Including but not limited to

How Brussels is emerging as a global regulatory superpower, establishing its data protection standard worldwide

Master Thesis

Supervisor

Maria Strömvik Lund University
Department of Political Science

Author

Sivan Pätsch Lund University
MSc European Affairs Department of Political Science

Submission Date 18.05.2018

LUNDS UNIVERSITET

Abstract

Can the European Union shape global regulatory policy? If it can, what conditions exist? This is the essential question at the centre of this thesis. This thesis will employ the case of global data protection regulation and put the two opposing theories of realist Daniel Drezner and institutionalist Anu Bradford against each other.

To answer the first questions data protection authorities around the world have been asked to complete questionnaires on principles in their laws and these have been matched with common European and non-European data protection frameworks. The data indicates that the European Union is able to shape global data protection legislation

Two answer the second question, the two theories have been compared and confronted with the results from the first research question. While both authors cannot be completely proven or disproven, taking only their central disagreement if the European Union can shape policy against the preferences of the United States, Bradford having answered this positively emerges with the data on her side.

Keywords: regulatory convergence, policy convergence, data protection, data privacy, Brussels effect

Wordcount: 19.997

Table of contents

List of tables

Abbreviations

AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
BSA	Bank Secrecy Act
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CFAA	Computer Fraud and Abuse Act
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
COPPA	Children's Online Privacy Protection Act
ECHR	European Convention on Human Rights
ECOWAS	Economic Community of West African States
EEA	European Economic Area
EU	European Union
FIPS	Fair Information Pracitces
FTC	Federal Trade Commission
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information and communications technology
IGO	International Governmental Organisations
MiFID II	Markets in Financial Instruments Directive II
MiFIR	Markets in Financial Instruments
ML	Machine Learning
National CSIRT	National Computer Security Incident Response Team
NATO	North Atlantic Treaty Organisation
NGO	Non-governmental Organisations
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
USA	The United States of America
WTO	World Trade Organisation

1 Introduction

"EUROPE IS STILL A SUPERPOWER"

It is questionable how many would agree with this remarkable claim by Andrew Moravcsik (2017). The growing consensus seems to be that Europe was never able to compete with the hegemon of the second half of the 20th century, the United States. And now that the US is flirting with a more isolationist policy, Europe could be finally getting its chance to lead again. However, it can be surely agreed upon the fact that Europe was neither the in past decades and nor will it be in the near future a leader in military power. And while Europe rested long on its economic importance, there are signs of its vanishing. Europe's population is ageing and shrinking, and its political process is slow and complicated. So why after all would Europe still be a superpower?

Although often not taken seriously – depending on the ideological perspective – Europe always has and still does hold an enormous amount of soft power. And with this, Europe possesses the ability to shape the face of market regulation worldwide. However, the question of Europe's strength remains – when the United States abandon multilateralism, are the Europeans able to keep wide international cooperation alive? When the United States withdraw from the Iran nuclear deal framework, are the Europeans able to keep the deal running? Can Europe really shape the way policies look around the world?

Daniel Drezner and Anu Bradford strongly disagree on questions like these. While Drezner contributes his theory from a realist point of view, positing that the European Union cannot shape global policies against the preferences of the United States. Bradford on the other hand, sees the world from an institutionalist point of view and believes the European Union can "wield unilateral influence across a number of areas of law" (Bradford, 2012, p. 1), determining global standards without using coercion. One of the fields both authors apply their theories to, is the field of data protection.

Data protection is a field where one could argue that the United States seem unwilling to lead. It can be alleged, that the US is prioritising the economic interests of Silicon Valley over the privacy interests of its and the world's citizens. Europeans, on the other hand, seem to share a more protective approach to privacy. This leaves plenty of room for data protection becoming a European success story, proving that Europe has the capability, know-how and state of mind to deal with the pressing issues of the 21st century. This could be the time to shine – proving that Europe has enough influence and reach, demonstrating its actorness to the world and even spread its standard against the stated preferences of the United States. Thinking this further and expanding this idea on other policy areas, this could even be a chance for the EU to give life to the aspirations of the European treaties, that aim to spread the EU's understanding of human rights around the world.

Data protection is becoming an increasingly important topic in daily life, fuelled by a constant barrage of privacy violations and breaches. Each and everyone's life is increasingly transferred onto digital devices and platforms; With these platforms knowing almost everything about us – just think about the intimate details your google queries reveal about you – in conjunction with advances in machine learning and artificial intelligence, that are able to make sense of human behaviour in an ever increasing measure, people's privacy is not only at risk, it is being breached on a daily basis, in plain sight. The data stored on these platforms can be monitored, analysed and monetised for commercial and political interests in very personal and potentially manipulative ways that were unthinkable only ten years ago. The individual can do little to protect him- or herself against these reaches into each one's private life, as usage of these platforms has become a necessity in modern societies – whoever is not on these platforms loses out on social life. Therefore, it appears that only the state can reasonably protect the individual by adopting legislation that builds fair and respectful rules for data usage and data protection.

Now putting all these considerations in a nutshell – data protection becoming an increasingly important topic for almost all citizens around the world and the fact that the EU has a seemingly citizen-friendlier approach of protecting data than the US, the question arises, if Europe's standards are already travelling around the world.

Therefore, this thesis is set out to answer two related questions: whether policy convergence is happening in data protection, and what that says about how policy convergence works, in context with the two opposing theoretical frameworks of Drezner and Bradford. These questions will not only firstly answer if the European data protection standard is being globalised; they will secondly also identify if the European Union is able to establish its standard against the preferences of the United States of America, thereby answering questions on the actorness of the EU; and thirdly provide an answer on a fundamental clash between two opposing theoretical camps.

In order to answer these two questions, this thesis is divided into seven parts. After this introduction, chapter two will introduce the field of policy convergence and the two theoretical frameworks as well as compare them on a general level. Chapter three will provide an overview of the relevant data protection frameworks in the world, so that the reader understands the different regulatory approaches to data protection. Following this, chapter four will explain the research design and used data. In this chapter, it will be explained how this thesis aims to use data collected from questionnaires sent to data protection authorities on the characteristics of their legislation to answer the question whether policy convergence is happening around the world. Chapter five will then take the data collected and answer the first research question. The second research question will be answered in chapter 6 by synthesising all the previously gained information on the theories, the data protection frameworks, the data on national legislation and by adding contextual information. The thesis will end with a conclusion, highlighting the most important inferences and suggesting a way forward.

2 Theoretical framework: Policy convergence theory

This chapter's initial purpose is to introduce the reader to policy convergence theory and to the writing of the two selected theorists. In this, firstly an overview of the field will be given. Subsequently, the conditions that the authors identify for policy convergence will be compared. Lastly, the two theories will be looked at more in-depth. The wider purpose of this chapter is to introduce the analytical framework used in chapter five to answer the first research question and to provide the necessary information for the analysis which of the introduced conditions are necessary for policy convergence, which will be performed in chapter six.

The seminally influential Colin J. Bennet defined policy convergence as "the tendency of societies to grow more alike, to develop similarities in structures, processes and performances" (1991, p. 1), a definition that has achieved broad consensus in the field (Knill, 2005, p. 765).

There is a multitude of different approaches to policy convergence theory (or as it is alternatively called, regulatory convergence theory), stemming from the many academic disciplines the authors originate from. There are related concepts such as policy transfer, isomorphism and policy diffusion, but due to this thesis's focus on the characteristics and change in similarity of policies, it will focus on policy convergence (Knill, 2005, p. 767). When analysing the causes and conditions put forth by policy convergence, Holzinger & Knill (2005, p. 778; Knill, 2005, p. 766) identify an increasing number of publications on the field in recent years, but also suggest a lack of "systematic theory-building" at the time. Drezner (2008, p. 3) concurs and writes that there is "increased scholarly attention on how the global economy is regulated in an era of globalization. However, the theoretical debates on this topic leave much to be desired."

It is clear when going through some of the theoretical writing on policy convergence that authors utilise a lot of overlapping conceptualisations, but use differing language to describe often similar concepts.

DiMaggio & Powell (1983) identify coercion, mimetic processes and normative pressures as deciding factors for policy convergence.

The seemingly most influential academic writing in the field of policy convergence, evaluated by number of citations,[1] comes from Colin J. Bennett (1991), providing an overview of the literature that existed at the time of writing and - possibly explaining the continued popularity - setting out to provide a guide for future research. He saw convergence occurring through emulation, elite networking, harmonisation and penetration.

Dolowitz & Marsh (2000) focus on the aspects of voluntary versus coercive convergence.

[1] 1417 citations per Google Scholar: https://scholar.google.se/scholar?cites=11880719927176825435

Hoberg (2001) classifies factors for increasing convergence as: parallel domestic problem pressures, emulation, international legal constraints and international economic integration.

Simmons & Elkins (2004) work with the term diffusion instead of convergence and see three mechanisms: direct economic competition, informational networks and social emulation.

In their influential paper[2], Holzinger & Knill (2005, p. 780) attempt to analyse the existing literature and summarise its scattered mechanisms and language into a single set of descriptors.

Mechanism	Stimulus	Response
Imposition	Political demand or pressure	Submission
International harmonisation	Legal obligation through international law	Compliance
Regulatory competition	Competitive pressure	Mutual adjustment
Lesson-drawing	Problem pressure	Transfer of model found elsewhere
Transnational problem-solving	Parallel problem pressure	Adoption of commonly developed model
Emulation	Desire for conformity	Copying of widely used model
International policy promotion	Legitimacy pressure	Adoption of recommended model
Independent problem-solving	Parallel problem pressure	Independent similar response

Table 1: Mechanisms based on Holzinger & Knill (2005, p. 780)

Next to these mechanisms, which will be utilised in chapter six, Holzninger & Knill also introduce a set of indicators. While *mechanisms* describe the process of policy convergence, i.e. how policy convergence happens, *indicators* describe the status of policy convergence, i.e. how far along the policy convergence process has got or whether it's occurring at all. The three indicators determining if policy convergence is present are: *degree*, *direction* and *scope of convergence*. This thesis will use these indicators as an analytical framework for gathering, systemising and analysing the data collected through the questionnaire in chapter 5.1 (Holzinger & Knill, 2005, p. 776).

The *degree of convergence* helps to determine whether policies across countries are similar enough to be deemed converging or not. Here Holzninger & Knill (p. 776) differentiate between policy outputs (the de-jure state of the policy) and policy outcomes (the de-facto state of the policy). The authors define how they measure the degree of convergence, which can simply be summarised as: The degree of convergence increases when policies become

[2] 633 citations per Google Scholar: https://scholar.google.se/scholar?cites=13481468155198106099

more similar. In their writing, they focus on policy outputs and this thesis will do so too. In relation to this, they state their opinion on why governments legislate: As a reaction to problem pressure, based on experience gained elsewhere, under pressure from powerful external actors, due to economic pressure and because of a legal obligation. These indicators make it possible to describe and analyse policy convergence, though they in themselves are not explanations for why the convergence happens. These aspects will be considered later.

The *direction of convergence* is related to the strictness of the regulation. *Laissez-faire*-policies are considered the "bottom", interventionist policies the "top". This categorisation is based on (Drezner, 2001), who has developed his own systematisation of the field. This dimension has a normative aspect, however, for example, in data protection strict regulation is often considered normatively good for the individual, even though it impedes the freedom of companies. It is therefore a question of values.

The *scope of convergence* describes the number of countries affected by the given "convergence mechanism" (Holzninger & Knill, 2005, p. 778).

I have adapted the indicators identified by Holzniger & Knill to use them as an analytical framework to systematise the data collected for my study. For this purpose, I have modified the research questions, simplified them for readability and removed the reference point, as it did not offer an increase in analytical clarity. The operationalisation was not modified.

Indicator	Research question	Operationalisation
Degree of convergence	To what degree have policies become more similar?	Decrease in standard deviation over time
Convergence direction	In what direction (strict or lenient) have policies developed?	Mean change
Convergence scope	Which (groups of) countries are converging in which direction?	Number of countries and policies

Table 2: Modified indicators table based on Holzninger & Knill, 2005, p. 778

2.1 Theory comparison

In this chapter I will introduce the two main policy convergence theories used in this thesis. They will provide the theoretical basis for the empirical discourse and be used to identify the conditions that are required for policy convergence. The first theory is Daniel W. Drezner's theory from *All Politics is Global* (2008). The second theory is Anu Bradford's *Brussels Effect* (2012). Both authors identify causes and conditions for regulatory convergence to happen and those will be introduced in this chapter.

Before starting the more detailed comparison of the two theories, it is necessary to make a couple of introductory distinctions.

It is important to understand that there is a difference between the *conditions for* policy convergence and the *causes of* policy convergence. Conditions are required for policy convergence to occur, but do not necessitate or guarantee it. Causes, on the other hand, are the actual trigger for it, the mechanisms, processes, events, that when the right conditions are met, will make policy convergence actually happen. This is an important distinction to make, but the authors in the field (and especially Drezner) do not very clearly differentiate between the two. As a side note, the trigger does not necessarily have to be an active process and initiated by the country whose law is being adopted, e.g. the mechanism "emulation" shows that third countries can take up part of another country's regulation by their own volition.

Secondly, it is important to differentiate between why a rule emerges as the global standard at all and why one *specific* rule is becoming that global standard. So, in other words, why it makes sense for governments to agree that there should be a global standard and why governments decide for some specific rule to be that standard. Holzninger & Knill look at why policy convergence happens at all, i.e. why states' regulation becomes more similar, but they do not look at why a specific standard is emerging. Bradford on the other hand describes conditions that make the regulation of the EU first de-facto and then de-jure the global regulatory standard, i.e. why one specific rule is becoming the global standard. In this regard Drezner is closer to Bradford than he is to Holzninger & Knill, as he is also mostly interested in why a specific standard becomes the worldwide standard, but he also covers aspects of why a standard is emerging at all. His scope is therefore a hybrid of the other two theories.

	Hozninger & Knill (2005)	Drezner (2008)	Bradford (2012)
Causes vs conditions	Causes	Hybrid	Conditions
Any rule vs a specific rule	Any rule	Hybrid	A specific rule

Table 3: Meta comparison Drezner & Bradford

Thirdly, what sets the Brussels Effect apart from other research on regulatory convergence is the more differentiated proposition on the conditions for why a particular regulatory standard becomes the global one. The most commonly mentioned factors determining regulatory convergence are *market power* and *economies of scale*, which Drezner also mostly focuses on, but Bradford arrives at a more nuanced systematisation. While *market power* is a part of the conditions, Bradford identifies additional factors that are not guaranteed to be present, but are required to be fulfilled for the effect to take place. With this, she proposes an alternative understanding why a certain standard is becoming the world standard to the established theories.

It should also be mentioned that Bradford is looking at the issue from the perspective of a regulator and not from a market perspective. Drezner takes a similar position here, as he is also only interested in the state perspective. Even though Bradford assumes private companies to have an important role through the *de-facto* effect, the rules still come from public actors. In her theory, private companies are only the middle man and do not play an active role. Therefore, all the conditions for policy convergence that she develops relate to characteristics of the government, not of a company. Companies are only part of the mechanism and the process begins and ends with governments. Drezner argues that "great powers – defined here as governments that oversee large internal markets – remain actors writing the rules" (Drezner 2008, p. 5) and thus agrees with Bradford. Even though Holzninger & Knill do not discuss the aspect of public versus private actorness, their assumptions clearly show they are considering the state to be the actor that shapes the global rules. There are some theories that suggest private organisations take a more leading role in globalised regulation (e.g. Büthe & Mattli, 2011), but I deliberately do not engage with those theories, as the policy field of data protection is a distinctly state-driven regulatory field.

In addition to this, Bradford makes an important distinction between *de-facto* and *de-jure* regulatory convergence. Previous research has concentrated almost exclusively on the de-jure effect, meaning when regulators or governments adopt the same or similar regulatory standard in law. Bradford crucially points out that this is not actually necessary for a global regulatory standard to emerge. Today, in many fields there is a high degree of consolidation in the corporate environment, with multinational, globalised companies being dominant players, being able to set standards for their supply chain, exporting the same product with minimal alterations to markets that are used to products being the same everywhere. This means that when such a multinational company commits to a regulatory standard, it can set the de-facto global standard in this field, making *de-jure* regulatory convergence just the codification of what is practiced already anyway.

2.2 Comparing conditions

Holzninger & Knill's framwork will mostly be used as an analytical framework. As they do not identify conditions, but causes, only Drezner and Bradford will be compared below.

Bradford argues that there are five conditions for the Brussels Effect to take place. According to her theory other territories in the world fulfil some of the conditions, but only the EU fulfils all and is therefore able to influence the global regulation. Drezner, on the other hand, identifies two conditions which are required to shape international regulation.

2.2.1 Market power

Drezner's two conditions for one standard actually succeeding in becoming the global standard are relatively simple. The first is the size of the internal market, as can be taken from Drezner's focus on it. He also suggests that currently, only the United State and the European Union possess enough market power to shape regulation, but they cannot do so in opposite directions, meaning both need to agree to make a rule the global rule (Drezner, 2008, p. 88).

