Forum Privacy and Self-determined Life
in the Digital World

DATA PROTECTION AUTHORITIES UNDER THE EU GENERAL DATA PROTECTION REGULATION

A new global benchmark (extended version)

Imprint

Data Protection Authorities under the EU General Data Protection Regulation. A new global benchmark (extended version)

Author

Philip Schütz[1]

Institutional Affiliation

(1) The author is a doctoral researcher at the University of Göttingen and a full-time Data Protection Coordinator at Mercedes-Benz

Editors

Michael Friedewald, Alexander Roßnagel, Christian Geminn, Murat Karaboga

Publication series

Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt

ISSN-Print	2199-8906
ISSN-Internet	2199-8914
DOI	10.24406/ISI-N-642963

Published

January 2022, 1. Edition
Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe

Recommended citation

Schütz, Philip (2022): Data Protection Authorities under the EU General Data Protection Regulation. A new global benchmark (extended version). Eds.: Michael Friedewald et al., Forum Privacy and Self-determined Life in the Digital World, Karlsruhe: Fraunhofer ISI.

Notes

This work is an extended version of the chapter "Data Protection Authorities under the EU General Data Protection Regulation – a new global benchmark" forthcoming in Maggetti, M.; Di Mascio, F.; Natalini, A.: The Handbook on Regulatory Authorities. Cheltenham: Edward Elgar Publishing.

Table of contents

1 The Importance and Peculiarity of Data Protection Regulation and Associated Supervisory Authorities

While most of the classical regulatory authorities operate in the realm of correcting market failures, supervisory authorities in the regulatory field of data protection, so-called data protection authorities (DPAs), are above all supposed to act as guardians of the fundamental right to data protection (data privacy) (cf. ECJ 2010: recital 23), monitoring not only corporations, but also the state itself in their insatiable hunger for more data, information, power and control.

As noted frequently, data has become the new oil of the 21st century information and knowledge societies, spawning ever larger and mightier growing IT companies, so-called Big Tech (mostly referring to the US-American Big Five Apple, Microsoft, Amazon, Alphabet (Google) and Facebook).[1] The market capitalisation of these monopolists is moving from one record to another, even accelerated by the COVID-19 pandemic, while at the same time entire state economies as well as certain economic sectors are in danger of collapsing.

In the meantime, the Snowden revelations of 2013 have impressively shown the increasing convergence of commercially collected data and state-run surveillance, whereas the *Cambridge Analytica* scandal exemplified the detrimental effect the unregulated access to massive collections of personal data by IT companies either willingly breaking or ignoring data protection laws can have on sensible points of democratically organised societies, such as their electoral processes. Both cases highlight the great significance of and the associated strategic interest in (personal) data (cf. e.g. Zuboff 2019).

Accordingly, the need for an effective regulation in that area is evident. With the General Data Protection Regulation (GDPR 2016) the European Union set a new global benchmark *inter alia* with regards to important legal requirements for an effective working supervisory authority. That is why the main focus of this contribution lies on DPAs in the EU (including – despite its withdrawal – the United Kingdom), however also taking data protection regulation in the United States of America, the most dominating data controlling nation worldwide, into account. This paper furthermore pursues a comparative perspective on DPAs, drawing on key results of the author's doctoral research study, including theoretically developed variables trying to explain regulatory effectiveness of DPAs, such as their independence, resources, regulatory powers and practices (cf. Schütz (forthcoming)).

After a state-of-the-art analysis summarises the most significant research and literature on DPAs, theoretical and methodological challenges in doing research on DPAs are outlined and a brief history of the development of data protection legislation is presented in order to get a better understanding of the current national and international data protection regimes. The empirical part of this work then focuses on a comparative analysis of DPAs' independence, resources, regulatory powers and practices, eventually concluding with prospects on future data protection research.

[1] Mostly left out of that list are other emerging US tech giants like Tesla as well as Chinese IT companies, such as Alibaba, Tencent and Baidu, which however become more and more relevant.

2 State of the Art

The media coverage on surveillance, privacy and data protection violations these days is enormous. However, the huge popularity of the topic should not hide the fact that this is an often shallow and non-scientific debate lacking systematic empirical research and long-term studies in the field. Not surprisingly, legal scholars from a more theoretical perspective and computer scientists with a more application-oriented approach have been dominating debates and research on data protection so far. Whereas the jurisprudence usually concentrates on interpreting data protection legislation and respective case law, information technology (IT) research aims at the development of technical and organisational concepts and solutions, such as identity management, privacy by design and privacy-enhancing technologies (PETs), which often work by means of access rights management, cryptography or anonymisation techniques.

On the contrary, social sciences, and in particular political science with some exceptions (cf. *inter alia* Bennett (1992), Bennett & Raab (2006), Busch (2010, 2011, 2013, 2015), Mayer-Schönberger (1998), Newman (2008), Raab (2011), Regan (2009), Schütz (2012a,b and 2018), Schütz & Karaboga (2015) and Karaboga (forthcoming)), have long neglected the policy field of data protection even in contempt of a high density of data protection regulations on the international, national and sometimes even regional level. That is why classical social science methods, such as quantitative and qualitative analyses, as well as comparative approaches have only slowly made their way into research on data protection.

Only a few authors (particularly Flaherty (1989), Bennett (1992), Bennett & Raab (2006) and Busch (2010)) have early on conducted comparative policy research in the field of data protection, contributing over the years to a better understanding of the differences in and mechanisms behind data protection legislations.

With regards to comparative research on data protection authorities, particularly the by now famous international comparison of privacy policies and associated regulatory authorities in West Germany, Sweden, France, Canada and the United States by Flaherty (1989) set a new benchmark in conducting in-depth comparative analyses of data protection legislation and regulatory practices of DPAs. While the contribution of Flaherty is extremely rich in detailed empirical research on different data protection regimes with practical recommendations for the improvement of privacy regulations in the end, the work of Bennett (1992) has a much more analytical character, trying to answer the question as to how and why different countries with divergent institutional settings and cultural traditions choose certain regulatory approaches to data protection.

With the emergence of the EU Data Protection Directive as the first legally binding international data protection framework there seems to be a break in comparative research on data protection legislation, rather shifting to analyses at the international level (e.g. Bennett & Raab 2006;[2] Mayer-Schönberger 1998) and investigating the creation of the Directive itself (e.g. Newman 2008), associated agreements (e.g. Busch 2013) or networks of DPAs (e.g. Raab 2011).

First publicly funded comparative studies on DPAs in the EU (Korff 1998, 2002) appeared in the wake of the evaluation of the Directive's implementation.[3] In the following Korff et al. (2010) conducted another major investigation for the EU Commission, comprising detailed country case

[2] Revisited in the light of the GDPR fifteen years later in Bennett & Raab (2020).

[3] Additionally, the EU Commission (2003) issued its own report on the implementation of the Data Protection Directive.

studies and analyses on data protection regimes in EU Member States (including information on budgets, personnel, different regulatory functions, powers and practices of DPAs). Next to that research that played a decisive role in preparing the grounds for the 2016 EU data protection reform package, the EU Agency for Fundamental Rights FRA (2009, 2010) produced a similarly comprehensive study, providing – as the Korff study – for the first time extensive empirical material and data on the different legal conditions for and *de facto* activities of DPAs.

One of the rare comparative social science research projects in data protection (Busch 2010) devotes itself to the analysis of the different national regulatory answers towards potentially privacy-invasive technologies. The project found not only different modes of regulation, but also varying degrees of politicisation often caused by citizens trust or distrust of the state (Ibid.: 20).

Important comparative works on DPAs in the following years involve particularly Righettini (2011), who focuses in her analysis on different regulatory activities and styles of the French and Italian data protection authority, Bignami (2011), dedicating her work to an empirical analysis of data protection regulatory styles in France, Britain, Germany and Italy, as well as Greenleaf (2012a,b) and Schütz 2012b, both dealing with the issue of DPAs' independence from a comparative perspective.

In 2013, the first major EU research project dealing exclusively with the subject of DPAs was launched. In the wake of GDPR's new challenging cooperation and coordination mechanisms among DPAs in EU Member States (cf. section 5.1) the PHAEDRA project aimed to improve practical co-operation and co-ordination between DPAs, privacy commissioners and privacy enforcement authorities, especially with regards to the enforcement of privacy laws. In 2015, a continuation of the project called PHAEDRA II followed. During the project series, several pieces of research that comprise helpful empirical data on DPAs were published (see for example Barnard-Wills (2017), De Hert et al. (2015) and Wright & De Hert (2016)). Further comparative works on DPAs and their different regulatory handling include Finn et al. (2014), González-Fuster et al. (2015) and Vranaki (2016).

With the advent of the GDPR, not only the EU Commission (2020) and the European Data Protection Board (EDPB) (2020) saw the need for a thorough evaluation of the status and role of DPA in EU Member States, but there was also an increased scientific interest in DPAs and e.g. associated case law (Bieker 2017), IT know how (Raab & Szekely 2017), strategic plans (Kress 2020) and enforcement practices (Daigle & Khan 2020; Sivan-Sevilla forthcoming).[4]

Beyond literature from DPA practitioners, such as Hijmans (2016), Hustinx (2009) and Jóri (2013), a vast amount of annual reports of DPAs and their networks frequently deliver helpful empirical information, such as figures on financial and personnel resources or insights into regulatory practices.

