data Prot. L. Rev.* 4: 168.

Kalyanpur, Nikhil, and Abraham L. Newman. 2019. ‘The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation.’ *JCMS: Journal of Common Market Studies* 57 (3): 448-67.

Kobrin, Stephen J. 2004. ‘Safe Harbors Are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance.’ *Review of International Studies* 30 (1): 111-31.

Koski, Heli, and Nelli Valmari. 2020. ‘Short-Term Impacts of the GDPR on Firm Performance.’ The Research Institute of the Finnish Economy. https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-77.pdf.

Kuner, Christopher. 2015. ‘Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law.’ *International Data Privacy Law* 5 (4): 235-45.

Kuner, Christopher, Fred H. Cate, Christopher Millard, and Dan Jerker B. Svantesson. 2012. ‘The Intricacies of Independence.’ *International Data Privacy Law* 2 (1): 1-2. https://doi.org/10.1093/idpl/ipr021.

Kuschewsky, Monika. 2014. ‘The New Privacy Guidelines of the OECD: What Changes for Businesses?’ *Journal of European Competition Law & Practice* 5 (3): 146-48.

Lam, Christina. 2017. ‘Unsafe Harbor: The European Union’s Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner.’ *BC Int’l & Comp. L. Rev.* 40: 1.

Landau, Susan. 2013. ‘Making Sense from Snowden: What’s Significant in the NSA Surveillance Revelations.’ *IEEE Security & Privacy* 11 (4): 54-63.

Lindsay, David. 2014. ‘The ‘Right to Be Forgotten’ by Search Engines under Data Privacy Law: A Legal Analysis of the *Costeja* Ruling.’ *Journal of Media Law* 6 (2): 159-79. https://doi.org/10.5235/17577632.6.2.159.

Lynskey, Orla. 2014. ‘The Data Retention Directive Is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland.’ *Common Market Law Review* 51 (6): 1789-1811.

Mandavia, Megha. 2019. ‘Personal Data Protection Bill Can Turn India into ‘Orwellian State’: Justice BN Srikrishna.’ *The Economic Times*, December 12, 2019. https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms.

Mantelero, Alessandro. 2021. ‘The Future of Data Protection: Gold Standard vs. Global Standard.’ *Computer Law & Security Review* 40: 105500.

Mercer, Shannon Togawa. 2020. ‘The Limitations of European Data Protection as a Model for Global Privacy Regulation.’ *American Journal of International Law* 114: 20-25.

Monyango, Francis. 2019. ‘Kenya: Overview of the Data Protection Act, 2019.’ DataGuidance. December 18, 2019. https://www.dataguidance.com/opinion/kenya-overview-data-protection-act-2019.

Newman, Abraham L. 2008. ‘Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive.’ *International Organization* 62 (1): 103-30.

Norwegian Consumer Council. 2018. ‘Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy.’ https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

Nouwens, Midas, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 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*, 1-13.

OECD. 2007. ‘OECD Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy.’ http://www.oecd.org/internet/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsprotectingprivacy.htm.

– – – . 2011. ‘Thirty Years After the OECD Privacy Guidelines.’

– – – . 2013. ‘The OECD Privacy Framework.’

Pasadilla, Gloria O., Yann Duval, and Witada Anukoonwattaka. 2020. ‘Next Generation Non-Tariff Measures: Emerging Data Policies and Barriers to Digital Trade.’ ARTNeT Working Paper 187. http://hdl.handle.net/10419/213424.

Pearce, Graham, and Nicholas Platten. 1998. ‘Achieving Personal Data Protection in the European Union.’ *JCMS: Journal of Common Market Studies* 36 (4): 529-47.

Perrone, Christian, and Sabrina Strassburger. 2018. ‘PRIVACY AND DATA PROTECTION-FROM EUROPE TO BRAZIL.’ *PANORAMA OF BRAZILIAN LAW* 6 (9–10): 82-100.

Privacy Shield Framework. 2020. ‘Privacy Shield List.’ 2020. https://www.privacyshield.gov/list.

Reidenberg, Joel R. 1999. ‘Restoring Americans’ Privacy in Electronic Commerce.’ *Berkeley Tech. LJ* 14: 771.

– – – . 2001. ‘E-Commerce and Trans-Atlantic Privacy.’ *Hous. L. Rev.* 38: 717.