Bradford also regards market power as a condition for regulatory convergence to happen. While she regards the United States, China and Japan to also have markets big enough to "use their markets as leverage", her view focuses more on the EU and she therefore points out that the EU (and EEA states) represent a huge single market where the same regulation applies, mandating that a good that can be sold in one member state can be sold in any other member state. Therefore, a company can produce one product for the whole single market. (Bradford, 2012, p. 11f.).

2.2.2 Regulatory capacity

For Bradford, regulatory capacity is set out to develop slowly from the market size of a country. Even though China has a very big economy, its regulatory capacity is limited by its “regulatory experience and institutional capacity to enforce their norms” (Bradford, 2012, p. 13). This benefits the EU and the US, as their historically grown economies give them an advantage in experience and capacity to make sound rules and enforce them, to the point of excluding them from market access. Even though the EU’s regulatory capacity is a newer development than the US's, it is based on the significant experience of its member states and did therefore develop quickly (Bradford, 2012, p. 12ff.).

Drezner does not consider this aspect.

2.2.3 Preference for strict rules

Bradford stipulates, that setting the strictest standard is a necessary condition to set the *de-facto* global standard, since if another territory would set a stricter standard, companies can no longer only abide by the first standard to satisfy all global regulatory requirements. On the one hand wealthier countries have a higher capacity to prioritise consumer protection over profitability, but on the other hand it is also a question of ideology. As opposed to the US, the EU follows the “precautionary principle”, meaning a product has to be proven safe before it can be sold. Though at points it seems Bradford simply regards Brussels as the most technocratic actor, giving it the most “stringent” rules. The US follow the opposite principle where a product has to be proven unsafe, so it can be banned from sales. This leads to more and stricter regulation from the EU system (Bradford, 2012, p. 14ff.).

Drezner does not consider this aspect.

2.2.4 Predisposition to regulate inelastic targets

Producers in elastic markets, such as finance, can engage in forum shopping, i.e. avoid regulation by changing their jurisdiction. This is especially true in case the product is immaterial. According to Bradford the EU is avoiding this by targeting inelastic markets, such as retail, as consumers in these markets do not change the jurisdiction in order to buy a product cheaper and companies therefore have to comply to the rules of the EU (Bradford, 2012, p. 16f.).

Drezner does not consider this aspect.

2.2.5 Non-divisibility of standards

Bradford explains that non-divisibility of standards occurs when it is cheaper for a company to comply only with one regulatory framework, based either on legal, technical or economic reasoning. This is essentially an economies of scale argument, where due to the products' characteristics, it makes economically more sense to produce one unified product. In this case that regulator is the most stringent regulator and adhering to its standards almost automatically will also satisfy the other regulatory frameworks, making other regulators unnecessary.

An example Bradford gives of a non-divisible standard is the chemicals market. Here companies only produce one range of products, comply to the European standard and sell it worldwide, because it is cheaper to produce one line under the higher cost of the stricter European market than it is to create a second line of products that conform to another set of regulations. An area where standards can be divided is labour standards. The EU has labour standards for EU workers, but does not regulate labour standards in general for products entering the EU. Companies can therefore choose to produce under different/lower standards in another jurisdiction and undercut the EU labour standards.

Drezner does not consider this aspect.

2.2.6 Usage of IGOs and NGOs

Drezner also envisions a crucial role for international governmental organisations (IGOs) and non-governmental organisations (NGOs). Harmonised standards require IGOs and NGOs for "regime management": forming and enforcing the standard. In case of a club standard (see next section), they act as "cheerlead[ers] on the sidelines" and with sham standards they "act as imperfect substitutes for state action". The great powers engage in forum shopping to maximise the use of these organisation (Drezner, 2008, p. 88).

Bradford does not consider this aspect to be a necessary condition.

2.2.7 Comparison conditions

Cause or Condition	Drezner (2008)	Bradford (2012)
Market power	Hybrid	Condition
Regulatory capacity	Not a factor	Condition
Preference for strict rules	Not a factor	Condition
Predisposition to regulate inelastic markets	Not a factor	Condition
Non-divisibility of standards	Not a factor	Condition
Effective NGO and IGO usage	Hybrid	Not a factor

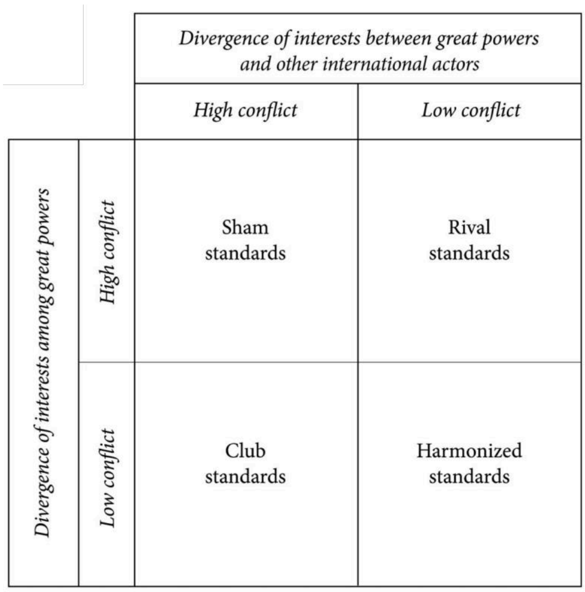
Table 4: Overview of causes / conditions of selected policy convergence theories per the authors

2.3 Drezner – All Politics is Global (2008)

International relations heavyweight Daniel Drezner[3] has informed[4] the debate on regulatory convergence in his much-reviewed game-theory based book *All politics is global: Explaining international regulatory regimes*. For Drezner adjustment costs are the main obstacle to a globalised regulatory regime, which he considers to be a natural result of globalisation, as such a regime reduces costs. Simply put, a globalised regime emerges when the adjustment costs for states are low. Starting form this point of view, Drezner seeks to answer what standard regimes emerge under which conditions. He argues that the size of the internal market is still the most important determinant of regulatory power, meaning that states still set the standard - here he agrees with Bradford. Where their opinions diverge, however, is in whether and why a single global standard emerges (Drezner, 2008, p. 32ff.). Drezner identifies only the US and EU, based on internal market size, as able to set global standards,

[3] Regular op-ed's for the New York Times, Foreign Policy, The New Republic and Foreign Affairs
[4] 985 citations per Google Scholar: https://scholar.google.se/scholar?cites=16659692181146125060

as they can force other states to join the standard by threatening to exclude them from their markets, applying coercive measures (Drezner, 2008, p. 38). He crucially proposes that the two powers cannot force each other to adopt a standard but need to cooperate to create a truly global standard together. They do this if they have similar interests (Drezner, 2008, p. 70). Great power cooperation is a necessary, but not necessarily a sufficient condition for the establishment of a global standard.



		Divergence of interests between great powers and other international actors	
		High conflict	*Low conflict*
Divergence of interests among great powers	*High conflict*	Sham standards	Rival standards
	Low conflict	Club standards	Harmonized standards

Table 5: Typology of regulatory coordination from Drezner (2008, p. 72)

Even when they agree, disagreement with other international actors can lead to “Club standards”. These emerge because the adjustment cost for other countries are high and they therefore choose to not join the common standard. In some cases, the two powers can still enforce their standard as the global standard, by using an IGO, such as the OECD, as a way to (usually slowly) spread their preferred rule to a number of states high enough to make it the *de-facto* standard in the world (Drezner, 2008, p. 75ff.).

Only when the US and EU as well as the other international actors agree can a truly harmonised standard emerge (Drezner, 2008, p. 72).

A "Rival standard" can emerge when one of the great powers is able to bring a significant number of other international actors on board with their standard, which can acquire a critical mass. This gives other states an incentive to switch to that standard (Drezner, 2008, p. 79f.).

When only one of the great powers tries to establish a standard, but finds no significant support among the other great powers and other international actors, a sham standard emerges. In this case there will almost certainly be no common global standard, as the market power of this standard is insufficient (Drezner, 2008, p. 81ff.).

If the two dominant rule setters disagree on a standard no global standard will emerge, since if the other international actors disagree there will either be a club or a rival standard, but no harmonised one (Drezner, 2008, p. 72). Therefore, Drezner believes that neither great power can establish a standard on their own. In contradiction to this, Bradford considers that the EU has a bigger capacity to set the global standard, based on its more stringent regulatory process.

2.4 Bradford - The Brussels Effect (2012)

Anu Bradford coined the term “Brussels effect” in 2012, seeking to explain how private companies and governments worldwide are signing on to Brussels regulations. Bradford suggests that “the EU is currently the predominant regulatory regime that can wield unilateral influence across a number of areas of law” (Bradford, 2012, p. 10).

The Brussels Effect is based on two theorems on the US state-level. The first one is the "Delaware Effect" and describes how states lower their standards or offer incentives to companies to be incorporated in their territory, thereby engaging in a race to the bottom. The "California Effect", on the contrary, explores the opposite dynamic. Since California is a huge market in the United States for companies to sell their products in and has a tendency to set strict standards, it has effectively often set the standard for the whole country and has therefore caused a race to the top (Bradford, 2012, p. 5).

> *Example 1 – Delaware effect*
>
> A relevant example of the Delaware effect is the competition to house the second headquarters of Amazon. A number of US cities (and Toronto) are in a race to the bottom to attain the tax revenue, affluent residents and image boost that being the second home of Amazon would bring, offering everything from deep tax breaks to giving away precious land for free. Here, the Delaware effect can be observed, as these cities are lowering their standards to attract a company. This is a situation where market access is not relevant and the ability of a single (devolved) government to prevent a race to the bottom is therefore very limited. Cities could negotiate common standards to prevent a race to the bottom and thereby engage in a localised version of "political globalisation of regulatory standards", but there is a risk of defection or betrayal. In line with the prisoner's dilemma in game theory, cities choose to not cooperate. In the absence of a higher level (federal) government or competition agency that is able and willing to set a common standard, a race to the bottom occurs.

> *Example 2 – California effect*
>
> The California effect is typically associated with environmental policy in the US. With the US federal government not being at the forefront of progressive environmental policy, California has historically picked up the slack. David Vogel (1995) discovered that often other states match the strict level of environmental protection without any legal requirement: California's "standards remained stricter than those of any other state. In 1990, Congress brought national emission standards up to California's and once again permitted California to impose stricter standards. It also gave other states the option of choosing either national or California standards. In 1994, 12 eastern states requested that the federal government permit them to adopt California's new standards. These standards are in turn likely to become the basis for the next round of federal minimum requirements" (Vogel, 1995, p. 259).

The Brussels Effect also seeks to debunk trade liberalisation theories of a "global race to the bottom" when it comes to standards, as the strict rules of the EU is one of the very reasons its standard is being taken up worldwide (Bradford, 2012, p. 4). This will be further investigated in chapter six.

Bradford proposes two types of the Brussels Effect, one following the other: the *de-facto* Brussels Effect and the *de-jure* Brussels Effect.

The *de-facto* Brussels Effect describes what one would arguably instinctively presume the Brussels Effects means when being made familiar with the theory. Based on the five conditions for unilateral influence that Bradford develops (*market power*, *regulatory capacity*, *preference for strict rules*, *predisposition to regulate inelastic targets*, *non-divisibility of standards*), multinational companies are choosing to adhere to a single rule for its product standards and choose the European one. This means that the Brussels rule is made the *de-*

facto global rule, the rule that companies and consumers adhere to and experience, without any legal obligation to do so from the local government (Bradford, 2012, p. 5f.)

The *de-jure* Brussels Effect is the next step in this process. Globalised, non-EU companies, having adopted the rules, now advocate (their) local governments to adopt the EU standard to create a level playing field for all companies and countries. When governments adopt the EU rule, they codify the *de-facto* standard in law, creating a *de-jure* rule (Bradford, 2012, p. 6).

3 Data protection frameworks

This chapter's initial purpose is to introduce the reader to the origins and development of data protection as an academic field as well as a legal and fundamental right. In this, the growing importance and relevance of this field should become apparent. Secondly, the chapter will explain the differences between the various data protection frameworks in the world. The wider purpose of this chapter is to help the reader understand what the key differences of the frameworks and the thinking behind them is, which will be important for the analysis in chapter five and six.

3.1 Terminology

Neither privacy nor data protection are defined legal terms and even legal professionals have struggled to find a common definition of the terms, with none prevailing and the terms being left in some degree of accepted vagueness (Finn, Wright, & Friedewald, 2013). Additionally, there are regional differences in the usage. For the purpose of this thesis, it is therefore important to clearly define what the term encompasses and what it doesn't.

3.1.1 Privacy

Privacy is often referred to as the overarching term and the earliest academic definition in 1890, by Warren and Brandeis in the Harvard Law Review, attempted to box it in as "the right to be left alone" (Hijmans, 2016, p. 39).

It usually includes the terms of data protection and data privacy as more modern developments, relating to the collection of data about a person. To this day there no agreed upon definition for privacy. In an attempt to narrow down the concept, Finn, Wright & Friedewald (2013) suggest seven types of privacy, which help close in on what privacy actually means.

- Privacy of the person (keeping body functions and body characteristics private)
- Privacy of behaviour and action (keeping habits, activities and practices private)
- Privacy of communication (keeping analogue or virtual communication private)
- Privacy of data and image (exercising control over data and its use)
- Privacy of thoughts and feelings (exercising control over the sharing of thoughts and feelings)
- Privacy of location and space (the right not to be identified, tracked or monitored in public spaces)
- Privacy of association (the right to associate freely with whomever without being monitored)

3.1.2 Data protection

In the US the term data protection usually means the protection from unauthorised access (or access, use, disclosure, modification, and inspection of information) to data. This definition is close to the widely accepted definition of information security.

In contrast to this, data protection in Europe usually refers to the regulation of authorised processing of data by legal means and has no direct connection to concepts of information security. This makes sense considering the term was developed in the 1970s, where the possibilities of information technology did not make such thinking necessary yet (Guaman, 2016).

In this, one of the main divides between the US and Europe is already visible. While the US view is mainly concerned with illegal access, the European point of view is informed by its history and considers data to be a threat to fundamental rights, unless correctly regulated.

3.1.3 Data privacy

Data privacy, on the other hand, has a similar meaning in the US to the European understanding of data protection: in relation to regulation. The term is not so common in Europe outside of the United Kingdom, but is gaining traction, possibly due to the effort of making data protection less a technocratic exercise. The term *data protection* implies that what is being protected is the data, not the person the data is relating to (Hustinx, 2013, p. 1; Bygrave, 2012, p. 26). Even though this is not how the term is meant, it devaluates its relevance for people. Data *privacy* on the other hand has a connotation that brings it closer to the individual, due to the established relevance of "privacy" for an individual. On the other hand, other authors have criticised the term *privacy* for implying it is given to someone and it not being a right, while data protection implies an obligation (Martineau, 2018).

In this thesis *data protection* and *data privacy* are being used synonymous, as relating to the regulation of data processing.

3.2 Origins of Data Privacy

Privacy as a general concept was already included in the 1950 European Convention on Human Rights (ECHR) of the Council of Europe (CoE): Article 8 codifies in general the "Right to respect for private and family life". All member states of the Council of Europe have to ratify the Convention (Council of Europe, 1950). In addition to this the 1948 UN Universal Declaration of Human Rights similarly proclaims the protection of privacy (United Nations, 1948).

Data privacy legislation has become a topic of legal discussion since the 1960s with the introduction of electronic personal data collection and processing technologies. Where the right to privacy protected the individual's freedom to be left alone, the right to data privacy is resulting from the increased loss of control of the individual over its own information and the power asymmetry between the individual and the data controller (Hijmans, 2016, p. 48). The first data privacy legislation of the world was adopted by the German State of Hessen in 1970. Shortly thereafter, in 1973, Sweden was the first country to adopt its own data privacy legislation. Both these countries already then adopted comprehensive data privacy bills. In contrast to this approach, the United States adopted in the same year the "Fair Information Practices" (FIPS), which only mandated broad guidelines for governmental information processors, but no general right to data privacy. This approach has been adopted in many countries outside the United Sates (Tikkinen-Piri, Rohunen, & Markkula, 2018).

3.3 Data Protection as a fundamental right

Today, the right to privacy and the right to data protection are protected as fundamental rights in the legal order of the European Union, both by the Treaty on the Functioning of the European Union (TFEU) and the Charter of Fundamental Rights of the European Union (Charter).

As fundamental rights, in Europe the right to privacy and data protection are both seen as "civil and political rights and as a reflecting human dignity" (Hijmans, 2016, p. 62). A common theme among professionals and researchers in the field can be observed in their description of the rights' purpose to not let individuals be reduced to *just a data point*, to not be *something less than an individual*, to *having a unique value* (Hustinx, 2013, p.1). Mireille Hildebrandt has eloquently elevated this understanding describing the purpose of privacy as "protecting what is uncountable, incalculable or incomputable" (Hildebrandt, 2017, p.1). Her discourse is influenced by the most recent developments in computer science, where computer systems are able to, to some degree, simulate human intelligence meaning they form artificial intelligence (AI). The technology known as machine learning (ML) differs from traditional computer systems in that it is not programmed by humans. In traditional computer systems every response is in some degree pre-programmed by a human. Machine learning uses vast amount of data to develop an understanding for patterns and has the ability for inexact reasoning even with incomplete, uncertain or fuzzy data (Negnevitsky, 2005).