Eventually, there are a variety of legal commentaries on the GDPR, national data protection legislation and associated supervisory authorities written by local data protection experts in their respective language. These commentaries range from works merely reciting the existing law and reflecting the most obvious to oeuvres conducting veritable, in-depth interpretation and far-reaching analyses of data protection policies, including as in the case of one of the most influential German commentary by Simitis et al. (2019: 158ff.) – unfortunately only in German – highly

[4] Worth to mention is moreover the dissertation project of the author of this contribution (cf. Schütz (forthcoming)) that deals with a comparative analysis of DPAs in Europe by taking a closer look at the data protection regimes in the UK and Germany, and identifying key determinants for an effective regulatory model.

elaborate historical and comparative analyses of data protection laws, DPAs and their regulatory practices.[5]

However, most of the mentioned research (and particularly the discussed studies) tends to have a rather descriptive than analytical character, rarely exploring the reasons as to why DPAs behave in a certain way. Often still dominated by legal scholars, the academic discourse on supervisory authorities furthermore mainly revolves around the *de jure* dimension, usually neglecting what DPAs' independence, capacities and regulatory approaches look like in practice. Additionally, rarely applying social science methods, existing data protection research does often neither produce useful quantitative nor qualitative data on DPAs.

[5] It should also be noted that particularly in countries with a long tradition in data protection as in Germany there seems to be a strong national data protection scene of data protection experts who only publish in their respective national language and are thus unfortunately – despite their undisputed profound data protection know-how – totally unknown at the international level.

3 Theoretical and Methodological Challenges

There have been, in particular, little theoretical frameworks and/or methodological approaches to the analysis of DPAs. Though theoretical foundations of and empirical findings on other independent regulatory authorities (IRAs), such as central banks, can help to serve as a framework for the analysis of DPAs (cf. Schütz (2012a,b)), existing research on IRAs very much focuses on the *de jure* and *de facto* configuration of independence (including the autonomy of IRA decision-makers, financial and organisational autonomy) (cf. e.g. Gilardi & Maggetti (2011)) and associated good governance principles (*inter alia* accountability, transparency and integrity) (e.g. Quintyn 2009), largely ignoring further elements that determine regulatory effectiveness, e.g. overall institutional settings at the national and supranational level, regulatory powers as well as individual leadership skills, regulatory styles and traditions (cf. Schütz (forthcoming)).

Since – as we will learn later – data protection legislation and surrounding *de jure* features of DPAs are more and more converging (at least within the EU), analysing differences in the *de facto* regulatory handling of supervisory authorities should come to the fore. In that respect, there are above all two important works focusing on regulatory practices of DPAs.

Making use of Richardson et al.'s (1982) national policy style concept, the first is Righettini (2011: 145), who identifies two major archetypes of regulatory styles that shape different approaches to the regulation of data protection: "the *active* type, focused on a *command and sanction* approach and the *reactive* type, focused on a *soft and self-regulation* approach". Following Jordana & Levi-Faur (2004: 6), Righettini (2011: 145) describes in more detail that the (pro-)active approach, also called regulation *for* data protection, and the reactive type, i.e. regulation *of* data protection, differ most of all in their degree of intrusiveness of the public independent authority. While the first "requires far more regulative capacities [...] [and its] institutional output is much more oriented towards an indirect promotion and defence of individual rights, and the enforceability of law, as well as to control the conformity of application by the use of administrative controls such as inspective powers and sanctions", the latter "is less intrusive and the institutional output is much more oriented towards a reactive use of judicial resources and towards implementation through para-judicial conflict resolution and soft regulation, i.e. self-regulation and simplification." (ibid.) Righettini further identifies DPAs' resources, independence, certain overall institutional settings (such as the role of the state or the landscape of other IRAs), but above all institutional leadership as key explanatory variables for the differences in regulatory outcomes (ibid.: 162).

The second is Bignami (2011) who observed a convergence not only in European data protection laws, but also in DPAs' regulatory practices. Opposed to the US-American adversarial litigation style in regulating data protection, she has coined the term *cooperative legalism* for the regulatory style of European DPAs, describing a mix of deterrence-oriented approaches (e.g. the threat of inspections or sanctions) and self-regulatory mechanisms (such as appointments of data protection officers or the usage of privacy seals) (ibid.: 460). Above all, she sees systemic variables, such as "regulatory realities of the new digital marketplace, [...] the credible commitments logic [of policy-makers] and the diffusion process triggered by Europeanization" responsible for that development.

Both of these works are extremely valuable to the comparative analysis of DPAs, but will only be briefly touched upon in this work that otherwise concentrates on the empirical analysis of differences in independence, resources, regulatory powers and practices.

4 The Four Stages of Development in Data Protection Legislation in Europe and the USA

According to Simitis et al. (2019: 179ff.) data protection legislation in the Western hemisphere – including the establishment of competent supervisory authorities – mainly followed four stages of development (cf. Figure 1).[6]

The first laws in the 1970s were directed towards restrictions of huge centralised data banks and storage facilities mostly operated by governments. The pioneering Hessian Data Protection Act (*Hessisches Datenschutzgesetz* – HDSG (1970), the Swedish Data Act of 1973 as the first national data protection law worldwide, the U.S. Privacy Act of 1974 and the Data Protection Act of the German state Rhineland-Palatinate in the same year, the German Federal Data Protection Act (*Bundesdatenschutzgesetz* – BDSG (1977) and the following legislations of the West German Länder can all be regarded as direct attempts to tackle the challenges arising from publicly-run mainframe computers and national data banks (Mayer-Schönberger 1998: 221). As part of that development, by and large three distinct regulatory models emerged: on the one hand, the German BDSG as well as the Austrian Data Protection Act (*Datenschutzgesetz* – DSG (1978)) focused on a more general, all-encompassing, yet also rather flexible legal framework with DPAs fulfilling a rather consultative and advisory function, whereas Sweden took the opposite direction, introducing a licensing approach that made the automated processing of personal data subject to prior authorisation by the competent supervisory authority, the Data Inspection Board (DIB) (Simitis et al. 2019: 179f.). The United States, on the other hand, neither established a general data protection framework (the Privacy Act only applies to the Federal Government) nor an independent DPA (as one of a few OECD countries left), but opted instead for a patchwork of different sector-specific regulations (ibid.: 180) that have been revealing large gaps in effectively regulating the processing of personal data (Bennett & Raab 2006: 131). Entrusted with the enforcement of the Fair Credit Reporting Act of 1970, the Federal Trade Commission (FTC) represents the central regulatory authority with regards to the processing of personal data by US companies, which are not at all subject to the afore-mentioned Privacy Act.

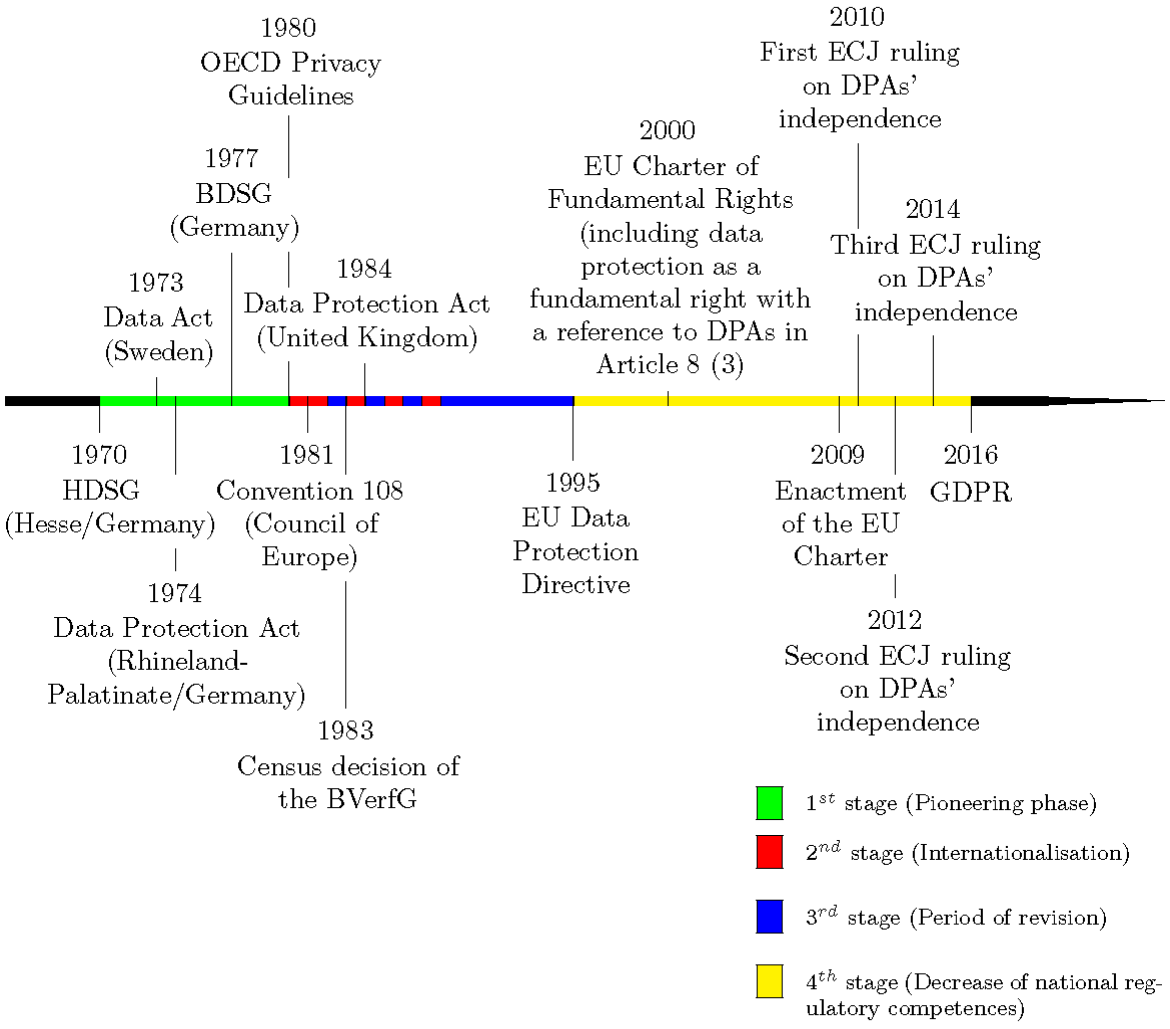
Within that first stage of development a second generation of data protection provisions focused on strengthening individual privacy rights, explicitly linking data protection to the right of privacy in the context of new emerging and rapidly spreading decentralised state- and business-run databases (Mayer-Schönberger 1998: 226ff.). At the very forefront of that legislative development were France (1978), Austria (1978), to a certain extent Denmark (1978) and Luxembourg (1979). Being ahead of their time, some European states, such as Portugal (1976) and Spain (1978),[7] as well as the German state of North-Rhine Westphalia (1978) even integrated data protection as a