Richards, Neil, and Woodrow Hartzog. 2015. ‘Taking Trust Seriously in Privacy Law.’ *Stanford Technology Law Review* 19: 431-72.

Sacks, Sam, Mingli Shi, and Graham Webster. 2019. 'The Evolution of China's Data Governance Regime: A Timeline.' New America. 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/china-data-governance-regime-timeline/.

Salbu, Steven R. 2002. 'The European Union Data Privacy Directive and International Relations.' *Vand. J. Transnat'l L.* 35: 655.

Schünemann, Wolf Jürgen, and Jana Windwehr. 2020. 'Towards a 'Gold Standard for the World'? The European General Data Protection Regulation between Supranational and National Norm Entrepreneurship.' *Journal of European Integration*, 1-16.

Schütz, Philip. 2012. 'The Set Up of Data Protection Authorities as a New Regulatory Approach.' In *European Data Protection: In Good Health?*, edited by Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet, 125–42. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-007-2903-2_7.

Schwartz, Paul M. 2019. 'Global Data Privacy: The EU Way.' *NYUL Rev.* 94: 771.

Schwartz, Paul M., and Karl-Nikolaus Peifer. 2017. 'Transatlantic Data Privacy Law.' *Georgetown Law Journal* 106 (1): 115-79.

Simitis, Spiros. 1995. 'From the Market to the Polis: The EC Directive on the Protection for Personal Data.' *Iowa Law Review* 80 (3): 445-70.

– – – . 2010. 'Privacy – An Endless Debate?' *California Law Review*, 1989-2005.

Solove, Daniel J. 2012. 'Privacy Self-Management and the Consent Dilemma.' *Harvard Law Review* 126: 1880.

Sørensen, Jannick, and Sokol Kosta. 2019. 'Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites.' In *Proceedings of the 2019 World Wide Web Conference, May 13–17 2019, San Francisco, CA, USA*. https://doi.org/10.1145/3308558.3313524.

Stevens, Gina Marie. 1999. 'Online Privacy Protection: Issues and Developments.' In . Congressional Research Service, Library of Congress.

Strycharz, Joanna, Jef Ausloos, and Natali Helberger. 2020. 'Data Protection or Data Frustration? Individual Perceptions and Attitudes Towards the GDPR.' *European Data Protection Law Review* 6 (3): 407-21.

Teebken, Jacob, and Guske. 2019. 'The TRIGGER Model for Evaluating Actorness: Testing EU Actorness and Influence in Domestic and Global Governance (D3.1).' https://trigger-project.eu/wp-content/uploads/2020/07/D3.1-Testing-EU-actorness-and-influence-in-domestic-and-global-governance.pdf.

Tene, Omer. 2021. 'Today's LIBE Committee Compromise Resolution Condemning DPC Ireland Was Leaked.' Tweet. 2021. https://twitter.com/omertene/status/1384144486104649742.

Tzanou, Maria. 2020. 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights.' *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty, Hart Publishing, Forthcoming*.

US Department of Health and Welfare. 1973. 'Records, Computers and the Rights of Citizens.' *Report of the Secretary's Advisory Committee on Automated Personal Data Systems*.

Utz, Christine, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. '(Un) Informed Consent: Studying Gdpr Consent Notices in the Field.' In *Proceedings of the 2019 Acm Sigsac Conference on Computer and Communications Security*, 973–90.

Weiss, Martin A., and Kristin Archick. 2016. 'US-EU Data Privacy: From Safe Harbor to Privacy Shield.' R44257. Congressional Research Service Reports. https://digital.library.unt.edu/ark:/67531/metadc855920/m2/1/high_res_d/R44257_2016May19.pdf.

White House. 1997. 'A Framework for Global Electronic Commerce.' https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.

Wiener, Jonathan B., Arthur C. Petersen, Christina Benighaus, John D. Graham, Kenneth A. Oye, Ortwin Renn, and Marie-Valentine Florin. 2017. 'Transatlantic Patterns of Risk Regulation: Implications for International Trade and Cooperation.' International Risk Governance Council.

WP12. 1998. 'Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of TheEU Data Protection Directive.' https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf.

WP29. 2015. 'Letter of the ARTICLE 29 Data Protection Working Party to Ilze Juhansone,' June 2015. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_msjuhansone_en.pdf.

Wright, David, and Charles Raab. 2014. 'Privacy Principles, Risks and Harms.' *International Review of Law, Computers & Technology* 28 (3): 277-98.