> Example 3
>
> A popular example is machine learning being able to reliably differentiate between a female face and a male face after having been fed thousands of pictures of either. The issue with machine learning becomes visible by this example, as it is still bound to the quality of data and categories it was trained on. Machine leaning is increasingly used for automated decision making, where it is becoming more and more usual to make decisions that were, in the past, made by humans. But machine learning is also inheriting issues - issues of biases inherited from data, which is based on human thinking, are increasingly appearing. For example, machines today are used to predict if convicted criminals will be able to re-socialise, determining their handling by the court. For this the machine is profiling the convicted and makes a recommendation that judges tend to follow. Researchers found out though that the machine was reproducing established biases towards people of colour and therefore was giving more negative predictions for that ethnic group than for other ethnic groups (Rieland, 2018).

People often trust the conclusions of machines as "objective" and therefore tend to scrutinise it less intensely. This shows why automated decision-making bears great risks. For this reason, automated decision making has been restricted in European data protection laws, so that individuals can object to being subject to it. Hildebrandt sees the risks for the individual and society inherent to these technological developments and therefore, as other authors have too, theorises private data to be removed from these systems, so that there remains an "incomputable" self (Hildebrandt, 2017, p. 9).

While Europe is certainly the frontrunner when it comes to establishing privacy as a fundamental right, there are indications that other countries and regions are increasingly embracing the European thinking on this question. For example, on 24 August 2017 the Indian Supreme Court ruled that privacy is a fundamental right per the constitution of India. It cited a familiar reasoning “the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone". The case related to the collection of biometric data, a category of data that cannot be processed under normal circumstances under European law but has come under increasing pressure to be used for various purposes such as security or profiling. The Indian Supreme Court has recognised this development, saying “technological change has given rise to concerns which were not present seven decades ago” (Figarella, 2017). The right to privacy is also recognised in the Brazilian, Jamaica, Mexican, Nigerian, the Philippian and South African constitutions (Privacy International, 2018). After the publication of the Cambridge Analytica scandal, even in the United States calls for a comprehensive data protection law became louder, with some congressmen suggesting to adopt GDPR-style legislation during a hearing of Facebook boss Mark Zuckerberg (Hautala, 2018).

3.4 Frameworks

3.4.1 Overview of data privacy regimes

See table 17, for an overview of the data protection regimes with international reach used in this thesis. See the annex for an overview of the presence of specific principles in the frameworks.

The UN also has developed privacy guidelines but since they have little to no influence in the world they have not been included here (Bygrave, 2014, 51ff.).

3.4.2 Council of Europe Convention 108

The Council of Europe Convention 108 is, in terms of its content, very similar to the OECD guidelines (see next section), as they were created in cooperation with each other, concurrently. While the Council of Europe Convention is more concerned with fleshing out Article 8 of the ECHR, the OECD guidelines take a more economic view, emphasising the importance of data for economic development. The Convention is a multilateral treaty, meaning it is binding, but only when countries accede to it. As of time of writing 46 of 47 Council of Europe members have ratified the Convention. EU accession is technically possible since 1999, but not yet in force (Bygrave, 2014, p. 32, 44).

The core principles can be reviewed in the annex, in table 18. As the Convention, together with the OECD guidelines were the first of its kind, all these principles were new and today form the basis of many data protection laws. Itself, it was mostly influenced by the emerging national data protection legislation in Sweden, Germany and Belgium of the early and mid 1970s. In 2001, an Additional Protocol was added to the Convention, giving it more detailed rules on transborder data flows and data protection authority role (Bygrave, 2014, p. 32f.). Since 2012 it was attempted to modernise the Convention, but this has failed due to resistance of Russia, as all signees need to agree. For this reason, the Convention Consultative Committee has decided to pursue the creation of a new, more robust Convention, to which all countries have to accede anew.

In regard to its own influence, the Convention always had an implicit global aspiration: Council of Europe members can invite non-members to accede, but this option had not been made use of. In 2005 the global conference of Data Protection and Privacy Commissioners called on the CoE to "invite, in accordance with article 23 […] non-member-states […] to accede to this Convention" (Data Protection and Privacy Commissioners, 2005) and in reaction to this the Convention Committee suggested in March 2008 to the member states to allow accession requests by non-members, which the member states followed, making it an open convention. In 2009 the EU in its Stockholm programme called on the Council of Europe to promote the Convention worldwide, demonstrating also the similarities to the EU standard. Uruguay has been the first beneficiary of this new procedure, in 2011 (Greenleaf, 2012). As of writing, nine non-members have been invited to accede to the Convention: Argentina, Burkina Faso, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and the aforementioned Uruguay. It is apparent that only Mexico and Argentina can be regarded as major economies, as they hold position 15 and 21 in the global GDP rankings per the United Nations, respectively, (United Nations, 2017) and the other countries have a relatively small weight in the global economic system. Due to the small number and limited economic weight of states, the influence on their accession to the Convention to the global regulatory system can be regarded as having a symbolic rather than a real economic impact.

3.4.3 OECD guidelines

As mentioned, the OECD has developed its own data protection framework in close cooperation with the Council of Europe but arrived at somewhat different results. The guidelines are more business-friendly, as countries should avoid "unjustified obstacles to transborder data flows", that according to the head of the expert group, who drafted the guidelines could results in "a cacophony of laws, which did little to advance human rights". In addition to this the guidelines are non-binding for OECD member countries. The present principles can again be taken from table 18, but what can be said is that while similar to the Convention 108, it is omitting some important protections and rights and can therefore be regarded as the laxer framework. The guidelines were revised in 2013, after an extensive assessment, but the eight principles and its non-binding nature remained essentially unchanged. The only noteworthy change is the addition of a recommendation to establish "privacy enforcement authorities", similar to the additional protocol of the Convention and the EU Directive (OECD, 2013). While the Convention has been very influential in Europe, the OECD guidelines have been more influential in other parts of the world, particularly in countries bordering the Pacific ocean up until the 2000s and has been touted to have had a significant influence on the APEC Privacy Framework of 2005 (Birnhack, 2008, p. 6; Bygrave, 2014, p. 44ff.; OECD, 1980).

3.4.4 EU Directive 95

In 1995 the EU passed a Directive on data protection and although the Commission seems to have also been driven by a desire to protect fundamental rights, it has, similar to the OECD Guidelines, mainly tried to prevent contradictory national data protection laws, which would have had negative consequences on the internal market. The Directive has though spearhead a development of incorporating human rights into the EU legal system, being the first directive to expressly be based on the protection of human rights. (Bygrave, 2014, p. 57). These two aspects neatly demonstrate that the Directive is caught between the protection of the right to privacy and the ongoing process of realising the single market. As was noted before, the EU supported and supports the Convention 108, but as it had not gained many accessions by the early 1990s, the Commission decided to start work on a binding legal act for the EU (Bygrave, 2014, p. 55).

In terms of its content, the Directive is visibly based on the Convention 108, but goes beyond it in multiple areas. In its recitals (legislative notes that contextualise the act's articles) the Directive makes a direct reference to Convention 108 and sets out to "amplify" it (European Union, 1995). Details in regard to the principles of the Directive can be viewed in table 18.

The Directive introduced the adequacy decision system, which was continued by the replacement Regulation GDPR. The adequacy system essentially requires countries that want to be able to receive personal data concerning EU citizens to adopt data protection laws at least "adequate" to the EU standard (Birnhack, 2008, p. 9; European Union, 1995). In this, an adequacy decision can be a major competitive advantage for a country, as only then cross-border processing of EU personal data can be done legally. Not having an adequacy decision can lead to companies not choosing to be based in the given country. In this, the system has also been described as a relatively aggressive measure (Birnhack, 2008, p. 3). Until the in force of the replacement, the GDPR, the Directive was clearly the most stringent and restrictive data protection framework in the world.

While the Directive 95 has certainly had some influence, Bennett notes that "nowhere has the Data Protection Directive been the sole reason for another country's passing a data protection law" (Bennett 1997, 2001 as cited by: Birnhack, 2008, p. 13). The adequacy decision has certainly resulted in some level of adoption of similar rules, as countries which want to do serious trade with the European Union need to obtain an adequacy decision from the European Commission, that their data protection law provides a comparative level of protection as the European one. According to Birnhacker, countries that have adopted legislation aspiring to approach the Directive are: Australia, Argentina, Hong-Kong, Israel, Japan, South Africa, Chile, Colombia, Mexico, Uruguay and New Zealand. Of these only Argentina, Israel, Switzerland and Uruguay actually managed to obtain an adequacy decision from the Commission. Notably, the United States obtained a quasi-adequacy decision from the Commission based only on self-certification of US companies, showing that economic weight also plays a factor (Birnhack, 2008, p. 15).

3.4.5 APEC Privacy Framework

APEC is an Asia-Pacific regional economic forum with 21 members, including most bigger countries in the area, established to promote growth and wealth creation. These states adopted an own framework in 2003. Bygrave notes the difference in motivation in relation to the EU approach. While the Directive had a dual-purpose: the protection of privacy and enabling the single market, the APEC guideline „appears to foster data privacy regimes less because of [a] desire to protect basic human rights than to endanger consumer confidence in business" (Bygrave, 2014, p. 75), no mention is being made of privacy as a fundamental right. It therefore makes sense that the APEC guidelines state its core principles coming from the less-strict OECD guidelines and not the Convention 108 or EU Directive (Asia Pacific Economic Cooperation, 2005, p. 3) and that the standard is not legally binding.

The principles can be viewed in table 18. It is apparent from that view that the framework is by far not as restrictive as the European approaches to data protection. The framework is mostly picking up a subset of not-too-invasive principles from OECD and European data protection law and has been dubbed "OECD lite" (Bygrave, 2014, p. 77). New is a "preventing harm" principle, of which the consequences remain unclear though. The APEC countries revised their 2005 guidelines in 2015. While the previous guidelines were based on the 1980 OECD guidelines, the 2015 revision is itself based on the 2013 revision of the OECD guidelines. As the OECD system was barely touched in its revision, the APEC Guidelines can be seen as a continuation of the 2005 rules (Birnhack, 2008, p. 8; Bygrave, 2014, p. 78ff.; Greenleaf, 2009, p. 8).

In terms of the influence of the Guidelines, Asian data protection law expert Graham Greenleaf (2009) takes a critical position. As the law is non-binding and its provisions only "a floor, not a ceiling", they had no influence on countries in the region that already had data protection laws, as they usually provided at least the same level of protection. Countries that were developing new laws were said to orient themselves more toward the higher European standard and the APEC Guidelines therefore represent "a floor on which no one seems to be dancing" (Greenleaf, 2009, p. 7)

3.4.6 ECOWAS Supplementary Act

In similar fashion as in the Pacific region, data protection is being led by a regional body in Africa. The 15 members strong Economic Community of West African States (ECOWAS) has adopted a "Supplementary Act on Personal Data Protection" to its main treaty in 2010, making it a legally binding part of membership. As opposed to the APEC framework, the ECOWAS act is though not primarily concerned with economics, but is clearly rooted in "the promotion and protection of human and peoples' rights" (ECOWAS, 2010). In this it is an instrument that shares many principles with the European frameworks (see table 18 for reference) and in some areas, such as automated decision making is even going further than the European ones. According to the NATO Cooperative Cyber Defence Centre of Excellence, the ECOWAS supplementary act has been strongly influenced by the EU Data Protection Directive (CCDCOE, n.d.). On the side of the ECOWAS act, it has influenced and spurred further development of data privacy regulation in Africa, as a reaction the African Union has drafted a cyber security and data privacy convention for the continent, but the ECOWAS Supplementary Act had little to no influence outside of Africa (Makulilo, 2016, p. 377).

3.4.7 GDPR

The replacement of the EU Directive 95, the General Data Protection Regulation (GDPR) will result in a harmonised data protection standard in the EU. This means that a market of 500 million citizens (the UK has already committed to the standard for after Brexit) will be covered by the same set of rules, with some smaller possibilities for national customisation. The GDPR is clearly continuing in the footsteps of the Directive but adopting them in the face of changed data processing in the age of big data. Many principles have been adapted to be more robust or stringent and the Regulation is more restrictive in general in terms of data processing. For the principles, see table 18. The GDPR probably represents the strictest data protection law in the world and is based on an understanding of data protection that seems unique to Europe. It expands the basic rules of the Directive to give them applicability and enforceability. Continuing and strengthening the Adequacy decision system, a company offering services in the EU, even if not situated in the EU, or offering online services only must abide by the rules and therefore the GDPR is exerting a sort of extraterritorial jurisdiction.

The influence of the GDPR is difficult to ascertain, as it is in the process of becoming applicable, but it has certainly caught the attention of regulators and companies worldwide and has been described as everything from a hype to craze (Lahiri, 2018; Rowntree, 2017). One of the main aims of this thesis is evaluating the degree of the influence the GDPR has had on the world.

3.4.8 The US framework

The United States has a “patch-work” of sectoral or type-specific laws, covering only sensitive information and no single, comprehensive federal law. Protected is only very specific health information via the Health Insurance Portability and Accountability Act (HIPAA) of 1996, some protection in the ICT sector via the Computer Fraud and Abuse Act (CFAA) of 1986 and the Cybersecurity Information Act of 2015 and in finance with the Bank Secrecy Act of 1970 (BSA). No single data protection regulatory authority exists, even though the Federal Trade Commission (FTC) has used some of its executive powers to enforce privacy rights. Data protection in the European sense only exists for children under the age of fourteen with the Children’s Online Privacy Protection Act (COPPA) (O’Connor, 2018). In addition to this, the United States has a myriad of state level legislation for any number of sectors (Safari, 2017). Lastly also the Privacy Act of 1974 exists, but only covers a limited scope in the public sector (United States, 1974). Since there is no single and comprehensive law giving rights to the general public, the United States are coded to not possess a data protection law and are therefore not represented in table 18.

This patch-work has resulted in multiple data breaches in the US being insufficiently handled, as no legal obligation exists. Companies like Uber have attempted to hide a data breach by for example trying to buy the data off the black market, while still being investigated for another data breach. No fines have been imposed (Bloomberg, 2018). Other companies, like credit rating company Equifax, have lost essentially all their customer data to hackers and have waited punishably long to disclose a breach, robbing users of the possibility to immunise themselves against the misuse of data (Fung, 2018). Based on these developments and as has been noted, the United States is today closer to ever to actually adopt a comprehensive data protection law.

———

4 Research design and data

This chapter's purpose is to explain to the reader what the two research questions are and how they will be answered. It will explain how data from data protection authorities was gathered to answer the first research question and how the second research question will be answered as a synthesis of the all the previously gathered information.

4.1 Research questions

Drezner and Bradford both believe in states shaping the conditions for a standard to emerge as the global standard, but don't believe in the same causes and conditions. Both authors use data protection as an example to prove their theory and by doing this, they also make it a crucial case study for their theory. If the theory does not hold up for this example, that is after all chosen by the author him- and herself, the validity of this theory has to be seriously called into question (George & Bennett, 2005, p. 33). They cannot both be right; therefore, data protection is an optimal choice for a case study.

Drezner and Bradford both use data protection as an example for proving their theory, but they use it to opposite ends. Drezner uses data protection to prove that neither of the big powers (the EU and the US) has managed to establish a standard in opposition to the other, meaning that no global standard has emerged or can emerge. Bradford uses it to prove that fulfilling her conditions can lead to exactly the opposite, meaning that a global standard does emerge. To say it simply: Something has to give.

But before getting into that, the data I generate will first help to answer a less theoretical and more practical question:

RQ1. Is global regulatory convergence happening in the field of data protection regulation?

This question has two sub-questions: Firstly, whether any data protection standard at all is emerging as the dominant standard in the world; and secondly, whether the European Union is successful in establishing their standard, a popular assumption in policy circles.

As for the conditions and causes for regulatory convergence, both Drezner and Bradford agree on market power being paramount, but only Drezner assigns an important role to NGOs/IGOs. Meanwhile Bradford has four other further conditions (*regulatory capacity, preference for strict rules, predisposition to regulate inelastic markets, non-divisibility of standards*). In chapter 2, I have shed some light on where they agree, where they are in conflict and why. In what follows I aim, using the data I generated for my case and combining it with the academic writing in the field, to generate some clarity about which of their conditions are actually important and applicable and which new ones can be added. Therefore, my second research question is:

RQ2. What are the conditions for global regulatory convergence, based on the example of data protection regulation?