[6] During the initial opinion-forming processes of data protection legislation in the late 1960s in Germany legal experts came to the conclusion that it would be wise to refrain from the fuzzy term and concept of privacy in legislative texts and rather create instead the neologism *Datenschutz* (later used in many jurisdictions and languages such as in English data protection, in French protection des données, in Spanish protección de datos, in Polish ochrona danych osobowych, etc.). Though the exact etymology of the term remains unclear, there are two main traces that can be followed in the literature. Whereas Hansjürgen Garstka (2008: 134), Data Protection Commissioner of Berlin from 1989 to 2005, sees an orientation and analogy towards the term of *Maschinenschutz*, a concept introduced in the 1960s in order to improve the safety of workers on power-driven machines, Spiros Simitis (2014: 83f.), creator of the first data protection act worldwide in Hesse as well as Hessian data protection commissioner from 1975 to 1991, is of the opinion that the term *Datensicherung* (data security) served as a role model.

[7] Austria declared data protection as a fundamental right only at a sub-constitutional level, namely in the Data Protection Act of 1978.

fundamental right into their constitution, but in the case of the first two without drafting a separate data protection law or setting up a competent supervisory authority (cf. Table 1). The role of DPAs in that period changed in so far as the new focus on individual privacy and the empowerment of data subjects called for an authority that would be able to handle complaints and assist citizens in their requests as an ombudsman-like institution (ibid.: 228).

Figure 1: Timeline of important developments with regard to DPAs in Europe from 1970 to 2016 (development stages colour-coded)



Source: own research – development stages based on Simitis et al. (2019: 179ff.).

Next to the numerous national data protection provisions, also international regimes, such as the OECD Privacy Guidelines (1980), started to play an influential role in the proliferation of data protection legislation in Europe. Opposed to the non-binding OECD Guidelines, the Data Protection Convention 108 of the Council of Europe (CoE) (1981) was the first international data protection agreement comprising legally binding rules for all signing member states.[8] However, except for

[8] Way before the Convention 108, the United Nations (1948) in its famous Universal Declaration of Human Rights (article 12) as well as the CoE (1950) in its European Convention on Human Rights (article 8) included a rather vague conception of the right to privacy/private life, only insufficiently covering aspects of informational privacy and data protection.

obliging designated supervisory authorities to cooperate (Article 13) as well as to assist in cases of foreign residents pursuing their data protection rights (Article 14), the Data Protection Convention fell short of setting international standards in DPAs' status and tasks (Hustinx 2009: 132). It was not until 2001 that the CoE adopted an additional protocol (ETS No.181) to Convention 108, requiring member states to set up an independent national supervisory authority that monitors compliance with data protection legislation.

For Simitis et al. (2019: 181), the Convention marks the advent of the second development stage of data protection legislation, heralding the **internationalisation** and beginning of data protection convergence in Europe. In that context, the authors (ibid.: 181) particularly refer to the UK as a textbook example of the major influence the Data Protection Convention had in resolving the gridlocked situation that dominated the national data protection policy-making process for over a decade, resulting in the first UK Data Protection Act of 1984.[9]

The third development stage is characterised by a **period of revision**, dominated by the question how to enable individuals to exercise control over their personal data in practice. In 1983, the landmark decision of the German Federal Constitutional Court (*Bundesverfassungsgericht* – BVerfG (1983)) to overturn the national census law and establish the fundamental right to informational self-determination provided a legal answer to this question. In that so-called *census decision*, the BVerfG (1983: 49) emphasised the involvement of independent data protection authorities as of significant importance for the effective protection of the right to informational self-determination.[10]

During that period of revision policy-makers also started to realise that none of the aforementioned different regulatory models, i.e. licensing, flexible arrangements or sectoral approaches, worked as effective and efficient as originally envisaged (Simitis et al. 2019: 181f.). On the one hand, the licensing approach in Sweden and France resulted in excessively bureaucratic and hence highly burdensome registration procedures, hindering competent supervisory authorities to adequately fulfil their other, equally or even more important regulatory tasks (Flaherty 1989: 394). On the other hand, the rather vague and fuzzy data protection provisions in Germany let data controllers profit from the different and sometimes even contradictory interpretations of the law, while sectoral regulations in the U.S. without any DPA whatsoever led to huge regulatory gaps and different standards in rules on how to handle the processing of personal data (Simitis et al. 2019: 182).[11]

In the late 1980s, Finland (1987), Ireland (1988) and the Netherlands (1988) followed the then still minority of EU Member States having enacted data protection legislation. Especially in the case of the Netherlands, which introduced data protection as a fundamental right at the constitutional level already in 1983, the first data protection act noticeably reflects the doubts about already

[9] For more examples of the impact of Convention 108 on other national laws see González-Fuster (2014: 92ff.).

[10] In further decisions the BVerfG (1984, 1987) continued to underline the importance of DPAs' regulatory role, e.g. by putting the independence and assignments of DPAs on the same level with those of courts (Wippermann 1994: 930). As a side note, the widely-used English translation of the census decision by Bröhmer et al. (2012: 150ff.) unfortunately comprises a fatal translation error. The German term "Datenschutzbeauftragter" was translated as "data protection officer", while in fact it can also mean "data protection commissioner", which seems to be the more appropriate meaning in the context and later interpretation of the relevant ruling.

[11] Within that period of revision Mayer-Schönberger (1998: 229ff.) furthermore differentiates between third-generation data protection statutes following the census decision of the BVerfG (such as the amendment to the Austrian DSG in 1986 or the late-coming General Amendment to the BDSG in 1990) and a fourth generation of holistic and sectoral approaches (e.g. in Finland 1987 or Belgium 1992), which aimed at further strengthening the still weak bargaining position of the individual by introducing mandatory legal protection in cases of processing of certain sensitive categories of personal data as well as establishing separate quasi-ombudsman advocative DPAs and more detached, impartial and adjudicative enforcement institutions.

existing regulatory models in data protection, while at the same time indicating the willingness of Dutch policy-makers after over a decade of discussing and continually postponed legislation to learn from the mistakes of the other countries and innovate regulation (Simitis 2014: 140f.). At the end of the period of revision, Portugal (1991), Spain (1992) and Belgium (1992) passed data protection statutes relatively late, whereas Italy and Greece remained at that point of time the last EU Member States without similar regulations in place (cf. Table 1).

Table 1: Data protection and freedom of information legislation in the EU, UK and USA

	Year of enactment of first data protection legislation	Reference of data protection as a fundamental right in the constitution	Freedom of Information (FOI) related tasks of DPA (enactment of first FOI legislation)
Austria	1978	No (but constitutional provision in the DSG of 1978)	No (since 1987)
Belgium	1992	No	No (since 1994)
Bulgaria	2002	No	No (since 2000)
Croatia	2003	Yes (art. 37) (since 1992)	No (since 2003)
Cyprus	2001	No	No (-)
Czechia	1992	Yes (art. 10) (since 1993)	No (since 1999)
Denmark	1978	No	No (since 1970)
EDPS (at EU level)	2000	Yes (art. 8) (since 2000/2009)	No (since 2001)
Estonia	1996	No	Yes (since 2000)
Finland	1987	Yes (art. 10) (since 1995)	No (since 1951)
France	1978	No	No (since 1978)
Germany (federal level)	1977	No	Yes (since 2006)
Germany (Länder)	1970-1992	Yes (10), No (6)	Yes (12), No (4)
Greece	1997	Yes (art. 9a) (since 2001)	No (since 1986)
Hungary	1992	Yes (art. 6) (since 1989)	Yes (since 1992)
Ireland	1988	No	No (since 2003)
Italy	1996	No	No (since 1990)
Latvia	2000	No	No (since 1998)
Lithuania	1996	Yes (art. 22) (since 1992)	No (since 1996)
Luxembourg	1979	No	No (-)
Malta	2001	No	Yes (since 2012)
Netherlands	1988	Yes (art. 10) (since 1987)	No (since 1978)
Poland	1997	Yes (art. 51) (since 1997)	No (since 2001)
Portugal	1991	Yes (art. 35) (since 1976)	No (since 2007)
Romania	2001	No	No (since 2001)
Slovakia	1992	Yes (art. 19) (since 1992)	No (since 2000)
Slovenia	1990	Yes (art. 38) (since 1991)	Yes (since 2003)
Spain	1992	Yes (art. 18) (since 1992)	Yes (since 2013)
Sweden	1973	Yes (art. 3) (since 1974)	No (since 1766)
United Kingdom	1984	No	Yes (since 2001)
USA (federal level)	1974 (but limited scope and no DPA)	No	No (since 1967)
USA (state level)	Several sectoral laws (no DPAs)	No (unlike a fundamental right to privacy)	No (but all 50 states have FOI laws)

Source: own research based on data from Bennett & Raab (2006: 127), Banisar & Davies (1999–2000), Roßnagel (2009: 103), the Fundamental Rights Agency FRA (2009), Banisar (2006) as well as AIE (Access Info Europe) & CLD (Centre for Law and Democracy) (2017).