4.2 Is there convergence in data protection regulation?

To answer the first research question, I will analyse the prevalence of different data protection principles in the world's data protection legislation. For this I have identified the principles of the nine most influential data protection frameworks (see table 18 in the appendix). There are five influential intergovernmental organisations that have developed their own privacy frameworks. The OECD, the Council of Europe, the EU, APEC and ECOWAS all have one. The UN also has its own, very similar to the OECD standard, but it has never gained much influence in the world (Bygrave 2014). Most of these frameworks have undergone revisions, and I have therefore identified a total of nine versions of these frameworks (see table 6 for an overview).

I have gone through these frameworks and with the help of additional secondary literature (mainly: Bygrave 2014; Tikkinen-Piri et al., 2018; de Hert & Papakonstantinou 2014; Greenleaf 2012; Hijmans 2016) identified the main principles of each framework. I did this in a chronological way, starting from the oldest and working my way up to the newest. Doing this I arrived at the principles described in table 18, which shows which principles are reflected in which privacy framework. The next step was to then collect data on which data protection principles are reflected in the world's data protection legislation. For this purpose, I have created an online questionnaire, asking data protection authorities to fill out which principle is present in their law or whether there is a law at all.

Asking data from data protection authorities ensures that the information one receives is reliable, as these authorities are the foremost experts on the legislation in their country. The data protection authorities were identified based on a multitude of structured and unstructured resources. The main resources, besides desktop research for the authorities on governments websites were: Asia Pacific Privacy Authorities, 2018; BakerHostetler, 2016; DLA Piper, 2016; Greenleaf, 2017; International Association of Privacy Professionals, 2018; International Conference of Data Protection & Privacy Commissioners, 2017; United Nations Conference on Trade and Development, 2017.

To collect the data, the questionnaires were sent to the authorities via email, some authorities were also called to increase the response rate. Since the response rate to the email survey was quite low and the extensive amount of work required to get replies from data protection authorities (over 500 emails were sent, around 25 calls to authorities resulted in a few additional completed surveys), desk research was employed to complete some unfinished questionnaires. For this the law itself and secondary literature was employed (BakerHostetler, 2016; DLA Piper, 2016), to ensure the data is reliable. Through this the data protection legislation (or lack thereof) of a total count of 26 countries could be analysed (see table 7).

The last step was to analyse the amount of times the principles of each framework were represented in the data that was gained. As I had data on where each principle has its origin, I was able to make inferences on which of the frameworks are dominant in the world. To make these inferences, I used the analytical framework provided by Holzninger & Knill introduced in chapter 2.

4.3 What are the conditions for convergence?

To answer the second research question, I will take the theoretical information I gained in chapters two and three and confront it with the data collected through the questionnaire. There is a simple and a more complex approach to this question.

The simple approach is to just answer who of the two authors is right and who is wrong. Looking alone at how Drezner and Bradford structure their theories, they immediately disagree whether convergence could happen in data protection. Drezner says it cannot happen, as the US and the European Union disagree on the topic and therefore, according to his theory, there cannot be a global standard. Bradford, on the other hand, says it is happening, because the EU as an institution fulfils all the necessary conditions that she sets. As mentioned before, one of them has to be wrong.

The more complex approach to the research question is to find which causes and conditions actually are required for regulatory convergence to happen and which ones are not relevant. To be able to answer this question, all previous findings will be employed. This means both authors theories, the information on the data protection frameworks, the conclusion on the first research question, both authors writings on the application of their theory on the data protection case and further contextual information.

4.4 Sample

Through the questionnaire, 26 answers were received (see table on the right). Out of that number, 15 questionnaires were completed by data protection authorities, 4 by information commissioners, 2 by government ministries, 1 from a National CSIRT (National Computer Security Incident Response Team, an agency that is in charge of handling data breaches, among other things). 4 replies were started by authorities but not finished; for these I have completed the questionnaire using the law text and secondary literature.

Respondents answered for their own country. 12 answers are from non-EU European countries. EU countries were not surveyed as the GDPR is replacing all national legislation and the GDPR was already analysed as one of the privacy

Single, comprehensive law
Africa
Benin
Ghana
Mauritius
Morocco
Senegal
Americas
Canada
Chile
Mexico
Asia
Philippines
Europe (excluding EU)
Albania
Andorra
Bosnia and Herzegovina
Faroe Islands
Georgia
Gibraltar
Isle of Man
Kosovo
Moldova
Montenegro
Ukraine
Draft law
Africa
Uganda
Americas
Honduras
Europe (excluding EU)
Liechtenstein
Multiple (sectoral) laws
Africa
Sierra Leone
Asia
Mongolia
No law
Americas
Paraguay

Table 6: Questionnaire replies

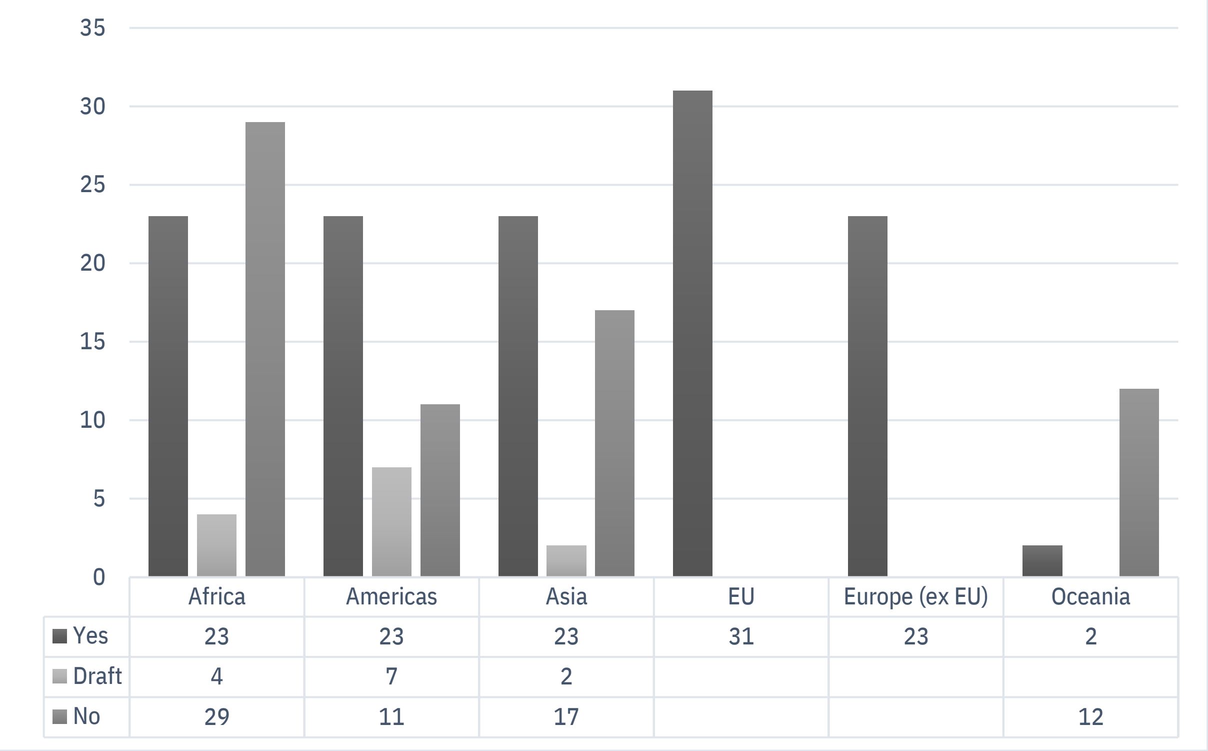
frameworks. 7 replies were from African countries, 5 from American and 2 from Asian countries.

Out of the respondent countries, 20 have a single comprehensive data protection law, which the answers were based on. 3 countries have a draft law, 2 of which have no existing law and 1 is in the process of recasting the country's existing law. 2 have no single comprehensive law, but multiple laws covering different sectors. Finally, 1 respondent country has no law at all and therefore no data protection framework.

From the countries with laws, 2 adopted their laws in the 1980s, 1 in the 1990s, 11 in the 2000s and 9 in the 2010s.

Apart from asking respondents on what data protection principles are present in their legislation, they were also asked if their country either has, is in the process of or is planning to amend their legislation in response to the adoption by the EU of the GDPR. This question was replied to in the positive by 21 respondents and negatively by 5, which means the countries that are amending their legislation in response to the GDPR is more than 5 times higher than that of those who do not. Countries in Europe and Africa almost all replied that they would amend their legislation, with only 1 country per region answering that they would not. Both Asian countries replied they would amend their legislation. On the other hand, in the Americas 3 out of 5 countries replied that they would not be amending their legislation.

Before delving in-depth into the actual data protection principles, I want to contextualise the questionnaire data and consider its relation to the more general data set. As mentioned before, I used desk research to collect information on countries' data protection laws and data protection authorities around the world. This data can be inspected in table 19 in the appendix.



	Africa	Americas	Asia	EU	Europe (ex EU)	Oceania
■ Yes	23	23	23	31	23	2
■ Draft	4	7	2			
■ No	29	11	17			12

Table 7: Existence of data protection laws by region

Comparing the questionnaire sample with the whole set of data protection laws in the world, it is clear that non-EU European countries are overrepresented, while Asia is underrepresented. Oceania does not feature in the sample, but only two laws exist in this area (Australia and New Zealand).

There is no European country without a data protection law, proving the continent's spearheading of the policy field. The 28 EU countries have had a constant stream of new laws since the early 1970s, with many Central and Eastern European countries adopting legislation after the 1990s. The last EU countries to adopt such legislation are Estonia and Croatia, in 2003. The non-EU countries generally started to adopt legislation at a later time and with less speed, though they kicked up the pace in the 2000s. Turkey was the last to adopt data protection legislation, in 2016.

The Americas and Asia have been on a largely coupled trajectory, only starting to adopt legislation on a wider scale in the 2000s, with both regions now roughly split between countries having legislation and countries having none. Since 7 countries in the Americas are now discussing a draft law, it can be expected that a significant amount of countries in the Americas will adopt data protection legislation in the near future.

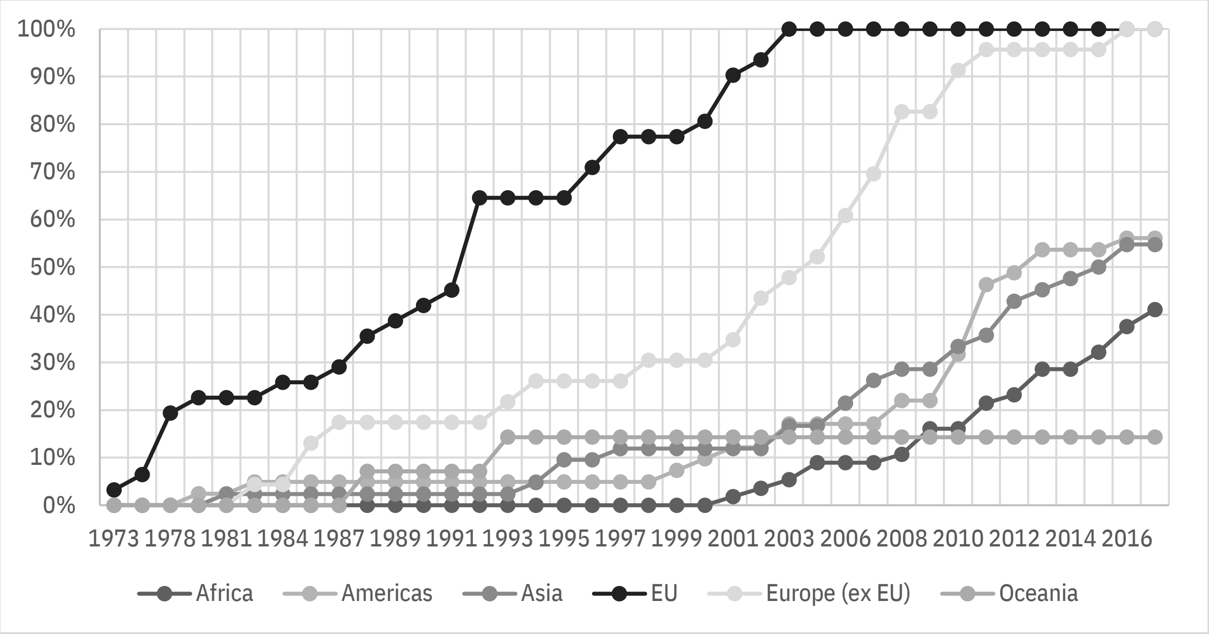


Table 8: Development of data protection laws by region

African countries were the last to begin the adoption process, also in the 2000s, but their continent has seen a constant output of legislation since then, now almost reaching parity in terms of number of countries with laws and number of countries without. Australia and New Zealand adopted their data protection legislation quite early, but none of the island states in Oceania have followed them.

When it comes to the presence of a data protection authority, a key principle of European data protection law, European countries are again leading the pack with only 2 countries having none. Africa, Asia and the Americas all have 6 to 9 countries that have legislation, but no data protection agencies. Due to the unclear situation for some countries, again mainly in

Africa, Asia and the Americas, for some countries the presence of data protection authorities is marked as "unknown". This is the case where data protection legislation exists and actually demands a data protection authority, but no such authority could be identified. In these cases, the authority might not have been established yet, or does not have much or any information available to the public. In Oceania all countries that have data protection legislation have appointed an authority for it.

Region	Yes	No	Unknown
Africa	17	34	5
Americas	16	17	8
Asia	13	22	7
EU	31		
Europe (excl. EU)	20	2	1
Oceania	2	12	
Total	**99**	**87**	**21**

Table 9: Existence of data protection authority by region

4.5 Limitations of the sample

Due the low response rate, the sample size is relatively low, at 26 responses. I argue that this is still sufficient to draw meaningful inferences, as it does represent one fifth of the world's data protection legislation and every respondent answered over forty questions, making it possible to group questions to make the data basis more robust. The results are quite clear, helping to make them credible, still, a higher sample size would have made the results more reliable.

Related to the sample size is the issue of making inferences about the temporal development of policy convergence in data protection. Firstly, looking at the development of legislation on a year-by-year basis does not seem to be fruitful, as not every year sees the introduction of new legislation. This issue can be mitigated by grouping the years to create intervals. A second temporal issue is due to the way some respondents answered the questionnaire. Authorities in almost all cases answered it based on either the most recent version of the law or a current draft. While four respondents also indicated years of revision for individual principles (i.e. the year when the principle was added), most did not. This means that legislation data skewers clearly to more recent years, making the data more reliable from the 2010s, consequently meaning also that inferences from there on are relatively reliable.

5 Is there convergence in data protection regulation?

This chapter's purpose is to answer the first research question if there is convergence in data protection regulation. For this purpose, the data gathered form data protection authorities will be analysed by employing the analytical framework from Holzninger and Knill, introduced in chapter two. They use the indicators *degree, direction* and *scope* of convergence to determine whether convergence occurs and to what level. The wider purpose of this chapter is to use the answer to the first research question to be a part of the answer to the second research question.

Due to the sample count of 26 not falling authoritatively in the large-n territory, a purely quantitative assessment of the data as suggested by Holzninger & Knill will be complemented by a qualitative contextualisation.

To turn the answers from the questionnaire into quantitative data, the yes/no answers for each principle and law have been coded into 1 and 0 values, arriving at a total of 975 data points describing whether a specific principle is present in a specific legislation. For each legislation the point of adoption by the country has been used to make inferences about the temporal development in the field. The following data is always based only on the laws adopted in the given years and not on accumulating laws.

Indicator	**Research question**	**Operationalisation**
Degree of convergence	To what degree have policies become more similar?	Decrease in standard deviation over time
Convergence direction	In what direction (strict or lenient) have policies developed?	Mean change
Convergence scope	Which (groups of) countries are converging in which direction?	Number of countries and policies

Table 10: Reminder: indicators by Holzninger & Knill

5.1 Degree of convergence

Assessing the *degree of convergence* means figuring out whether different legislations have become more similar or dissimilar to each other. Holzninger & Knill suggest measuring the decrease in standard deviation over time. Standard deviation helps to identify how much variation exists in a dataset. A high value indicates a high *degree of divergence* and an increasing value indicates a rising *degree of divergence*. A low value indicates a high *degree of convergence* and a falling value indicates a rising *degree of convergence*. As the data has been coded into 1 and 0 answers, the result will be a number between those values.

To measure development over time, the legislations have been grouped into five-year intervals, based on the year of adoption of the law or the revision of the law. Then the standard deviation has been measured for each group and compared to the total mean.

Holzninger & Knill actually suggest measuring each group internally, but I argue that it makes more sense to compare the deviation from the total, as this will say more about whether legislation is converging on one standard than looking at whether convergence is happening toward the mean of the interval, meaning whether legislation is particularly similar in that timeframe only.