With the end of the Cold War the drafting of data protection legislation received a significant boost throughout the whole of Europe. Most ex-communist countries in Central and Eastern Europe, including the new federal states of Germany, not only quickly passed data protection acts (e.g. Slovenia even before the collapse of Yugoslavia in 1990, Hungary in 1992, Czechoslovakia – later the two separate countries Czech Republic and Slovak Republic – in 1992), but also incorporated data protection as a fundamental right into their newly created constitutions, such as in Hungary (1989), Slovenia (1991), Slovak Republic (1992), Croatia (1992), Lithuania (1992) Czech Republic (1993) and all of the New German Länder (1992–93). While that development highlights the great priority attributed to data protection as a fundamental right in the democratisation processes and emergence of constitutional states in Central and Eastern Europe, data protection in most of the Western European states had already begun throughout the 1980s to "cease to be merely a human rights issue; it was also intrinsically linked to the operation of international trade." (Bennett & Raab 2006: 93) Thus, particularly in the context of rapidly spreading computer technology, not only in the public, but more and more in the private sector, the processing of personal data and associated transfers across borders had finally become a crucial factor in economic trade and politics.

Due to the complicated patchwork of different data protection acts and standards in Europe the international transfer of personal data particularly among transnational corporations became increasingly difficult. National data protection rules had become above all a veritable trade barrier. The imminent risk of a serious obstacle in the completion of the internal market was in the following used as the main argument for the European Commission to start drafting the proposal for a Data Protection Directive in 1990 (cf. Gutwirth 2002: 91). The rather pragmatic economic argument did not only help to convince national governments as well as private-sector stakeholders of the benefits of a common legal framework, but also served as a legitimate reason for the EU Commission to get active, primarily based on Article 100a of the EEC (1957: 1029) and later EC Treaty (1992: 23), which allows for legislative initiatives by the Commission that "have as their object the establishment and functioning of the internal market."[12] Hence, the proposal of the Directive was mainly developed in the Internal Market portfolio of the EU Commission (Bennett & Raab 2006: 93). However, as González-Fuster (2014: 124ff.) rightfully points out, the European-wide implementation of rules for the protection of individuals with regards to the processing of personal data remained the main objective of the legislative project, accompanied by a major second objective: to ensure the free flow of data.

Regarding the emergence of a common EU data protection framework in 1995, Simitis et al. (2019: 183ff.) speak eventually of a fourth development stage characterised by a significant **decrease of national regulatory competences (supranationalisation)**, particularly true for all EU Member States and candidate countries at that time, but also applicable to other nations with close economic ties to EU countries and associated transborder flows of personal data.[13] Opposed to CoE's Convention 108, this time EU Member States did not have a choice in transposing the Directive into national law. That way, even EU nations which had not yet succeeded in passing their own data protection legislation, such as Italy (1996) and Greece (1997), were forced to draft their first data protection acts. With the prospects of ex-communist countries in Central and East-

[12] In that context it is important to note that the commitment of the European Economic Community (EEC) in the 1987 amendment (Single European Act) to the Treaty of Rome (1957: art. 8a) to aim for the completion of the internal market until 1992 put additional pressure on harmonisation efforts of the EU Commission (González-Fuster 2014: 126).

[13] Since Article 25 of the EU Data Protection Directive (1995) (later continued in Article 44 GDPR) prohibits the transfer of personal data from EU Member States to third countries which do not provide an adequate level of data protection, even non-EU countries with an interest in the preservation of free transborder flow of personal data were pressured to adjust their legislations to the standards foreseen by the Directive or later Regulation.

ern Europe to join the EU those states which had not yet passed data protection legislation, e.g. Poland (1997) or the Baltic states of Estonia (1996), Lithuania (1996) and Latvia (2000), could align their newly created acts closely to the requirements and standards of the EU Data Protection Directive.[14] The EU enlargement in 2004 caused also Malta (2001) as well as Cyprus (2001) to pass their first data protection acts, which was likewise the case for Bulgaria (2002) and Romania (2001) before their accession in 2007, as well as Croatia (2003) in 2013. In contrast to countries with a rather short history in regulating the use of personal data, EU Member States that could look back at a long tradition of data protection, such as France and Germany, particularly struggled – even under the threat of EU infringement procedures – to bring their data protection laws in line with the Directive (Simitis 2019 et al.: 183; Dente 2011: 122).

Part of the fourth development stage is the fact that data protection became a fundamental right in the EU Charter of Fundamental Rights (2010: art. 8). Though the Charter only came into force in 2009 when the Treaty of Lisbon was enacted, the protection of the individual with regards to the processing of personal data was enormously strengthened, now constituting a legally binding fundamental right at the European level.[15] Additionally, DPAs were granted constitutional status in Article 8 (3) of the EU Charter of Fundamental Rights, clarifying that compliance with data protection rules "shall be subject to control by an independent authority." And also the Lisbon Treaty, which amended the Treaty on European Union (TEU (2010)) as well as the Treaty on the Functioning of the European Union (TFEU (2010)) adopted the same wording in Article 39 of TEU and Article 16 of TFEU.[16]

With the enactment of the GDPR in 2016 the period of supranationalisation preliminary finds its end (Simitis et al. (2019): 183), resulting in an even more-assertive generation of data protection legislation that not only continues the process of decreasing national regulatory competence in data protection (relevant for all EU Member States and candidate countries, as well as transnational actors processing personal data of EU residents (cf. *Lex loci solutionis*)), but also significantly enhances the enforceability of already existing data protection principles by strengthening above all DPAs' intervention powers, such as the opportunity to issue monetary penalties of up to 4 per cent of the annual turnover of non-compliant data controllers. That way, the GDPR has become a new global benchmark for rules governing the processing of personal data.

The following empirical part will analyse the *de jure* and *de facto* role of DPAs under the GDPR, including important elements of their effective functioning, such as their independence, resources, regulatory powers and practices.

[14] Additionally at the European level, EU institutions subjected themselves in form of Regulation 45/2001/EC to a newly created supervisory authority, the European Data Protection Supervisor (EDPS).

[15] While all EU Member States have enacted data protection legislation as well as installed competent supervisory authorities, only 15 of 28 EU nations (not including Austria, which only passed a constitutional provision in the Data Protection Act of 1978, and Germany with regards to the federal level) recognise data protection as a fundamental right in their constitutions (cf. Table 1).

[16] The gradual transfer of national regulatory competences in data protection to the EU-level is eventually accompanied by an increasing importance of the EU judiciary and its decisions (see section 5.3 and footnote 23).

5 The Role of DPAs under the GDPR

At the international level, the EU General Data Protection Regulation represents the most comprehensive and influential legislative framework of data protection worldwide. Opposed to its predecessor, the EU Data Protection Directive of 1995, the GDPR did not have to be transposed into national law. As an EU Regulation, the GDPR is a legal act that becomes immediately enforceable as law in all Member States at the same time, limiting the before existing leeway in the transposition of EU law (except for some opening clauses). Crucial to note is that the GDPR (article 56) foresees a single national supervisory authority (i.e. the *lead authority*) to be responsible for the data controller that is located with its main establishment (including European headquarters of international corporations) in the authority's jurisdiction. That approach is called the *one-stop shop principle*.[17]

5.1 International cooperation and coordination mechanisms as well as networks of DPAs

In order to ensure its consistent application, the GDPR foresees several cooperation (article 60-62) and coordination (article 63-67) mechanisms. For example, to counter the risk of a lead authority failing to carry out its regulatory duties, Article 63 provides for a so-called *consistency mechanism*, which enables remaining DPAs of the Member States as part of the European Data Protection Board (EDPB), i.e. the EU supranational data protection body composed of representatives of the EU Member States' DPAs, to issue legally binding decisions by a two-third majority that would overrule previous decisions made by a lead authority or enforce otherwise omitted regulatory actions. Contrary to its predecessor under the Data Protection Directive, the Article 29 Working Party, the EDPB that way not only functions as an advisory but also as a decision-making body. Though the consistency mechanism has often failed to fulfil its function so far (since necessary majorities in the EDPB are difficult to organise)[18] the latest monetary penalty against WhatsApp shows that the mechanism can indeed work in practice, giving hope that data protection can be dealt with in a consistent manner throughout the EU (cf. section 5.5.2).

Established by the Data Protection Convention 108 of the CoE (1981: art. 18), the *Consultative Committee of Convention 108* (T-PD) is another international data protection network that consists of representatives of Member States having signed and/or ratified the Convention (complemented by observers from other States and international organisations). The Committee is *inter alia* responsible for making proposals to facilitate or improve the application of the Convention, to amend the Convention as well as for issuing opinions (including reports and guidelines) on data protection issues (ibid.: art. 19). However, only part of the representatives sent out by the Member States and/or observer states are DPA officials.

The *European Conference of Data Protection Authorities* (or so-called *Spring Conference*) is an annual event that brings together DPAs from member states of the EU and the CoE. Discussing matters of common interest and exchanging information and experiences on different topics, the

[17] Under certain conditions, however, the ECJ (2021) only recently ruled that "a national supervisory authority may exercise its power to bring any alleged infringement of the GDPR before a court of a Member State, even though that authority is not the lead supervisory authority with regard to that processing."

[18] That way, important transnational data controllers (such as the already mentioned Big Five) that are collecting massive amounts of personal data throughout the European Union and worldwide are regulated by a single DPA, such as the Irish, whose regulatory practices now determine the fate of all European citizens.

Conference usually ends with the adoption of a varying number of resolutions (EDPS 2017). Since 1979 the equivalent of the Spring Conference on a global scale is the *International Conference of Data Protection and Privacy Commissioners* (ICDPPC) – from late 2019 on called *Global Privacy Assembly* (GPA 2019) – connecting the efforts of 130 privacy and data protection authorities from across the globe.

There are furthermore a number of specialised international networks of DPAs. For example, the *International Working Group on Data Protection in Telecommunications* (IWGDPT), i.e. the so-called *Berlin Group*, which was founded in 1983 on the initiative of the Berlin Data Protection Commissioner, who has been chairing the Group ever since, concentrates – as the name already suggests – on data protection issues in telecommunications. Comprising representatives of DPAs, other bodies of national public administrations, international organisations as well as scientists from all over the world, the Berlin Group meets twice a year and regularly publishes recommendations in the form of *Common Positions* and *Working Papers* that inspire and provide DPAs and other international networks with relevant expertise. Another specialised network is the *Global Privacy Enforcement Network* (GPEN), which was established in 2010 after the OECD had adopted the Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy in 2007. GPEN aims at connecting privacy enforcement authorities in order to promote and support cooperation in cross-border data protection enforcement.[19]

5.2 Inner-organisational structures

The most widespread organisational principle of DPAs in the EU (but also worldwide) is the so-called *Commissioner model*, which 18 out of 28 Member States chose to follow, while 10 DPAs in the EU are organised in form of a commission with varying numbers of appointed officials (from two to 17).[20] Despite the rather balanced result on pros and cons of the two models (cf. Stewart 2004), there is a trend towards the *Commissioner model* (see for example the latest shift from Data Protection Commission to Data Protection Commissioner in Austria in 2014), strengthening the view of Flaherty (1986: 15) that "individualistic direction of data protection has been more effective than collective efforts".

5.3 The complete independence requirement

Contrary to the work of most IRAs, e.g. monitoring (financial) markets or the utilities sector, it is a distinctive feature of DPAs that they are not only assigned to watch over private-sector organisations, but also to check on the compliance of the public sector, including political actors, such as ministries.[21] Since these political actors can become subject to harsh criticism and potentially strict regulations by supervisory authorities themselves, they have an increased interest in being able to influence and at worst controlling the output and outcome of DPAs' actions (cf. Schütz 2012a: 125f./136). Thus, DPAs administratively linked and accountable to the political executive are particularly at risk of being held in check by governments.

[19] A comprehensive overview of international networks of DPAs and their cooperation mechanisms can be found in Kloza & Galetta (2015: 77ff.) as well as online at https://globalprivacyassembly.org/other- networks/ (last visited 15/07/2021).

[20] In Germany, only Rhineland-Palatinate had set up a parliamentary data protection commission from 1974 to 1991. In the U.S., the Federal Trade Commission (FTC) represents the central supervisory authority when it comes to the regulation of data protection in the private sector.

[21] As Hijmans (2016: 285ff.) does, one could argue that DPAs become that way a separate branch of government as part of the system of checks and balances.

That is why Article 52 (1) of the GDPR – as equally stipulated already by the Directive – explicitly foresees that a DPA "shall act with complete independence in performing its tasks and exercising its powers […]." Opposed to the Directive and as a learning effect from a set of later discussed judgements of the European Court of Justice (ECJ) (cf. Bieker 2017: 127), the GDPR (art. 52 (2-6)) specifies in much more detail concrete conditions for that independence:[22]

2. The DPA "shall […] remain **free from external influence**, whether direct or indirect, and shall neither seek nor take instructions from anybody." (Decisional independence)
3. DPA officials "shall **refrain from any action incompatible with their duties** and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not." (Autonomy of decision-makers/Incompatibility arrangement)
4. The DPA shall be "**provided with the human, technical and financial resources, premises and infrastructure** necessary for the effective performance of its tasks and exercise of its powers […]." (Adequate resources)
5. The DPA shall choose and have "its **own staff** which shall be subject to the exclusive direction of the [DPA] […]." (Organisational independence)
6. The DPA shall be "subject to **financial control which does not affect its independence** and that it has separate, public annual budgets, which may be part of the overall state or national budget." (Financial autonomy)

Moreover, Article 53 and 54 provide for additional safeguard with regards to the necessary competence and the autonomy of DPA decision-makers, stipulating that "[e]ach member shall have the qualification, experience and skills, in particular in the area of the protection of personal data […]" (Art. 53 (2)), "shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties" (Art. 53 (4)), and have a term of office of no less than four years (Article 54 (b)).

In the past, the legal and political reality of applying the complete independence requirement of the Directive has been difficult, reflecting extremely different interpretations and notions of the term "complete independence". The legal set up and status of DPAs, the appointment and dismissal procedures of data protection commissioners (or members of data protection commissions), as well as the degree of organisational and financial autonomy of DPAs have varied from country to country or in a federal state like Germany even from Land to Land sometimes enormously (cf. Schütz 2012b).

In that context, it is worthwhile to briefly discuss three seminal rulings of the ECJ on independence of DPAs that had decisive influence on the aforementioned GDPR stipulations.[23] In the first

[22] Beyond the EU level, the United Nations laid down independence requirements for so-called *national human rights institutions* (NHRIs) in a set of standards in 1994: the so-called *Paris Principles*. According to the annex of the Resolution 48/134, NHRIs should have 1) a composition and appointment of its members that ensures "the pluralist representation of the social forces (of civilian society)", 2) "an infrastructure which is suited to the smooth conduct of its activities, in particular adequate funding, [...] [enabling the NHRI] to have its own staff and premises", and 3) an appointment that "shall be effected by an official act which shall establish the specific duration of the mandate" and its potential renewability. For more information on the set up of DPAs and the *Paris Principles* see Greenleaf (2012a: 6).

[23] The process of European integration with regards to data protection has not only led to an increasing number of EU legislative frameworks, but also resulted in more and more importance of the EU judiciary, above all the European Court of Justice (ECJ) and its decisions. With the enactment of the EU Charter of Fundamental Rights through the Treaty of Lisbon in 2009, the ECJ was now even able to base its decisions in cases of privacy or data protection violations on Article 7 (Respect for private and family life) and/or Article 8 (Protection of personal data), strengthening and expanding the Court's authority. Due to the increasing relevance of DPAs' regulatory role in society, further ECJ judgements on supervisory authorities can be expected.

judgement, the ECJ (2010) found some of the German Länder had violated the Directive's complete independence requirement by incorporating supervisory authorities responsible for monitoring non-public data controllers into the ministerial bureaucracy (mostly ministries of the interior) and thereby subjecting them to State scrutiny, i.e. legal and administrative supervision (in German *Rechts- und Dienstaufsicht*). The court was of the opinion that complete independence "precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task[s] […]", serving as a blueprint for Article 52 (2) GDPR.

The second ruling of the ECJ (2012) addressed the lack of organisational independence of the Austrian Data Protection Commission (at that time). The court particularly saw a violation of the Directive in the fact that not only the managing member of the Commission, but also the staff (mostly civil servants) of the DPA were directly employed by the Federal Chancellery. This finding led to the discussed formulation of Article 52 (4) GDPR.

Eventually, the third decision by the ECJ (2014) denounced the dismissal of then Hungarian Data Protection Commissioner András Jóri by his Government in 2011, clarifying that the premature dismissal of data protection commissioners must be subject to stringent restrictions with regards to the occasion and reasons for that dismissal – even in cases of passing or amending superior (e.g. constitutional) law. This ruling found reflection in Article 53 (4) GDPR.

Beyond the clear influence that these ECJ decisions had on GDPR stipulations, there are a variety of aspects influencing DPAs' independence that were not (or only partially) touched upon in the Regulation. One of the most important is open, fair and transparent nomination and appointment procedures of DPA decision-makers.[24] While the GDPR provides for more transparency in appointment procedures (art. 53 (1)) and explicitly requires qualifications and eligibility conditions for the appointment of DPA decision-makers to be integrated into the respective national data protection law (art. 54 (b)) (in order to avoid the appointment of incompetent regulators), the Regulation refrains from addressing the highly significant selection processes of DPA decision-makers prior to the actual appointment as well as the obligatory involvement of a branch of government (other than the executive), such as parliament, in appointment and nomination procedures. And indeed, reality shows that the government is still very often the agenda-setter in not at all open and transparent nomination and appointment procedures of DPA decision-makers, with the absurd effect that also in times of the GDPR the executive, as an important regulatee itself, often chooses its own regulator.