Interval	1995 – 1999	2000 - 2004	2005 – 2009	2010 – 2014	2015 - 2019
Standard deviation	0,454	0,394	0,263	0,304	0,146

Table 11: Standard deviation per year-group

There is a clear and constant trend toward more similar laws. While legislation in the first two groups (1995 – 2004) are essentially only little more than half alike, the last group (2015-2019) is almost approaching uniform characteristics. There is a strong downward blip in the 2005 – 2009 group: This group is composed exclusively of African countries, which compared to the data of the complete sample tend to adopt strict legislation. While this is in line with the general direction of legislation (see next section), African countries have adopted such legislation earlier than the rest of the sample and therefore converged earlier.

5.2 Convergence direction

As it is clear now that convergence is happening, and laws are therefore becoming more similar, the next step is to assess in which direction of convergence the laws have developed. This will show if legislation is becoming stricter or more lenient. To measure this, the prevalence of the data protection principles in legislation will be utilised. As all but one of the principles are giving either a right to consumers or putting an obligation on data controllers, the inclusion of a principle can be regarded as a step toward a stricter regime. Conversely, the exclusion of a principle is then to be considered as a step toward a more lenient regime. To measure development over time, legislation has been divided into the same intervals as before.

Interval	1995 – 1999	2000 – 2004	2005 – 2009	2010 – 2014	2015 – 2019
% of strict principles present	28%	57%	77%	69%	86%

Table 12: Prevalence of data protection principles

The results are again clear and show a continuing trend toward stricter legislation over the years. While the first interval is quite extreme, possibly an outlier, it is evident even when disregarding the first interval that regulation has become stricter, with recent legislation incorporating almost all possible principles of data protection. The 2005 – 2009 group is again showing a blip, which has to attributed to the strict African laws of this group.

With reference to table 18, it is relevant to point out here that the EU GPDR features all but two principles from the total list of identified principles.

5.3 Convergence scope

Convergence scope determines which countries and policies are actually converging toward a common standard. To answer this question, both the sample from the questionnaire and the data set covering all countries are relevant. As data protection is a new policy field, having a law at all is already an endorsement for data protection as a civil right. In chapter 4, it became evident that many countries have made the choice to adopt data protection legislation in the last 50 years. In 2012 the number of countries having adopted legislation overtook the number of countries without and as of writing, countries with legislation lead countries without by a number of 43. It would therefore seem the trend is not yet slowing down. This means 125 countries in the world are falling under the convergence scope of making the decision to adopt legislation.

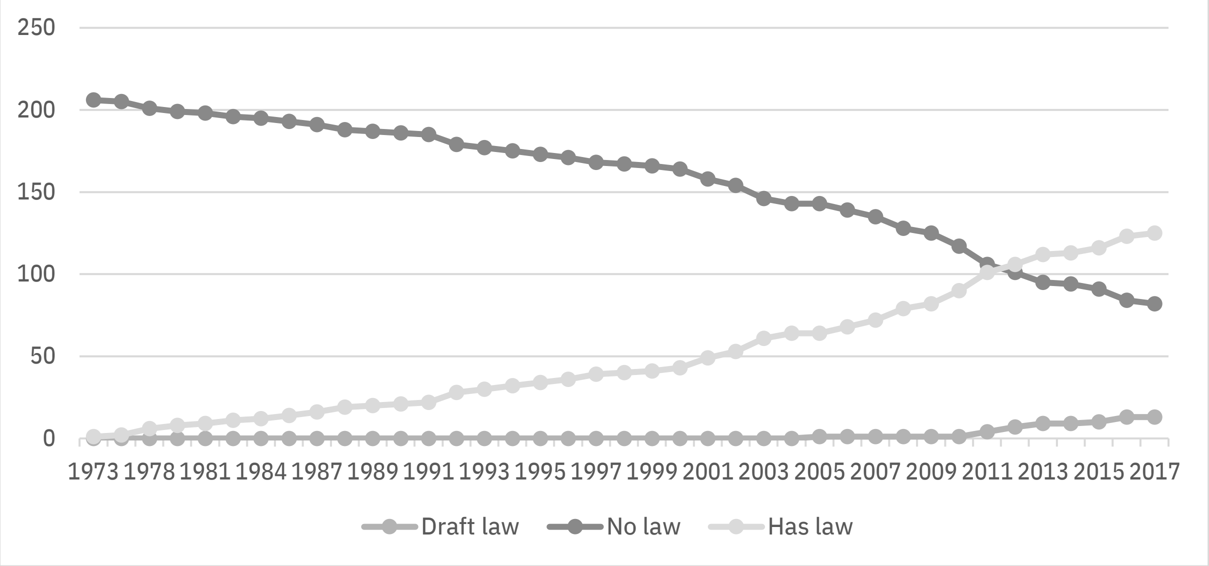


Table 13: Development of data protection laws

Analysing all of those 125 countries exceeds the scope of this thesis, but based on the sample some inferences can be made. For this, in the next section, more focus will be on affected regions than on temporal factors. Chapter 4.5 already showed which regions have adopted data protection legislation and to what degree, with Europe being at the forefront and the Americas, Asia and Africa all following at a similar pace.

5.4 Is the European standard emerging as the global standard?

Assessing the prevalence of data protection legislation by region offers the opportunity to move on to the second sub-question: Is the European standard emerging as the global standard? To answer this question, I have matched every principle from each of the frameworks with the corresponding principle in all the respondents' legislation. That is, for each principle in the law, an algorithm checked whether that principle was set to the same status in each of the frameworks. Where it matched (meaning either both were set to yes or both were set to no, the absence of a principle in both is a match too) a match point was given; where it did not, none was given. After these 9.360 calculations, the results were divided by the amount of principles for each law and framework, arriving at a percentage, which shows to which degree each law and each framework are alike, meaning the *degree of convergence* on the different frameworks. In what follows I will inspect the result of this process.

First, from a regional point of view, considerable divergence in affiliation to frameworks emerge. The following table show to what percentage the countries' legislation, grouped by regions, matches the different frameworks. The cells have been coloured to help identify where there is a high match (green) and where there is a low match (red).

Region	OECD (1980)	CoE 108 (1981)	Directive (1995)	CoE 108 (2001)	APEC (2005)	ECOWAS (2010)	OECD (2013)	APEC (2015)	GDPR (2016)
Africa	40%	52%	66%	58%	43%	61%	42%	43%	76%
Americas	47%	61%	61%	64%	47%	61%	49%	47%	65%
Asia	39%	53%	61%	53%	47%	56%	39%	47%	72%
Europe (excl. EU)	47%	63%	74%	69%	53%	70%	46%	53%	66%

Table 14: Match percentages per region and framework

The African laws are quite closely aligned to the European frameworks, especially to the EU legislation and already match the recently adopted GDPR quite well. The GDPR legislative process lasted over seven years and it is therefore not unlikely that it already emanated some influence before adoption in 2016, especially considering that the Commission proposal went public in 2012. Much fewer similarities exist with the more lenient OECD and APEC guidelines, meaning that the African laws go further than those lenient frameworks (as mentioned, a match point is only given when law and framework match up, even when the law is stricter). Interestingly, the African countries share more commonalities with the European standards than with the African ECOWAS protocol. This can be explained by most African countries in the sample adopting stricter legislation than is required by the ECOWAS protocol.

Legislation form the American countries is the least clearly-aligned, staying inside a roughly 20%-wide range between 47%-65% matching for all of the frameworks. Scores for the European frameworks as well as the African ECOWAS (which matches the Directive relatively closely, see table 18 in the annex for reference) are all in the low to mid 60% area, while all the other (lenient) frameworks are in the high 40% values.

The data on Asian legislation, having a sample count of only two countries, is not be as reliable as that on the other regions. Nonetheless, the sample shows a similar if less slightly less pronounced picture to the one from the African countries, with a relative dominance of the EU standard. Interestingly, there is relatively little common ground with the APEC guidelines, with less than 50% of the laws and framework matching up. This confirms other authors' views about the APEC framework only representing a baseline.

Lastly, the European countries are closely aligned with the EU directive, with a 74% match. Given the proximity to the EU and its multiple association agreements with non-EU European countries, this is not very surprising. The Council of Europe and ECOWAS frameworks also match with around 70%, with the GDPR closely behind, but not (yet) in first or second place. The OECD and APEC frameworks don't seem to be very influential, barely exceeding the 50% mark.

This data shows that the European data protection framework is the most prevalent one in all sampled regions in the world, even though it's not necessarily dominant in all regions and especially not in the Americas. African countries in particular seem to adopt legislation that is quite similar to EU legislation and while the data suggests Asian countries are doing the same, it is difficult to draw reliable inferences from two samples. The non-EU European countries are closely aligned with EU legislation.

To completely answer the question whether the European standard is emerging as the global standard, it is necessary to also identify the *direction of convergence* on a framework-basis. For this, the previously used year-intervals return, to be able to assess the temporal development.

The following table show to what percentage the countries' legislation, grouped by year-intervals, matches the frameworks. The cells have been coloured to help identify where there is a high match (green) and where there is a low match (red).

Interval	OECD (1980)	CoE 108 (1981)	Directive (1995)	CoE 108 (2001)	APEC (2005)	ECOWAS (2010)	OECD (2013)	APEC (2015)	GDPR (2016)
1995-1999	72%	78%	53%	69%	67%	56%	67%	67%	33%
2000-2004	56%	74%	76%	76%	63%	76%	54%	63%	56%
2005-2009	42%	51%	69%	59%	45%	64%	42%	45%	75%
2010-2014	47%	61%	72%	67%	52%	69%	46%	52%	67%
2015-2019	35%	50%	64%	57%	38%	59%	38%	38%	79%
Mean	46%	60%	69%	65%	50%	66%	46%	50%	68%

Table 15: Match percentages per interval and frameworks

Systematising the data, *three phases of data protection law* seem to exist. The first is the decreasing prevalence of laxer frameworks, such as the OECD and APEC guidelines and to some degree the original Council of Europe Convention 108. While legislation in the 90s and early 2000s seems to have been oriented around them and consequently has been quite lax, during the late 2000s and early 2010s these seem to have lost influence quite rapidly, with more robust regulation taking its place.

The stricter frameworks, such as the 1995 EU Directive, the additional protocol to the Council of Europe Convention from 2001 and the ECOWAS protocol took over and seem to have been the most dominant in the 15-year period between 2000 and 2014 period. Most legislation shows significant similarity to these frameworks, but with the most recent legislation this similarity has dropped considerably.

Lastly and most recently, the age of the GDPR seems to have begun, as it is clearly the dominant framework in the most recent year bracket of 2015 to 2019, overshadowing all other frameworks. Within this interval match, a mean of 79% of the legislation adopted, or revised their laws according to, the characteristics of the GDPR. In particular the laxer frameworks seem to now have only little relevance left for legislators.

After analysing the sample, the first research question – whether regulatory convergence is happening in the field of data protection – can likely be answered positively. Not only is, as a first step, convergence happening in terms of adopting data protection legislation at all, the legislation that has been adopted or has been revised is also becoming increasingly similar to each other and, crucial to this study, increasingly approaching the European Union standard. The sample size means some caution is necessary and it does not in itself allow any prediction of how legislation will evolve after this point, but it can be concluded that currently, the European data protection standard and especially characteristics of the new GDPR are being increasingly adopted by countries around the world.

6 What are the conditions for convergence?

The purpose of this section is to answer the second research question, namely what conditions have to be fulfilled for regulatory convergence to occur. For this, I will combine the theoretical frameworks of Drezner and Bradford from chapter 2, the information gained from the data protection frameworks in chapter 3 and the results of the questionnaire and analysis from chapters 4 and 5 to synthesise a reasoned argument about which conditions apply. This chapter will follow the same structure as the section on the conditions in chapter 2.2, for clarity.

As was discussed in chapter 4, both Drezner and Bradford discuss data protection as a case in their theory, but they are not basing their discussion on an own study into whether regulatory convergence is happening in this field, but on other authors' writings. In terms of the basis for making claims about regulatory convergence, this thesis is unique as no other study known to this author has conducted an investigation into data protection regulatory convergence by analysing how similar or dissimilar countries' legislation is both to each other and to the existing frameworks for this kind of legislation. This will allow me to make claims both Drezner and Bradford could not have made.

Both authors firstly give an overview of how they see regulatory convergence in data protection. Drezner and Bradford take similar paths. Drezner says the US attitude “is based on freedom from state intervention”, while the European Union approaches privacy as a “fundamental right to be protected by the state” (Drezner, 2008, p. 104). In essence, the US prefers industry self-regulation, while the EU prefers stringent legislation. Bradford notes how the US and the EU have a fundamentally different relation to privacy, how in the EU the right to privacy cannot be “contracted away”. She makes the distinction between the EU and the US approach: The EU has comprehensive data protection legislation and enforcement agencies; the US has scattered sectoral laws and no uniform enforcement (Bradford, 2012, p. 22).

For Drezner, in line with his previous prediction, there are two rival standards, the US and the EU approach to privacy, and he therefore expects that no global standard can emerge while the two great powers disagree. Opposed to this, Bradford theorises the global expansion of the European, comprehensive approach, that she purposes could even have an influence on the US itself. Here, she is going beyond Drezner, though it should be noted she does benefit from an additional four years of time passed (Bradford, 2012, p. 22).

6.1 Market power - Can the EU establish a global standard against the US?

As explained in chapter 2.3, Drezner has developed a systematisation of how great powers and other countries interact in terms of regulatory convergence (see table 5 for details). Since the US approach is to not have a single, comprehensive legislation, a country having such single, comprehensive legislation is already a win for the European standard. In 2008, at time of publication, countries having no data protection legislation still outnumbered countries with data protection legislation. According to my data, this would not constitute a *rival* *standard*, as Drezner says, since such is characterised by "low conflict" between the other countries, but a *sham standard*, as the other countries are split (meaning there is conflict over this question not only between the great powers, but between the smaller powers too). If the smaller actors come to decidedly follow one of the two standards, as it is now increasingly happening, then it would become a *rival standard*. If one of the standards is becoming the de-facto standard in the world, while one of the powers has not adopted it, then it would not conform to the classification created by Drezner, as one of the great powers was indeed able to establish a global standard *against* the preference of the other great power.

In the last ten years alone, coinciding with how long ago Drezner published his book, 53 countries have adopted for the first time a single, comprehensive data protection law. According to the data gained from my sample, the countries who have adopted legislation in this time-period can be expected to have adopted legislation similar to the European legislation. Therefore, there is a clear trend toward the European standard, without the US signing on to it. It has to be concluded that the EU is able to establish (be that actively or passively) its own standard in the world without support from and even against the preferences of the US. If one of the standards is becoming the de-facto standard in the world, while one of the powers has not adopted it, then it would not conform to the classification created by Drezner, as one of the great powers was able to establish a global standard against the preference of the other great power.

But Drezner's position can also be defended. Yes, other countries seem to sign on to the European standard, but can a standard truly be considered dominant if the US does not support it? This is to some degree a question of semantics and personal conviction more than facts, but I would argue that given the findings, the European standard can be called dominant. Additionally, given how the world is developing, it does seem to be only a question of time until also the US will come around and adopt legislation to deal with the fallout of technical development.

In conclusion it does seem like market power is required to establish a global standard, although it also does not seem to be sufficient to prevent another great power from establishing its standard as the global standard.

6.2 Regulatory capacity – Do countries just trust EU expertise?

Bradford assesses that market size is not sufficient to shape global regulation. Regulatory capacity is her second condition, meaning that jurisdictions must consciously decide to become a source of regulation and have "regulatory expertise and resources" to enforce such legislation (Bradford, 2012, p. 12). In the area of data protection legislation, no other region in the world has more expertise and resources than Europe. There is a unique tradition of appointing data protection authorities and due to the high GDP of European countries these agencies tend to be well staffed. The French data protection authority for example has 195 employees and a yearly budget of 16 million euros (CNIL, 2018). The German authority has 160 employees and a budget of 15 million euros (BMF, 2018; BfDI, 2017). These authorities are also not reluctant to engage with international companies to enforce European law. The

Belgian data protection authority for example fined Facebook 125 million euros in 2018 (Bendix, 2018).

Apart from this internal enforcement, the EU has actively attempted to enforce its standard around the world. Drezner sees the EU adequacy system introduced by the Directive 95 as an attempt to prevent the circumvention of its privacy rules (details see chapter 3.4.4). This has prompted some other states to adopt similar rules to gain access to the EU market and until today eleven countries have obtained adequacy decisions from the Commission, most being small states inside Europe or within its vicinity (European Commission, 2018). The US, however, as one of the two great powers with a rivalling standard did not accept the EU regulation. It negotiated a compromise (the safe harbour system) where US companies could self-certify that they comply to EU rules when processing EU citizens' data, but the country itself did not have to adopt legislation similar to the EU Directive. This compromise was notoriously poorly enforced, with companies not adhering to the rules and both the US government and the European Commission trying to hide this fact, in order to not endanger trade between the two blocs (Drezner, 2008, p. 105; Stupp, 2017).