With the GDPR's harmonisation and improvement of crucial elements in DPA independence (above all organisational and financial autonomy) and – as we will see later – regulatory powers, other variables determining regulatory effectiveness that can not necessarily be dealt with in legal terms become more and more important, such as the actual funding and staffing, individual leadership skills, regulatory styles and practices.

5.4 Financial and human resources

Since the legally most independent DPA can only fulfil its tasks properly with an adequate budget and number of staff, the material dimension of DPAs' independence is closely linked to the ques-

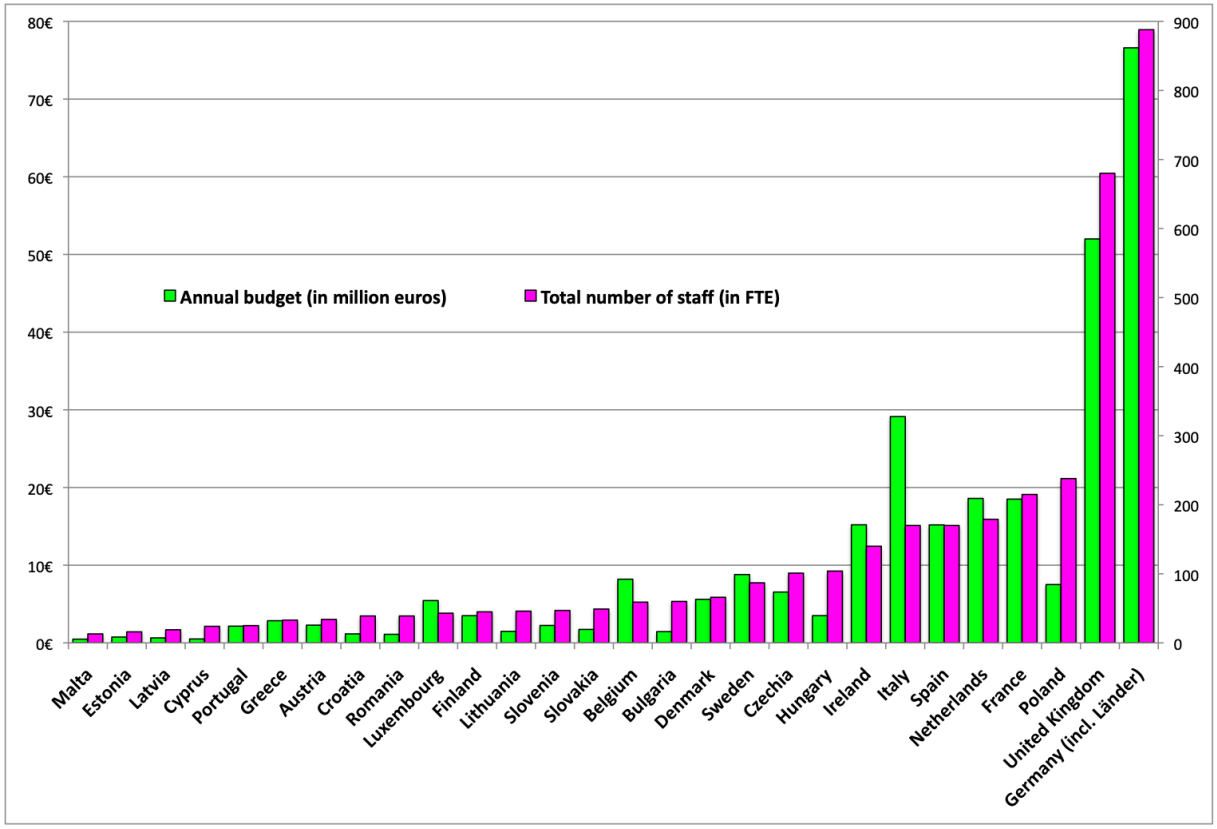
[24] For example, the already mentioned FRA study (2010: 19ff.) found that numerous DPAs suffer from a lack of structural independence, particularly with regards to nomination and appointment procedures of data protection commissioners or other managerial staff, exclusively selected by the government and without the input, review or consent of the legislature. And also an IAPP (2011: 39) study confirms the finding that most of the EU Member States have set up procedures for the appointment of DPA decision makers that are solely determined by the relevant executive branch of government.

tion as to what financial and human resources supervisory authorities can draw on in their regulatory day-to-day work.[25] This is also reflected in the legal requirement of Article 52 (4) GDPR, stipulating that the DPA shall be "provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers […]."

In practice, a variety of studies and reports came repeatedly to the conclusion that many DPAs in Europe suffer from an insufficient level of financial and personnel resources, limiting them in their *de facto* independence and fulfilment of their tasks (e.g. FRA 2010: 20; Schütz 2018). In order to check on these findings and provide in-depth empirical data on the subject, this section presents a comparative analysis of the levels of budget as well as numbers of staff of DPAs in the EU, based on latest figures by the EDPB.[26]

The following Figure 2 shows the total annual budget and number of staff of DPAs in the EU as of 2019, sorted by total number of staff in ascending order.

Figure 2: Financial and human resources of DPAs in the EU (2019)



Source: EDPB (2020).

[25] Though of utmost importance, the quality of staff (including IT specialists) is not dealt with in this paper. Different contributions, such as Raab & Szekely (2017), a study conducted by Brave Software Inc. (Ryan 2020) as well as Sivan-Sevilla (forthcoming), however, come to the conclusion that most DPAs in Europe severely lack relevant IT know-how, which significantly reduces their capabilities of effectively regulating data controllers.

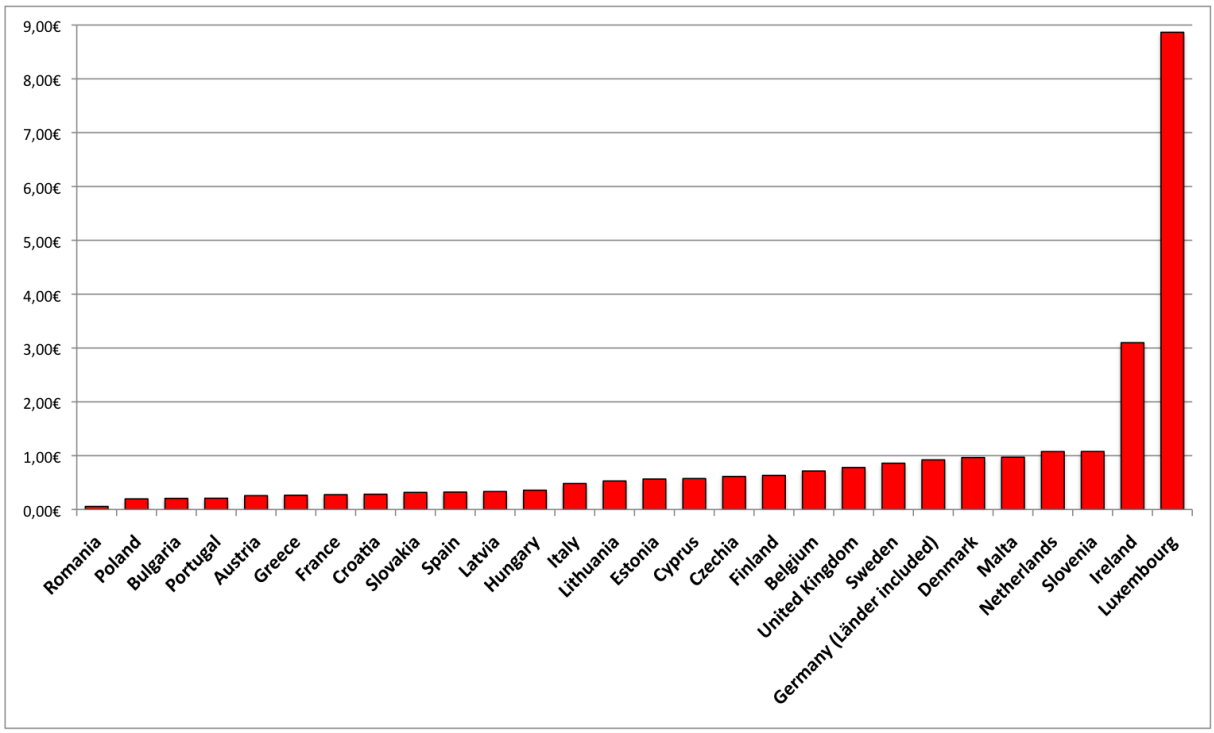
[26] The author is aware of the fact that these figures comprise to a large extent approximate values being subject to certain inaccuracies. For example, figures do not differentiate between DPAs only responsible for data protection and those additionally tasked with monitoring compliance of freedom of information (FOI) issues, such as in Estonia, Germany, Hungary, Malta, Slovenia and the UK (cf. Table 1). Additional funding sources, such as research grants, administrative fines (as in the case of the Spanish DPA) or other subsidies are as well often not included in the data. The figures presented in the following should thus rather be treated as proxies aimed at giving an impression of the financial and personnel situation of DPAs in Europe.

In terms of the absolute amount of financial (76.6 million euros) and human resources (888 FTEs) made available to DPAs, Germany is by far the leading nation not only in the EU but also worldwide. However, since Germany as a federal state has currently eighteen different DPAs, all German figures presented in the following comprise sums of numbers on the federal and state DPAs, hence not necessarily giving evidence of e.g. the financial and staff situation of each single German DPA.[27]

In contrast, clearly the best-financed (52 million euros) and -staffed (680 FTEs) single DPA in Europe is the Information Commissioner in the UK, followed at some distance with approximately only a third (or even less) of the staff and budget by DPAs in Poland, France, the Netherlands, Spain, Italy and Ireland. Poland and Italy represent special cases insofar as the Polish DPA (as supervisory authorities of other East European Member States) shows a huge gap between a relatively small budget (7.5 million euros) and a high number of staff (238 FTEs) probably due to the low level of wages, whereas the opposite is true for the Italian DPA that is apparently confronted with relatively high fixed costs. It also comes as no surprise that the smallest EU Member States Malta, Estonia, Latvia and Cyprus (with the exception of Luxembourg) mark the end of that ranking.

However, if DPAs' level of funding or number of staff is put in relation to the population of the respective country, the new adjusted rankings look quite different (cf. Figure 3 and Figure 4).[28]

Figure 3: Euros spent by EU Member States on DPAs per capita (2019)



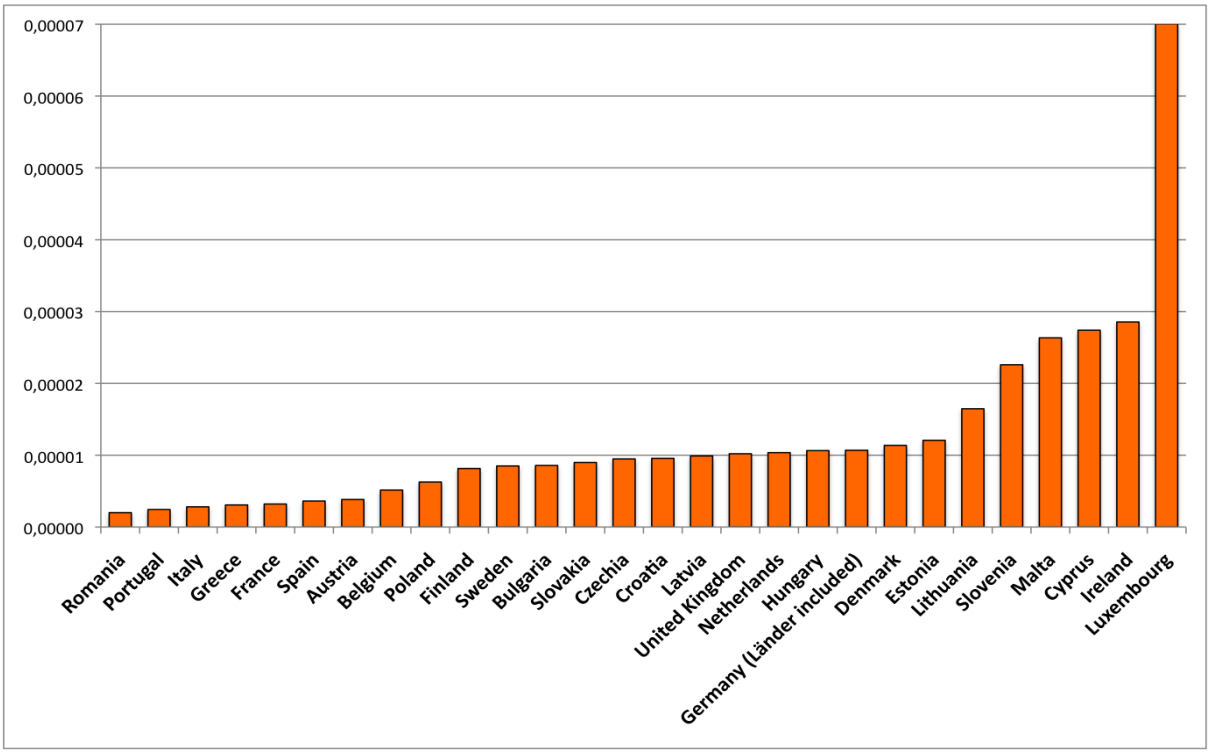
Source: own research based on data from EDPB (2020) and Eurostat (2021a).

[27] For example, whereas the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte(r) für den Datenschutz und die Informationsfreiheit* – BfDI) was provided with a budget of 23.3 million euros and a staff of 240 FTEs in 2019, the DPA of the smallest city state Bremen had only an amount of about 1 million euros and a staff of 13 FTEs at its disposal in the same year, making it much more difficult to ensure the adequate fulfilment of its regulatory tasks. For more information on budgets and staffing in German states see Schütz (2018).

[28] This analysis is particularly interesting in the light of the EU Parliament's (2013: Amendment 64, recital 92) proposal in its final report on the GDPR to take the size of the population into account when providing DPAs with adequate financial and personnel resources.

First of all, particularly Luxembourg (8.87 euros) and Ireland (3.10 euros) stand out by only recently providing their DPAs with a disproportionally high level of budget and number of staff in relation to their overall population. This is probably due the fact that a significant number of the world's leading IT companies (such as the afore-mentioned Big Five) have chosen to locate their European headquarters in one of these two countries, making it necessary to invest additional sums in order to be able to present a credible commitment for an effective supervision of data protection. Slovenia and the Netherlands (both 1.08 euros) as well as Malta and Denmark (0.97 euros) follow the two outliers with respect to the amount of euros spent on their supervisory authority as well as DPA staff per capita (with the exception of the Netherlands). On the other end, by far Romania (0.06 euros), but also Poland (0.20 euros), Bulgaria and Portugal (both 0.20 euros) spend rather little financial resources per capita on its DPA (keeping in mind the afore-mentioned bias probably due to low labour costs) as well as – in the case of Romania and Portugal – provide it with a number of staff per capita that is way below average (the latter being also the case for Italy, Greece, France, Spain and Austria).[29]

Figure 4: DPAs' number of staff per capita (2019)

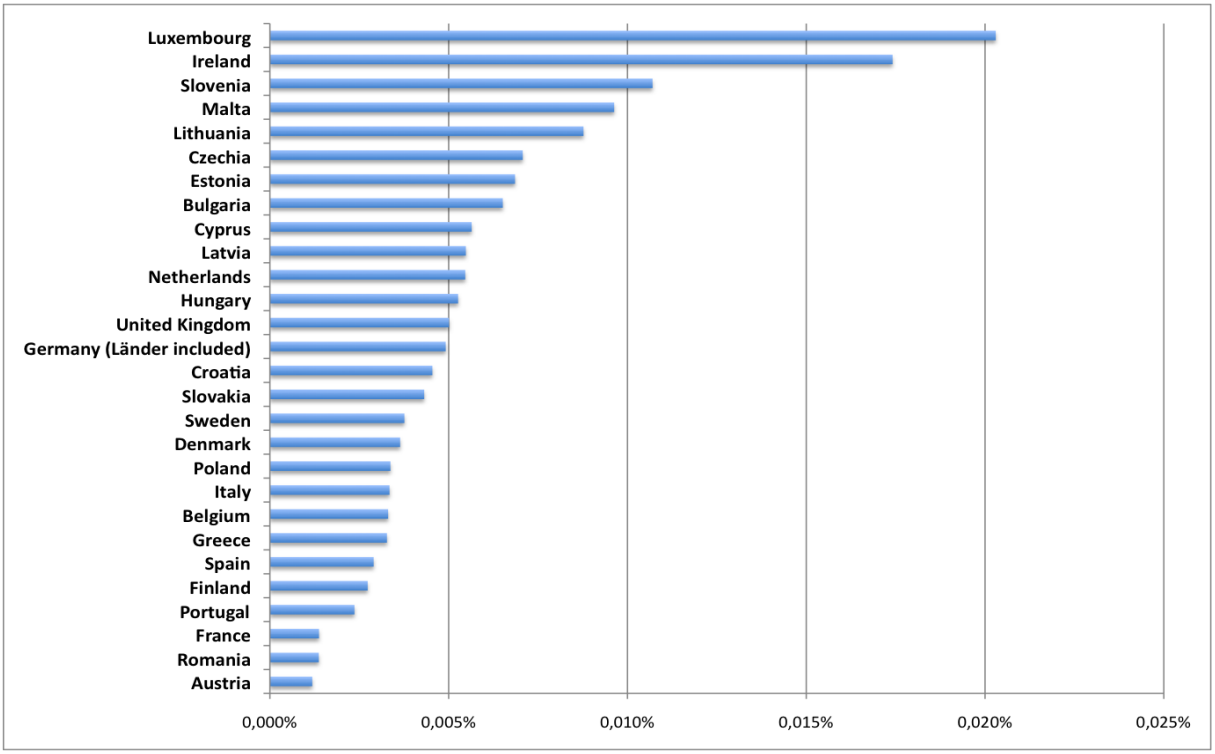


Source: own research based on data from EDPB (2020) and Eurostat (2021a).

In order to get an even more accurate picture of what EU Member States are indeed willing and able to invest in their supervisory authorities it is worthwhile to take a look at DPA budgets in relation to the overall general government expenditures of the respective country (cf. Figure 5).

[29] Nonetheless, it is important to bear in mind that less populous countries are privileged in these rankings, having to set up a more or less functioning supervisory authority with a minimum of resources and staff that can in relation to their small population already outscore the per capita figure of other, rather large countries.

Figure 5: DPA budgets in per cent of total general government expenditures of EU Member States (2019)



Source: own research based on data from EDPB (2020) and Eurostat (2021b).