Bradford also mentions the adequacy decision system (Bradford, 2012, p. 24), a system that appears to contradict her. As mentioned before, she does not expect the EU to require coercive measures, yet the adequacy decision system could be regarded as a unilateral coercive system. It forces other countries to adopt a system that offers at least the same protections as the European one. But there is another contradiction here. Bradford, as does Drezner, goes into the Safe Harbour agreement between the US and the EU. Bradford paints it much more as a win for the EU than for the US, as she regards the adequacy system to be a sign of the US accepting the EU approach. She does not mention the enforcement issues that have plagued the certification scheme. These issues could be interpreted as the US having never actually accepted the EU approach. The CJEU struck down the adequacy system for that exact reason in 2015 (Schrems case, CJEU, C-362/14). Safe Harbor was de-facto continued with the Privacy Shield, showing the Commission was not willing to endanger trade with the United States over data protection and unable to force the other great power to adopt its standard against its preferences. Therefore, the EU has not actually influenced the US legislation much in data protection through this and apparently preferred to protect its trade interests. Bradford's interpretation of the development lines up much more neatly with her prediction that the EU is able to shape global policy, in opposition to Drezner's interpretation that the resistance of the US has led to no global standard emerging.

In conclusion, it does not seem that the adequacy system, with its somewhat coercive elements have had such a great impact, as neither the United States, nor a high number of third countries have pursued an adequacy decision. In this, Bradford seems to overestimate the external enforcement impact. As will be argued in the following sections, the regulatory capacity as legal and technological subject matter know-how and available resources do play a very crucial role.

6.3 Preference for strict rules – Do countries want higher or lower standards?

More than its coercive enforcement abilities, I will argue that the reason for why some states are adopting the European approach is the fact that the Europeans possess the expertise and willingness to set strict standards when it comes to legislation. Countries that are content with less strict legislation can orient themselves toward the Asian, OCED or African frameworks. My data shows they are increasingly not doing so, but opt for strict legislation, in line with the European one. It therefore appears that this aspect does play a role in countries choosing a standard to converge to. The European countries are leading the world on strict data protection legislation because they have a long tradition of regulating this area and have invested in building regulatory experience and expertise. This means they have the knowledge tools to actually create strict legislation, something that many other countries do no possess, because data protection is not such a present topic in these countries. Almost all of the strict principles of data protection originate from European legislation (see table 18 in annex), and most countries do not have the know-how to go their own way in a field that is highly complex, technical and legalistic, being strongly affected by long-term impact assessments and the evaluation of unintended consequences. For this reason, countries may opt to follow the trusted and established EU standard. This means that regulatory capacity (being regulatory expertise and resources) and preference for strict rules are closely intertwined as conditions.

Bradford theorises that companies prefer strict rules, because it allows them to adapt their products to one set of regulations and then sell those products all over the world. They then lobby their governments to adopt legislation similar to the standard they already adhere to, to level the playing field with local competitors that choose not to follow the strict rules. This specific causality is possible, but its assessment is out of scope for this thesis, as it is not a state-driven action.

Bradford's theory is built on the California effect, a theory that speaks about how a regulatory race to the top can ensue when one legislator is setting high standards (see chapter 2.4 for more details). In similar fashion Vogel & Kagan (2002) have, based on Vogels California effect, further developed it to apply to globalisation and arrive at the conclusion that in many policy areas and cases no race to the bottom occurs globally. Popular media and NGOs tend to report on globalisation as a catalyst for more lenient legislation and therefore a race to the bottom, for example in labour or environmental regulation (Keegan, 2014; Weyler, 2016). Data, with its unterritorial nature initially seems to be a prime suspect for a regulatory race to the bottom as companies can theoretically change their jurisdiction, forcing other countries to also lower their standards to attract companies to their area, which would make data protection an inelastic target and data non-divisible product. The following two sections will discuss this in more detail, but it can already be said that the identified global shift to the stricter European standard therefore also means that at least in data protection, globalisation seems to have not led to a global race to the bottom, but the exact opposite.

6.4 Inelastic targets – Is the EU not regulating some markets?

Drezner concentrates his analysis of internet governance on the fact that the internet "overcomes all barriers of [...] borders" (Drezner, 2008, p. 91). He considers the main issue of internet (and privacy) governance to be the possibility for private actors to circumvent "bothersome regulations" (Drezner, 2008, p. 91) by moving their official headquarters to a different jurisdiction, i.e. engaging in forum shopping. Bradford would classify a market with this kind of behaviour as an *elastic market*. Drezner's analysis suffers to some degree from the velocity with which our understanding of the internet's effects on our societies has developed and by extension of how different regulating the internet actually is from regulating any other part of society. For example, data-based companies like social media or data analytics firms could be tempted to choose less strict jurisdictions to have more freedom in processing personal data. Facebook has transferred its jurisdiction for non-EU citizens outside of the European Union, to not be required to process data under the strict EU rules for non-EU citizens (Hern, 2018). But crucially, Facebook is not allowed to move to another, non-EU jurisdiction for its EU users, which means the EU rules do still apply. Facebook's behaviour can therefore not be regarded as classic forum shopping.

Companies in general are having more difficulties these days to engage in such behaviour, especially in developed markets such as Europe, for multiple reasons. The GDPR illustrates this. Firstly, legislation is becoming more tough in terms of the regulative application – the GDPR demands processing of EU citizen data to always be done under European rules, even if the processing is happening outside of EU territory, and with this addresses the immaterial nature of data. Secondly, the application of rules is being enforced through the possibility of very significant fines, increasing the cost of non-compliance. Lastly, public scrutiny has increased significantly in recent years, meaning that digital companies, of which many depend on usage by private individuals, risk losing their customers over non-adherence.

When smaller markets adopt similar rules, as they increasingly do according to my data, very big technology companies have the possibility to circumvent these markets' legislation. If no or very few competitors exist, these companies can bet on the fact that these smaller territories might not enforce their rules. After all, losing a small market means little to huge multinationals, but losing a service to which there is no alternative would be hurtful for, and possibly anger, the citizens of these territories. Therefore, these smaller markets have little to no leverage against the big technology giants. The EU is not a small market though. Losing it would mean losing a potential userbase of 500 million. Market power, as pointed out before, is an influential tool.

In brief, this means the field of data cannot fully be considered an elastic market, contrary what Drezner says. That doesn't make it a fully inelastic one either; Facebook is still able to move jurisdictions for its non-EU users, though if the GDPR framework continues to emerge as the dominant data protection framework worldwide, this remaining elasticity of the market will continue to decrease.

This development ties into the general theme of regulators reasserting themselves over internet governance, which will be discussed in the next section.

Investigating more closely how Bradford frames *predisposition to regulate inelastic targets*, it seems that it is not actually a condition which applies to the EU as an actor in general. It appears to be a condition of the fields that her theory applies to. Logically, observing that "an actor is only regulating a selection of policy fields” is not an answer to the question "what condition is necessary for policy convergence to happen". This means that Bradford is attempting to restrict the policy fields that her theory applies to, but does not actually do this by excluding certain policy fields, but by putting a relatively arbitrary restriction on the EU as an actor. Restrictions on applicable policy fields have been pointed out by other authors writing about regulatory convergence, such as Fritz W. Scharpf and Gary Marks, who often suppose that regulatory globalisation only happens in a limited number of areas in environmental law (Bradford, 2012, p. 8). Bradford does a similar thing, but in doing so neglects that the EU is also regulating elastic markets, for example the financial market with the MiFID II and MiFIR Directives (Cox, 2018). Bradford's restriction seems then to be a product of a desire to fit this exception into a condition for the EU instead of putting restrictions on the applicability of her theory. Whether policy convergence is also happening in elastic markets exceeds the scope of this thesis, but assuming Bradford’s assumption that there is no convergence on those fields is correct, her theory should in general be just applied to fully inelastic markets.

As has been discussed in this section, it does not seem like data protection is an elastic market, as regulators are increasingly able to effectively enforce data protection legislation also onto foreign companies. In conclusion means that this exception does not apply to data protection.

6.5 Non-divisibility of standards – Broken by the balkanisation of the internet?

In her discussion of *non-divisibility of standards*, Bradford classifies data as falling under *technical non-divisibility*, meaning that the product cannot be divided since that would be technically impossible. She purposes that if the EU would ask Google to change their data practices for European users, Google would be unable to do so only for European users and would have to adjust the practices for all (Bradford, 2012, p. 18). Already in the previous sections there have been examples as to why that is not necessarily the case, but especially the recent attempts of governments to regulate their “part” of the internet have shown that it is possible to cut the internet up and just regulate one’s own part, although such regulation seems to require the state to have a sufficient market size for private actors to respect the rules, as has been shown by how US internet companies like Google and Apple have adapted to Chinese, Russian and European internet regulation (Denyer, 2017; Tang, 2017).

There is an increasing trend toward the “balkanisation” of the internet (Bleiberg & West, 2014). Many countries, with EU countries and the EU itself leading the charge, are contributing to this process. Russia and other countries have passed laws that require localising data storage, meaning that data has to be stored in a data centre geographically located inside the jurisdiction (Barbour-Lacey, 2015). The CJEU has effectively mandated a localised version of the internet by creating the right to be forgotten, where only European users can request the deletion of their content when it is not relevant anymore and only

European users are affected by the deletion (De Ruyck & Fraser, 2014). Companies are contributing too, offering localised products to other companies and consumers for specific markets based on the markets' preference. For example, Microsoft is offering a higher-cost version of its Office product to privacy-minded customers, which is hosted on German servers and therefore bound to German data protection law (Microsoft, n.d.). As has been mentioned before, it can be posited that governments are re-asserting their jurisdiction over the internet, which for long was thought to circumvent or slip underneath the regulatory power of countries. Through deconstructing the un-geographic nature of the internet and creating regional versions of it, governments have found a way to regulate the internet, at least insofar as their own population is concerned.

Taking these developments into account, it shows that data (related to the person or not) does not seem to be a *non-divisible product* as posited by Bradford and it is possible for companies and countries alike to break up data according to territory-specific rules. As policy convergence seems to be happening in data protection and since data is not an *non-divisible product*, my findings contract Bradford on this point.

But this condition presents this analysis with another issue. Though Bradford lists it as one of her conditions, in her description it is actually not a condition, but a trigger for regulatory convergence to actually be initiated, given that the other conditions are met. It should have consequently not been classified as such and, from a general perspective (meaning not applied to this case), I therefore argue that the theory is left with only three conditions and one trigger. But since I argue that non-divisibility does not apply to data and therefore data protection as a field, it additionally means that in this case, it leaves Braford without a trigger for her theory. As has been discussed in chapter 2.2, fulfilling all conditions is not itself sufficient to cause convergence; policy convergence requires a trigger to start the process.

At this point it also becomes relevant how Drezner and Bradford look differently at how the spread of convergence works. It is noticeable that Drezner regards the process of establishing a regulatory standard as an active one: one of the big powers is actively attempting to shape global policy. In Bradford's theory, on the other hand, the process is happening in a more automatic fashion: even though she does identify a cause or trigger, as mentioned before, she still believes that the EU's rules are becoming the global standard not because the EU is attempting to achieve this, but because it makes most sense for everyone else involved. Based on my argumentation, I would agree.

6.6 Usage of NGOs/IGOs – Does the EU need NGO/IGO allies?

The last condition discussed by the two authors is the state's usage of NGOs and IGOs to advance its own regulatory standard. Drezner assigns multiple roles to NGOs and IGOs, but if one interprets his classification of standards in a strict way, data protection is a field with *rival standards*, as the US has not taken up the EU standard, and for this case he does not assign a role to NGOs or IGOs. If one assumes, however, as the data suggests, that the European standard has to some degree achieved regulatory convergence, the applicable type is a harmonised standard and in this case NGOs and IGOs are tasked with regime management (Drezner, 2008, p. 88).

It can be deduced from Bradford's discourse on the Brussels effect that she regards it as a process without a need for coercion or international institutions. Bradford says: "[T]he EU is not coercing others to adopt its rules either. Market forces are sufficient to create 'involuntary incentives' to adjust to the rules of the strict regulator" (Bradford, 2012, p. 9). Because of globalisation, companies have an incentive to take up this standard, even when the EU has formally no influence on this. Her assertion that the EU does not require international institutions for promulgating its regulatory standard may be initially surprising, given the EU's propensity to turn to multilateral solutions through multilateral institutions, such as the United Nations, the OECD, the WTO and others in an effort to promote the EU's point of view when it comes to international regulation. On closer view, it becomes clear that she is not negating this behaviour, but her analysis is taking a different point of view. She writes that there is no "political globalisation of regulatory standards" (Bradford, 2012, p. 4), as there is no negotiated standard. With the Brussels effect she describes a process that sets in, when there is no global standard per rules, but it is becoming a global standard because there is a strong incentive for other countries and companies to accept the EU standard out of their own interests and there is no promotion through international or multinational organisations required.

Though the Council of Europe (an IGO) has developed a data protection regime before the European Union, it can be said that both the CoE and the EU have supported each other in the process of promulgating similar data protection rules around the world. The EU has encouraged other states to join the open Convention 108 of the Council of Europe and closely coordinates with the IGO (see more on this in chapter 3.4.2). Many CoE member countries, including Russia, that are not EU members, are therefore adhering to *a* European standard. The Council membership ensure that those countries stay within the confines of the European standard. My data indicates though that the Convention 108 is increasingly becoming a baseline standard, like the OECD and APEC standard, as countries are advancing to stricter standards, more akin to the new EU regulation. The IGOs importance is difficult to ascertain, but it could be argued that the Council of Europe was important to promulgate the European standard in the past, but since now countries are adopting GDPR-like legislation, this support might not be needed anymore, even if it may be helpful in fostering baseline adherence.

6.7 What *are* the conditions for convergence?

Having analysed my own data and data protection frameworks, the conditions and causes Drezner and Bradford identified and having applied it to the case, I arrive at conclusions that differ in a number of aspects from Drezner and Bradford. These differences are summarised in the below table.

Cause or Condition	Drezner (2008), own revision	Bradford (2012), own revision	Own analysis on data protection case
Market power	Hybrid	Condition	Condition

No convergence against great power	Condition	Has happened	Has happened
Regulatory capacity	Not a factor	Condition	Cause
Preference for strict rules	Not a factor	Condition	Condition
Predisposition to regulate inelastic markets	Not a factor	Not a condition for actor, but an exception	Not relevant, as data is an inelastic market
Non-divisibility of standards	Not a factor	Cause	Does not apply, as data is *not* a non-divisible product
Effective NGO and IGO usage	Hybrid	Not a factor	Possibly condition

Table 16: Revised table of causes and conditions after analysis

As a concluding analysis, I want to argue for a different cause of convergence in data protection regulation. Other countries are adopting the European standard because they want to profit from the European expertise on data protection. As I have put forth before, the European expertise in data protection legislation is unrivalled. This is based on a unique historical sensitivity for the topic, Europeans are especially watchful of the consequences of surveillance and therefore such concerns are a higher priority. This has led to Europeans leading this field in terms of legislative initiative. Since electronic data processing is inherently making surveillance more prevalent and more intrusive (computer systems as opposed to humans can and usually do log and save everything), this historic sensitivity has put the Europeans on the forefront of a technological as well as legal challenge, that an increasing number of countries have also identified and are now approaching also by adopting legislation. As my data shows, countries emulate the European approach by passing laws that are essentially very similar to the European ones. These countries are reacting to *problem pressure* based on technological changes and seem to arrive, based on a mix of *lesson-drawing* and *emulation*, at the same conclusion as the Europeans, but as my data shows, to some degree later. It does not appear that the EU is employing overtly coercive measures, other than enforcing its own laws for its own citizens. *International harmonisation* is happening to a limited degree, but does not look to play a crucial role. Economic concerns can also be used to explain to some degree why the United States has not given into this pressure. Most of the world's data-driven companies are situated in the US (Statista, 2017); alas, this is not surprising, as lenient regulation allows data companies to innovate more easily with data-based business models. Regulating this area would endanger a business model that has brought huge wealth to these companies and its employees. Lawmakers in the United States are therefore understandably hesitant to follow this route. But most other countries in the world don't risk big economic consequences when adopting strict data protection legislation, since few of their companies depend on data like in the US. Taking into account recent developments though, it is possible though that the belief will take over that the societal risks of this technology outweigh the economic profit, especially since this economic profit it relative focused on a small amount of people.

7 Conclusion

This thesis set out to answer two questions: whether policy convergence is happening in data protection, and what that says about the conditions and causes for policy convergence as put forward by the two opposing theoretical frameworks of Drezner and Bradford. To answer these questions, I have collected and analysed my own empirical research data and confronted it with the development of global data protection legislation throughout the past couple of decades and the theories Drezner and Bradford developed.

The answer to the *first research question* is quite clear: Policy convergence is happening in the field of data protection and the standard that seems to be becoming the dominant one is the European Union GDPR framework.

The data also suggests there have been *three phases of data protection law* in the last twenty years, with ever increasing standards. The end of 90s and early 2000s saw the prevalence of lenient frameworks, such as the OCED and APEC guidelines and the original CoE Convention. From there on stricter frameworks took over, such as the Directive 95 and the additional protocol to the CoE Convention in 2001 and saw high adherence until the early to mid 2010s. Lastly, from the mid 2010s the strictest of the ages with the adoption of the GDPR has begun, with very high similarity in adopted legislation. It should be pointed out again here that the data sample was limited, so any conclusions drawn from them have to be treated with caution.

The answer to the *second research question* is more complicated and nuanced. Drezner and Bradford have each put forth their own causes and conditions, in many cases disagreeing with each other.

Possessing a very high degree of *market power* to project and enforce regulation is a clear condition, as both authors suggest. Though, analysing this condition in the case of data protection seems to contradict Drezner's suggestion that neither the EU nor the US can establish a standard that goes against the preferences of the other. The EU standard is in fact emerging as the dominant one and therefore this case study supports Bradford’s notion on this aspect.

As opposed to what Bradford proposes, data is really *not* a *non-divisible good*, meaning data can be divided into smaller parts and therefore regulated differently in different territories. For Bradford non-divisibility is one of the conditions for why the European standard is emerging globally, meaning this part of her theory cannot hold up.

In similar fashion, when it comes to *inelastic markets* (here defined as the possibility to circumvent legislation by forum shopping), both authors can be criticised. Bradford’s assumption that the EU tends to *only regulate inelastic markets* does not hold, even though in the end it has to be concluded that data is an inelastic market. Meanwhile, Drezner’s assumption that data is a fully elastic market, where companies can just change their jurisdiction, also seems to have been disproven, based on enforcement successes.

A jurisdiction’s *preference for strict rules* was confirmed as a condition for policy convergence, as the European approach to data protection is uniquely strict as compared to other existing data protection frameworks and this is where regulation worldwide is moving toward. The condition has been modified from Bradford’s outline, as she investigates a degree of private-actor involvement that is out of the scope of this thesis.

Lastly, *regulatory capacity* turned out to be a crucial aspect and I argue that the Europeans' regulatory expertise and resources, in connection with their *preference for strict rules* is actually the cause for the emerging dominance of the European standard. European history has made regulators and enforcement authorities possess unique know-how and resources in and for this complex field, making them the legislator who knows best how to write the rules in a stringent and effective way. Other countries are therefore looking towards the EU in order to adopt strict and sensible legislation and for this reason are adopting the European standard.

It is clear that some of Drezner's and Bradford's conclusions do not hold up when confronted with the case of data protection, a case which they have both themselves elevated as a test case for their theory. Neither Drezner's opinion, whose theory is more US-aligned, nor Bradford's stance, whose theory is more Europe-friendly, has been completely proven or disproven. Taking only their main argument - whether the European Union can shape global policy alone or not - the conclusion in the case of data protection is that seemingly it can. That means the European Union at the least can pick up policy leadership in this one, for the future very important, area. Whether the EU can perform the same feat in other areas, however, is a different question.

The question of the characteristics of European leadership in data protection regulation alone provides many promising avenues for future research. One could develop a fully comprehensive new theoretical approach to policy convergence or approach the topic from normative angles, such as analysing the EU’s motivations in this field and its role as a norm-setter. Questions of cultural imperialism and colonialism are also evident. A much more in-depth investigation into all legislation as well as a country-by-country discussion of the emergence of the European standard in a more nuanced way would undoubtedly offer additional interesting insights.

Bibliography

Asia Pacific Economic Cooperation. (2005). *APEC Privacy Framework (2005)*. *APEC*. https://doi.org/10.1017/CBO9780511494208.006

Asia Pacific Privacy Authorities. (2018). APPA members. Retrieved May 7, 2018, from http://www.appaforum.org/members/

Bach, D., & Newman, A. L. (2007). The European regulatory state and global public policy: Micro-institutions, macro-influence. *Journal of European Public Policy*, *14*(6), 827–846. https://doi.org/10.1080/13501760701497659

BakerHostetler. (2016). *2015 International Compendium of Data Privacy Laws*. Retrieved from https://towerwall.com/wp-content/uploads/2016/02/International-Compendium-of-Data-Privacy-Laws.pdf

Barbour-Lacey, E. (2015). *Understanding Localization in Russia*. Retrieved from https://leaglobal.com/thought_leadership/Russia Briefing Understanding Localization in Russia.pdf

Bendix, A. (2018). EU Fines Facebook $122 Million. Retrieved May 15, 2018, from https://www.theatlantic.com/news/archive/2017/05/facebook-receives-122-million-fine-from-the-european-union/527325/

Bennett, C. J. (1991). What Is Policy Convergence and What Causes It? British Journal of Political Science. Cambridge University Press. https://doi.org/10.2307/193876

BfDI. (2017). Tätigkei*tsbereicht zum Datenschutz*. Retrieved from https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/Themen26 TB.pdf?__blob=publicationFile&v=1

Birnhack, M. D. (2008). The EU Data Protection Directive: An Engine of a Global Regime. *ComputerLaw & Security Report*, *24*(6), 123. Retrieved from http://ssrn.com/abstract=1268744

Bleiberg, J., & West, D. M. (2014). How to Stop the Internet from Breaking Apart. Retrieved May 11, 2018, from https://www.brookings.edu/blog/techtank/2014/10/06/how-to-stop-the-internet-from-breaking-apart/

Bloomberg. (2018). Uber Data Breach Exposed Personal Information of 20 Million Users. Retrieved May 7, 2018, from http://fortune.com/2018/04/12/uber-data-breach-security/

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review*, *107*(1), 1–67. Retrieved from https://pdfs.semanticscholar.org/2c55/404a1e09859c289644c517020aecd7fe48e4.pdf

Bundesministerium für Finanzen. (2018). Bundeshaushalt-Info.de: Einzelpläne 2017 - Übersicht Soll Ausgaben. Retrieved May 15, 2018, from https://www.bundeshaushalt-info.de/#/2017/soll/ausgaben/einzelplan.html

Büthe, T., & Mattli, W. (2011). *The New Global Rulers: The Privatization of Regulation in the World Economy* (First). Princeton: Princeton University Press.

Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199675555.001.0001

CCDCOE. (n.d.). ECOWAS | CCDCOE. Retrieved March 6, 2018, from https://ccdcoe.org/ecowas.html

CNIL. (2018). Le fonctionnement | CNIL. Retrieved May 15, 2018, from https://www.cnil.fr/fr/le-fonctionnement

Council of Europe. European Convention on Human Rights (1950). Retrieved from www.echr.coe.int

Cox, J. (2018). MiFID II: What is it, how will it affect the world of finance and why should we care? Retrieved May 11, 2018, from https://www.independent.co.uk/news/business/analysis-and-features/mifid-ii-2018-what-is-how-effect-financial-investments-markets-in-financial-instruments-directive-a8139361.html

Data Protection and Privacy Commissioners. (2005). Montreux Declaration The protection of personal data and privacy in a globalized world: a universal right respecting diversities The Data Protection and Privacy Commissioners assembled in Montreux for their 27. In *27th International Conference (14- 16 September 2005)* (p. 4).

de Hert, P., & Papakonstantinou, V. (2014). The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition. *Computer Law & Security Review*, *30*(6), 633–642. https://doi.org/10.1016/J.CLSR.2014.09.002

De Ruyck, J., & Fraser, J. (2014). The European Right To Be Forgotten Might Be A Pandora's Box. Retrieved May 11, 2018, from http://www.ip-watch.org/2014/07/04/the-european-right-to-be-forgotten-might-be-a-pandoras-box/

Denyer, S. (2017). Apple CEO backs China's vision of an 'open' Internet as censorship reaches new heights. Retrieved May 11, 2018, from https://www.washingtonpost.com/news/worldviews/wp/2017/12/04/apple-ceo-backs-chinas-vision-of-an-open-internet-as-censorship-reaches-new-heights/?noredirect=on&utm_term=.789219f297c8

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147. https://doi.org/10.2307/2095101

DLA Piper. (2016). DLA Piper Global Data Protection Laws of the World. Retrieved May 7, 2018, from https://www.dlapiperdataprotection.com/index.html?t=world-map&c=TR

Dolowitz, D. P., & Marsh, D. (2000). Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making. *Governance*, *13*(1), 5–23. https://doi.org/10.1111/0952-1895.00121

Drezner, D. W. (2001). Globalization and Policy Convergence. *International Studies Review*. WileyThe International Studies Association. https://doi.org/10.2307/3186512

Drezner, D. W. (2008). *All Politics Is Global: Explaining International Regulatory Regimes*. *Princeton University Press*. https://doi.org/10.2307/j.ctt7st6p

ECOWAS. (2010). *Supplementary Act on Personal Data Protection*. Retrieved from http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf

European Commission. (2018). Adequacy of the protection of personal data in non-EU countries. Retrieved May 15, 2018, from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

European Union. (1995). 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. *Official Journal of the European Communities*, (L281/31), 31–50. https://doi.org/ISSN 0378-6978

Figarella, M. (2017). Global consensus emerges on biometric data protection. *Biometric Technology Today*, *3*, 5–7. https://doi.org/10.1016/S0969-4765(17)30152-2

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. *European Data Protection: Coming of Age*, (May 2014), 3–32. https://doi.org/10.1007/978-94-007-5170-5_1

Fung, B. (2018). Equifax's massive 2017 data breach keeps getting worse. Retrieved May 7, 2018, from https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?utm_term=.d7ae42676e26

Gady, F. (2014). EU / U. S. Approaches to Data Privacy and the "Brussels Effect": A Comparative

Analysis. *Georgetown Journal of International Affairs*, *1*(International Engagement on Cyber IV), 12–23.

George, A. L., & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences*. MIT Press.

Greenleaf, G. (2009). Five years of the APEC Privacy Framework: Failure or promise? *Computer Law and Security Review*, *25*(1), 28–43. https://doi.org/10.1016/j.clsr.2008.12.002

Greenleaf, G. (2011). 76 GLOBAL DATA PRIVACY LAWS. *Privacy Laws & Business*. Retrieved from https://poseidon01.ssrn.com/delivery.php?ID=8161160740640010290920160920670310810240360420280910051050671190260930780910740841260090031160140060090300661220171111101050841140260280800920020680961121071020790040690070260810661231250171000921000860741230731

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Greenleaf, G. (2017). Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey. *Privacy Laws & Business International Report*, *45*, 10–13. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035

Guaman, D. (2016). Privacy vs. Data Protection vs. Information Security | Software and Services Engineering. Retrieved February 5, 2018, from http://blogs.upm.es/sse/2016/11/01/privacy-vs-data-protection-vs-information-security/

Hautala, L. (2018). Zuckerberg hearings get Congress weighing EU-style privacy regulations. Retrieved May 7, 2018, from https://www.cnet.com/news/privacy-imported-zuckerberg-hearings-get-congress-weighing-eu-style-regulations-to-protect-your-data/

European Commission. (2018). Adequacy of the protection of personal data in non-EU countries. Retrieved May 15, 2018, from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

Hijmans, H. (2016). *The European union as a constitutional guardian of internet privacy and data protection*. Brussels, Belgium: Springer International Publishing. https://doi.org/10.1007/978-3-319-34090-6

Hildebrandt, M. (2017). Privacy As Protection of the Incomputable Self: Agonistic Machine Learning. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3081776

Hoberg, G. (2001). Globalization and policy convergence: Symposium overview. *Journal of Comparative Policy Analysis: Research and Practice*, *3*(2), 127–132. https://doi.org/10.1080/13876980108412657

Holzinger, K., & Knill, C. (2005). Causes and conditions of cross-national policy convergence. *Journal of European Public Policy*, *12*(5), 775–796. https://doi.org/10.1080/13501760500161357

Hustinx, P. (2013). *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation* (Collected Courses of the European University Institute’s Academy of European Law). Retrieved from https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf

International Association of Privacy Professionals. (2018). IAPP Privacy Tracker. Retrieved May 7, 2018, from https://iapp.org/news/privacy-tracker/

International Conference of Data Protection & Privacy Commissioners. (2017). Participation in the Conference. Retrieved May 7, 2018, from https://icdppc.org/participation-in-the-conference/

Keegan, W. (2014). Globalisation: we can avoid a race to the bottom. Retrieved May 6, 2018, from https://www.theguardian.com/business/2014/jun/29/globalisation-can-benefit-everyone-william-keegan

Knill, C. (2005). Introduction: Cross-national policy convergence: concepts, approaches and explanatory factors. *Journal of European Public Policy*, *12*(5), 764–774. https://doi.org/10.1080/13501760500161332

Lahiri, K. (2018). U.S. Businesses Can't Hide From GDPR.

Makulilo, A. B. (Ed.). (2016). *African Data Privacy Laws* (Vol. 33). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-47317-8

Martineau, P. (2018). Stop saying 'privacy,' start saying 'data protection.' Retrieved May 7, 2018, from https://theoutline.com/post/4409/stop-saying-privacy-start-saying-data-protection?zd=1&zi=ht3freyn

Microsoft. (n.d.). Azure Germany Cloud Computing. Retrieved May 11, 2018, from https://azure.microsoft.com/en-us/global-infrastructure/germany/

Moravcsik, A. (2017, April). Europe Is Still a Superpower – And it's going to remain one for decades to come. *Foreign Policy*. Retrieved from http://foreignpolicy.com/2017/04/13/europe-is-still-a-superpower/

Negnevitsky, M. (2005). *Artificial intelligence: a guide to intelligent systems* (2. ed). Harlow: Addison-Wesley.

O'Connor, N. (2018). *Reforming the U.S. Approach to Data Protection and Privacy*. Retrieved from https://www.cfr.org/report/reforming-us-approach-data-protection

OECD. (1980). *The OECD Privacy Guidelines (1980)*.

OECD. (2013). The OECD Privacy Guidelines (2013). *The OECD Privacy Framework*, 1–154, 9–18. https://doi.org/10.1787/5kgf09z90c31-en

Privacy International. (2018). State of Privacy. Retrieved from https://privacyinternational.org/type-resource/state-privacy

Rieland, R. (2018). Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased? | Innovation | Smithsonian. Retrieved April 22, 2018, from https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/

Rowntree, L. (2017). The GDPR: Hype or Hyperbole?

Safari, B. A. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall Law Review*, *47*(6), 810–848. Retrieved from http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1600&context=shlr

Simmons, B. A., & Elkins, Z. (2004). The Globalization of Liberalization: Policy Diffusion in the International Political Economy. *American Political Science Review*, *98*(01), 171–189. https://doi.org/10.1017/S0003055404001078

Statista. (2017). Top internet companies: global market value 2017. Retrieved May 16, 2018, from https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/

Stupp, C. (2017). Tech industry slams data watchdogs over damning privacy shield report. Retrieved May 11, 2018, from https://www.euractiv.com/section/data-protection/news/tech-industry-slams-data-watchdogs-over-damning-privacy-shield-report/

Tang, F. (2017). Apple's Tim Cook and Google's Sundar Pichai attend Chinese state-run internet conference. Retrieved May 11, 2018, from http://www.scmp.com/news/china/economy/article/2122632/apples-tim-cook-and-googles-sundar-pichai-attend-chinese-state

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security*

Review: The International Journal of Technology Law and Practice, *34*, 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

United Nations. Universal Declaration of Human Rights (1948). Retrieved from http://www.un.org/en/universal-declaration-human-rights/index.html

United Nations. (2017). United Nations Statistics Division - National Accounts. Retrieved March 2, 2018, from https://unstats.un.org/unsd/snaama/dnlList.asp

United Nations Conference on Trade and Development. (2017). Data Protection and Privacy Legislation Worldwide. Retrieved May 7, 2018, from http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

United States. Privacy Act of 1974 (1974). United States of America.

Vogel, D. (1995). *Trading up : consumer and environmental regulation in a global economy*. Harvard University Press.

Vogel, D., & Kagan, R. A. (2002). *Dynamics of Regulatory Change: How Globalization Affects National Regulatory Policies* (Vol. UCIAS Edit). Berkley: University of California Press. Retrieved from http://linkinghub.elsevier.com/retrieve/pii/S0166432810007667

Weyler, R. (2016). Globalisation's dark side. Retrieved May 6, 2018, from https://www.greenpeace.org/archive-international/en/news/Blogs/makingwaves/globalisation-dark-side/blog/57141/

Zielonka, J. (2008). Europe as a Global Actor: Empire by Example? *International Affairs (Royal Institute of International Affairs 1944-)*, *84*(3), 471–484. Retrieved from http://www.jstor.org/stable/25144812

Appendix

Overview of data protection frameworks

Regime	Country/Organisation	Introduced	Short in tables
Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	Organisation for Economic Co-operation and Development (OECD)	1980	OECD (1980)
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	Council of Europe (CoE)	1981	CoE (1981)
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	European Union (EU)	1995	Directive (1995)
Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows	Council of Europe (CoE)	2001	CoE (2001)
APEC Privacy Framework (Original 2005 version)	Asia-Pacific Economic Cooperation (APEC)	2005	APEC (2005)
Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS	Economic Community of West African States (ECOWAS)	2010	ECOWAS (2010)
Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013 revision)	Organisation for Economic Co-operation and Development (OECD)	2013	OECD (2013)

APEC Privacy Framework (2015 revision)	Asia-Pacific Economic Cooperation (APEC)	2015	APEC (2015)
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	European Union (EU)	2016	GDPR (2016)

Table 17: Overview of data protection frameworks

Frameworks and questionnaire questions

Principles	OECD (1980)	CoE 108 (1981)	Directive (1995)	CoE 108 (2001)	APEC (2005)	ECOWAS (2010)	OECD (2013)	APEC (2015)	GDPR (2016)	CoE 108 (2017)
Automated decision making: Prohibition	n	n	n	n	n	y	n	n	n	n
Automated decision making: Right to object	n	n	y	n	n	n	n	n	y	y
Automated decision-making: Right to logic information	n	n	y	n	n	n	n	n	y	y
Base principles: Demonstrate compliance trough certification	n	n	n	n	n	n	n	n	y	n
Base principles: Legally binding and enforceable	n	y	y	y	n	y	n	n	y	y
Base principles: Rights apply irrespective of nationality	n	n	y	n	n	y	n	n	y	y
Collection requirement: Data subject consent	y	y	y	y	n	y	y	n	y	y
Collection requirement: Fair and lawful collection	y	y	y	y	y	y	y	y	y	y
Collection requirement: Legitimate purpose	n	y	y	y	n	y	n	n	y	y
Collection requirement: Sensitive data	n	y	y	y	n	y	n	n	y	y
Data controller obligation: Appoint a DPO	n	n	n	n	n	n	n	n	y	n
Data controller obligation: Data accuracy	y	y	y	y	y	y	y	y	y	y
Data controller obligation: Data minimsation	n	y	y	y	n	y	n	n	y	y
Data controller obligation: Data protection by default	n	n	n	n	n	n	n	n	y	y
Data controller obligation: Data protection by design	n	n	n	n	n	n	n	n	y	y
Data controller obligation: Easily understandable information	n	n	n	n	n	n	n	n	y	n
Data controller obligation: Notification	n	n	y	n	n	n	y	n	y	y
Data controller obligation: Processing information	n	n	y	n	y	y	n	y	y	y

Data controller obligation: Risk or impact assessments	n	n	n	n	n	n	y	n	y	y
Data subject right: Data portability	n	n	n	n	n	n	n	n	y	n
Data subject right: Judicial recourse	n	y	y	y	n	n	n	n	y	y
Data subject right: Right to access	y	y	y	y	y	y	y	y	y	y
Data subject right: Right to be forgotten	n	n	n	n	n	n	n	n	y	n
Data subject right: Right to correction	y	y	y	y	y	y	y	y	y	y
Data subject right: Right to remedy	y	y	y	y	n	n	y	n	y	y
Derogation from rights: Public interest	y	y	y	y	y	y	y	y	y	y
DPA: Can impose fines	n	n	n	n	n	n	n	n	y	y
DPA: Judicial review of DPA decision	n	n	y	y	n	y	n	n	y	y
DPA: Non-jurisdiction controllers have to assign a representative for the DPA	n	n	n	n	n	n	n	n	y	n
DPA: Required	n	n	y	y	n	y	y	n	y	y
General principle: Preventing harm	n	n	n	n	y	n	n	y	n	n
Liability: Data controller and processers	n	n	n	n	n	n	n	n	y	y
Processing requirement: Purpose limitation	n	y	y	y	y	y	n	y	y	y
Requirement: Data security	y	y	y	y	y	y	y	y	y	y
Territorial scope: Data has to be processed according to rules of the data subject jurisdiction no matter where the processing is taking place	n	n	n	n	n	n	n	n	y	n
Trans-border data flow: adequacy system	n	n	y	n	n	y	n	n	y	y
Trans-border data flow: Privacy may not restrict free flow of personal data	y	n	y	n	y	n	y	y	y	y
Trans-border data flow: Restrictions on	y	n	y	y	n	y	n	n	y	y

Table 18: Frameworks and questionnaire questions

List of data protection acts

Country	Has law	From	Latest	Region	DPA
Afghanistan	No			Asia	None
Albania	Yes	2008	2012	Europe (ex EU)	Commissioner for Personal Data Protection
Algeria	No			Africa	None
Andorra	Yes	2003		Europe (ex EU)	Andorran Agency of Data Protection
Angola	Yes	2011		Africa	Agência de Proteção de Dados (APD)
Antigua and Barbuda	Yes	2013		Americas	Information Commissioner
Argentina	Yes	2000		Americas	Dirección Nacional de Protección de Datos Personales(DNPDP)
Armenia	Yes	2002	2015	Europe (ex EU)	Personal Data Protection Agency
Aruba	Yes	2011		Americas	Unknown
Australia	Yes	1988	2012	Oceania	Privacy Commissioner
Austria	Yes	1978	2018	EU	Datenschutzbehörde
Azerbaijan	Yes	1998	2010	Europe (ex EU)	None
Bahamas	Yes	2003		Americas	Data Protection Commissioner for the Bahamas
Bahrain	No			Asia	None
Bangladesh	No			Asia	None
Barbados	Yes	2001		Americas	Unknown
Belarus	Yes	2007		Europe (ex EU)	None
Belgium	Yes	1992	2018	EU	Commission for the Protection of Privacy
Belize	No			Americas	None
Benin	Yes	2009		Africa	Commission Nationale de l'Informatique et des Libertés
Bermuda	Yes	2016		Americas	Privacy Commissioner of Bermuda
BES Islands	Yes	2010		Americas	Commission supervision data protection BES
Bhutan	Yes	2006		Asia	None
Bolivia	Yes	2011		Americas	None

Country	Has law	From	Latest	Region	DPA
Bosnia and Herzegovina	Yes	2006		Europe (ex EU)	Personal Data Protection Agency
Botswana	No			Africa	None
Brazil	Draft	2011		Americas	None
Brunei	No			Asia	None
Bulgaria	Yes	2002	2018	EU	Bulgarian data protection authority
Burkina Faso	Yes	2004		Africa	Commission for Computer and Civil Liberties
Burma (Myanmar)	No			Asia	None
Burundi	No			Africa	None
Cambodia	No			Africa	None
Cameroon	No			Africa	None
Canada	Yes	1983	2002	Americas	Office of the Privacy Commissioner of Canada
Cape Verde	Yes	2001		Africa	Comissão Nacional de Proteção de Dados Pessoais
Central African Republic	No			Africa	None
Chad	Yes	2015		Africa	None
Chile	Yes	1999	2012	Americas	Consejo para la Transparencia (CplT)
China	No			Asia	Cyberspace Administration of China
Colombia	Yes	2008	2012	Americas	Superintendence of Industry and Commerce of Colombia
Comoros	No			Africa	None
Congo, Dem. Rep. of	No			Africa	None
Congo, Rep. of	No			Africa	None
Costa Rica	Yes	2011	2013	Americas	PRODHAB
Côte d'Ivoire	Yes	2013		Africa	Autorité de protection des données à caractère personnel
Croatia	Yes	2003	2018	EU	Croatian Personal Data Protection Agency
Cuacao	Yes	2010		Americas	Unknown
Cuba	No			Americas	None
Cyprus	Yes	2001	2018	EU	Commissioner for Personal Data Protection

Country	Has law	From	Latest	Region	DPA
Czech Republic	Yes	1992	2018	EU	Office for Personal Data Protection
Denmark	Yes	1978	2018	EU	Datatilsynet
Djibouti	No			Africa	None
Dominica	Draft	2011		Americas	None
Dominican Republic	Yes	2013		Americas	Instituto Dominicano de las Telecomunicaciones
Dubai	Yes	2007		Asia	None
East Timor	No			Africa	None
Ecuador	Draft	2016		Americas	None
Egypt	No			Africa	None
El Salvador	No			Americas	None
Equatorial Guinea	Yes	2016		Africa	Personal Data Protection Governing Authority
Eritrea	No			Africa	None
Estonia	Yes	2003	2018	EU	Estonian Data Protection Inspectorate
Ethiopia	No			Africa	None
Faroe Islands	Yes	2001	2004	Europe (ex EU)	Faroese Data Protection Agency
Fiji	No			Oceania	None
Finland	Yes	1987	2018	EU	Data Protection Ombudsman
France	Yes	1978	2018	EU	La Commission Nationale de l’Informatique et des Liberte ́s (CNIL)
Gabon	Yes	2011		Africa	National Commission for the Protection of Personal Data
Gambia	Yes	2009		Africa	Unknown
Georgia	Yes	2011		Europe (ex EU)	Office of the Personal Data Protection Inspector
Germany	Yes	1977	2018	EU	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Ghana	Yes	2012		Africa	Data Protection Commission
Gibraltar	Yes	2004		Europe (ex EU)	Data Protection Commissioner
Greece	Yes	1997	2018	EU	Data Protection Authority
Greenland	Yes	1979	2016	Americas	Unknown

Country	Has law	From	Latest	Region	DPA
Grenada	No			Americas	None
Guatemala	No			Americas	None
Guernsey	Yes	1986	2010	Europe (ex EU)	Data Protection Office
Guinea	No			Africa	None
Guinea-Bissau	No			Africa	None
Guyana	No			Americas	None
Haiti	No			Americas	None
Honduras	Draft	2013		Americas	Institute for the Access to Public Information
Hong Kong SAR	Yes	1995	2002	Asia	Office of the Privacy Commissioner for Personal Data
Hungary	Yes	1992	2018	EU	National Authority for Data Protection and Freedom of Information
Iceland	Yes	1989	2010	EU	Icelandic Data Protection Authority
India	Yes	2011		Asia	Data Security Council for India
Indonesia	Yes	2016		Asia	Unknown
Iran	Yes	2003		Asia	None
Iraq	No			Asia	None
Ireland	Yes	1988	2018	EU	Office of the Data Protection Commissioner
Isle of Man	Yes	1986	2002	Europe (ex EU)	Data Protection Supervisor
Israel	Yes	1981		Asia	Privacy Protection Authority
Italy	Yes	1996	2018	EU	Garante per la protezione dei dati personali
Jamaica	Draft	2012		Americas	Unknown
Japan	Yes	2003	2015	Asia	Personal Information Protection Commission
Jersey	Yes	1987	2005	Europe (ex EU)	Data Protection Office
Jordan	Draft	2016		Asia	None
Kazakhstan	Yes	2013	2015	Asia	Unknown
Kenya	Draft	2012		Africa	None
Kiribati	No			Oceania	None

Country	Has law	From	Latest	Region	DPA
Kosovo	Yes	2010		Europe (ex EU)	National Agency for the Protection of Personal Data
Kuwait	Yes	2014		Asia	Unknown
Kyrgyz Republic	Yes	2008		Asia	State Registration Service
Laos	No			Asia	None
Latvia	Yes	2000	2018	EU	Data State Inspectorate
Lebanon	No			Asia	None
Lesotho	Yes	2011		Africa	Data Protection Commission
Liberia	No			Africa	None
Libya	No			Africa	None
Liechtenstein	Yes	2002	2015	Europe (ex EU)	Datenschutzstelle
Lithuania	Yes	1996	2018	EU	State Data Protection Inspectorate
Luxembourg	Yes	1979	2018	EU	Commission Nationale pour la Protection des Données (CNPD)
Macao SAR	Yes	2006		Asia	Office for Personal Data Protection
Macedonia (FYROM)	Yes	1994	2005	Europe (ex EU)	Directorate for Personal Data Protection
Madagascar	Yes	2015		Africa	Commission Malagasy sur l'Informatique et des Libertés
Malawi	Yes	2016		Africa	Unknown
Malaysia	Yes	2010	2013	Asia	Personal Data Protection Commissioner
Maldives	No			Asia	None
Mali	Yes	2013		Africa	Personal Data Protection Authority, Mali
Malta	Yes	2001	2018	EU	Office of the Information and Data Protection Commissioner
Marshall Islands	No			Oceania	None
Mauritania	No			Africa	None
Mauritius	Yes	2017		Africa	Data Protection Office
Mexico	Yes	2010	2016	Americas	Federal Institute for Access to Information and Data Protection
Micronesia	No			Oceania	None
Moldova	Yes	2007	2011	Europe (ex EU)	National Center for Personal Data Protection

Country	Has law	From	Latest	Region	DPA
Monaco	Yes	1993	2015	Europe (ex EU)	Commission for Control of Personal Data
Mongolia	No			Asia	None
Montenegro	Yes	2008	2012	Europe (ex EU)	Agency for Protection of Personal Data and Free Access to Information
Morocco	Yes	2009		Africa	Data Protection National Commission
Mozambique	No			Africa	None
Namibia	No			Africa	None
Nauru	No			Oceania	None
Nepal	Yes	2007		Asia	Unknown
Netherlands	Yes	1988	2018	EU	Autoriteit Persoonsgegevens
New Zealand	Yes	1993	2010	Oceania	Privacy Commissioner Office
Nicaragua	Yes	2012		Americas	Unknown
Niger	Yes	2017		Africa	Unknown
Nigeria	Draft	2011		Africa	None
Norway	Yes	1978	2010	EU	Datatilsynet
Oman	No			Asia	None
Pakistan	Draft	2005		Asia	None
Palau	No			Oceania	None
Panama	Draft	2016		Americas	None
Papua New Guinea	No			Oceania	None
Paraguay	No			Americas	None
Peru	Yes	2011		Americas	Dirección de Protección de Datos Personales
Philippines	Yes	2012		Asia	National Privacy Commission
Poland	Yes	1997	2018	EU	Inspector General for the Protection of Personal Data
Portugal	Yes	1991	2018	EU	Comissão Nacional de Protecção de Dados
Qatar	Yes	2016		Asia	Unknown
Romania	Yes	2001	2018	EU	National Supervisory Authority For Personal Data Processing

Country	Has law	From	Latest	Region	DPA
Russia	Yes	2006	2014	Europe (ex EU)	Roscomnadzor
Rwanda	No			Africa	None
Samoa	No			Oceania	None
San Marino	Yes	1983	1995	Europe (ex EU)	Unknown
São Tomé and Príncipe	Yes	2016		Africa	Unknown
Saudi Arabia	No			Asia	None
Senegal	Yes	2008		Africa	Commission de protection des données personnelles
Serbia	Yes	2008		Europe (ex EU)	Commissioner for Information of Public Importance and Protection of Personal Data
Seychelles	Yes	2003		Africa	Office of the Data Protection Commissioner
Sierra Leone	No			Africa	None
Singapore	Yes	2012		Asia	Personal Data Protection Commission
Slovakia	Yes	1992	2018	EU	Data Protection Office of the Slovak Republic
Slovenia	Yes	1990	2018	EU	Information Commissioner of the Republic of Slovenia
Solomon Islands	No			Oceania	None
Somalia	No			Africa	None
South Africa	Yes	2013		Africa	Information Regulator
South Korea	Yes	1994	2015	Asia	Ministry of the Interior
Spain	Yes	1992	2018	EU	Spanish Data Protection Commissioner’s Office
Sri Lanka	No			Africa	None
St. Kitts and Nevis	Draft	2012		Americas	None
St. Lucia	Yes	2011		Americas	Unknown
St. Maartens	Yes	2010		Americas	Personal Data Protection Supervisory Committee
St. Vincent and the Grenadines	Yes	2003		Americas	Unknown
Sudan	No			Africa	None

Country	Has law	From	Latest	Region	DPA
Suriname	No			Americas	None
Swaziland	Draft	2013		Africa	None
Sweden	Yes	1973	2018	EU	Datainspektionen
Switzerland	Yes	1992	2006	EU	Federal Data Protection and Information Commissioner
Syria	No			Asia	None
Taiwan	Yes	1995	2010	Asia	National Communication Commission
Tajikistan	No			Asia	None
Tanzania	No			Africa	None
Thailand	Yes	1997		Asia	None
Togo	No			Africa	None
Tonga	No			Oceania	None
Trinidad and Tobago	Yes	2011		Americas	Office of the Information Commissioner
Tunisia	Yes	2004		Africa	National Personal Data Authority, Tunisia
Turkey	Yes	2016		Europe (ex EU)	Kişisel Verileri Koruma Kurumu
Turkmenistan	No			Asia	None
Tuvalu	No			Oceania	None
Uganda	Draft	2015		Africa	None
Ukraine	Yes	2010	2017	Europe (ex EU)	Ukrainian Parliament Commissioner for Human Rights
United Arab Emirates	Yes	2015		Asia	Commissioner of Data Protection
United Kingdom	Yes	1984	2018	EU	Information Commissioner’s Office
United States	No			Americas	None
Uruguay	Yes	2008		Americas	Unidad Reguladora y de Control de Datos Personales
Uzbekistan	No			Asia	None
Vanuatu	No			Oceania	None
Venezuela	No			Americas	None
Vietnam	Yes	2010		Asia	Unknown

Country	Has law	From	Latest	Region	DPA
Yemen	Yes	2012		Asia	Unknown
Zambia	No			Africa	None
Zimbabwe	Yes	2002		Africa	Unknown

Table 19: List of data protection acts and authorities