Thus, Luxembourg and Ireland – as before – take top positions when it comes to financial resources spent on their DPAs in relation to the overall government expenditures, followed at some distance by Slovenia and Malta. On the contrary, supervisory authorities in Austria, Romania and France seem to receive a much smaller share of what is in general publicly spend by their governments.

Regarding the development of DPAs' financial and personnel resources in the EU (see Table 2), there is a clear trend towards a more solid funding and staffing of DPAs under the GDPR. On the one hand, again Ireland leads the way with an enormous percentage growth rate between 2013 and 2019, followed by Luxembourg, the Netherlands and Finland (possible catch-up effects included). On the other hand, DPAs in Greece, Romania, Estonia, Bulgaria and Portugal have even suffered from layoffs or smaller budgets, while still a crucial number of supervisory authorities (e.g. in Spain, France, Belgium, Czechia, Latvia and Italy) have not experienced any significant change with regards to their finances and/or number of staff within the same time period.

To sum up, the analytic results of this section show that there are a variety of EU Member States that score way below average with regards to DPAs' level of budget (Romania, Poland, Bulgaria, Portugal, Austria, Greece, France and Croatia) and number of staff per capita (Romania, Portugal, Italy, Greece, France, Spain and Austria), indicating in some cases that they do not provide their DPAs with adequate financial and/or personnel resources.[30] However, whereas to some extent Bulgaria seems to push their financial limits in the attempt to provide adequate resources, especially Austria, Romania and France appear to rather ignore DPAs in the allocation of public funds,

[30] These results correspond to a large extent with the findings of the already mentioned FRA (2010: 20) study, which identified systematic understaffing and a chronic lack of adequate financial resources of DPAs in Austria, Bulgaria, Cyprus, Greece, France, Italy, Latvia, the Netherlands, Portugal, Romania and Slovakia.

probably lacking the political will to do so (cf. Figure 5). All of this is particularly relevant in the light of Article 52 (4) GDPR. Complementing the already discussed complete independence requirement as yet another safeguard for the effective functioning of supervisory authorities, adequate financial and personnel resources of DPAs have thus become a legally mandatory requirement that could – with a view to the understaffing and –resourcing of some DPAs in the EU – become subject to judicial review of the ECJ in the near future.[31]

[31] For example, the company Brave Software Inc. filed a complaint to the EU Commission against 27 Member States for failing to adequately implement the GDPR by under-resourcing their DPAs, requesting to launch infringement procedures and refer the case to the ECJ (Taylor 2020).

Table 2: Growth of funding and staffing of DPAs in the EU from 2010 to 2019

EU-27	2010		2013		2019		2010-2013	2010-2013	2013-2019	2013-2019
	Budget	Staff	Budget	Staff	Budget	Staff	Growth budget	Growth staff	Growth budget	Growth staff
Austria	-	20	-	21.8	2.3	34	-	9.3	-	55.6
Belgium	5.9	56	6.8	53	8.2	59	15.3	-5.4	19.8	11.3
Bulgaria	1.2	67	1.4	67	1.4	60	12.8	0.0	4.8	-10.4
Croatia	-	-	0.7	28	1.2	39	-	-	65.3	39.3
Cyprus	0.2	16	0.3	17	0.5	24	9.3	6.3	95.8	41.2
Czechia	3.8	97	5.0	100	6.5	101	29.2	3.1	31.9	1.0
Denmark	2.7	35	3.0	35	5.6	66	10.7	0.0	86.0	88.6
Estonia	0.6	17	0.6	18	0.8	16	14.5	5.9	18.8	-11.1
Finland	1.5	20	1.7	20	3.5	45	10.8	0.0	104.9	125.0
France	14.7	148	16.9	178	18.5	215	15.0	20.3	9.5	20.8
Germany (Länder included)	30.5	404.8	39.1	502.1	76.6	888	28.3	24.0	95.8	76.9
Greece	2.9	39	1.8	42	2.8	33	-37.9	7.7	56.8	-21.4
Hungary	1.4	48	1.6	56	3.5	104	15.9	16.7	122.5	85.7
Ireland	1.4	22	2.0	30	15.2	140	35.3	36.4	675.1	366.7
Italy	16.5	118	23.0	122	29.1	170	39.4	3.4	26.6	39.3
Latvia	0.4	19	0.4	19	0.6	19	-0.4	0.0	69.5	0.0
Lithuania	0.5	30	0.6	30	1.5	46	1.7	0.0	166.7	53.3
Luxembourg	1.4	13	1.6	14	5.4	43	7.8	7.7	250.7	207.1
Malta	0.3	8	0.3	8	0.5	13	-3.4	0.0	71.4	62.5
Netherlands	7.7	77	7.8	74.9	18.6	179	1.7	-2.7	137.6	139.0
Poland	3.5	127	3.6	135	7.5	238	3.5	6.3	109.2	76.3
Portugal	2.0	28	2.4	18	2.2	25	17.8	-35.7	-8.7	38.9
Romania	0.9	47	0.8	44	1.1	39	-10.4	-6.4	40.9	-11.4
Slovakia	0.7	34	0.9	33	1.7	49	20.3	-2.9	97.6	48.5
Slovenia	1.5	33	1.3	32	2.2	47	-13.9	-3.0	73.7	46.9
Spain	15.4	154	13.5	158	15.2	170	-12.3	2.6	12.3	7.6
Sweden	3.3	44	4.9	41	8.8	87	49.2	-6.8	78.7	112.2
United Kingdom	23.5	351	24.7	370	52.0	680	5.1	5.4	110.2	83.8

Source: own research based on data from the Article 29 Working Party (2013, 2016) as well as from the EDPB (2020).

5.5 Tasks, powers and regulatory practices

5.5.1 Legally stipulated tasks and powers

Undoubtedly, the most significant harmonisation effect the GDPR has had was on the specification of tasks and powers of DPAs in the EU. While supervisory authorities in times of the Data Protection Directive particularly differed in their advisory, investigative and enforcement powers (see e.g. FRA 2010: 20ff.),[32] the GDPR foresees a very detailed and extended set of tasks (article 57) and powers (article 58) that each DPA in the Member States is assigned and provided with.

On the one hand, there are the rather soft regulatory assignments and powers, such as complaint handling, educating and raising awareness with the general public, consulting and influencing the private and public sector (including the power to directly address the public, parliament or government, and give advice in legislative processes).[33] On the other hand, hard regulatory instruments involve investigative powers, such as the ability to conduct audits and investigations, as well as corrective powers, including the ability to issue monetary penalties and order a data controller to inform about, publish, erase, correct or cease the processing or transfer of certain personal data. Summarising these different functions, Bennett & Raab (2006: 135) conclude that DPAs are not only expected to serve as ombudsmen, auditors, consultants, educators, policy advisors and negotiators, but they should also be able to enforce changes in behaviour, when private or public actors violate data protection legislation.

With the *de jure* harmonisation of most tasks and powers of DPAs in the EU differences in regulatory practices including the *de facto* application of these powers (analysed to some extent in the following section) come to the fore as important explanatory variables for regulatory outcomes.

5.5.2 Regulatory practices

Unfortunately, there is very little comparative empirical research on *de facto* regulatory activities and styles of supervisory authorities, such as actual consulting, auditing or enforcement practices, before and after the GDPR.

With regards to the pre-GDPR period, Bignami (2011: 442ff.) and Righettini (2011: 155ff.) are two of the very few researchers providing concrete figures (including some time series from as early as 1986 to 2009) on regulatory activities of the Italian, French, UK and a German (Hesse) DPA, such as their number of received complaints, inspections, administrative orders and sanctions. Except for the significantly higher number of complaints in Italy (3,400) and figures on administrative

[32] For example, in the pre-GDPR era only a little bit more than half of the Member States (17) obliged their public bodies to be consulted by DPAs in matters concerning the processing of personal data (FRA 2010: 27). Moreover, four supervisory authorities were found to be incapable of referring a case to the police or judicial authorities, while even a majority at that time of 14 countries did not allow their DPAs to bring a case directly before judicial authorities (ibid.: 25). Surprisingly, even more DPAs (16) were not allowed to refer relevant matters to national parliaments (ibid.: 25). With respect to investigatory competences only four countries, namely France, Malta, Romania and the UK, did not grant their DPAs the power to search premises and seize without judicial warrant. Whereas there were only a handful of DPAs that are not capable to do prior checking (i.e. to authorise processing operations likely to present specific risks) or to order the erasure and/or destruction of data if necessary (inter alia all DPAs in Germany), seven EU Member States, after all, did not provide their supervisory authorities with the power to authorize the transfer of data to third countries. Eventually the study revealed that in 2010 DPAs in eight Member States (namely Austria, Belgium, Denmark, Hungary, Lithuania, Poland, Sweden and the UK) could not at all draw on the sanctioning power of administrative fines (ibid.: 34).

[33] Additionally, somewhat in-between are new authorisation powers that enable the DPA to e.g. adopt standard contractual and standard data protection clauses, to approve draft codes of conduct, to authorise contractual clauses, to accredit certification bodies or to draft the criteria for and conduct accreditation of a body for monitoring codes of conduct.

investigations (650) and regulatory sanctions (45) in Hesse (Germany) in 2007, all of the other data largely correspond with numbers researched by the Spanish NGO *Mind Your Privacy* (2014) and its founder (Pols 2014) seven years later. According to those, the UK led the ranking when it comes to complaints (13,808 in 2013), followed by Spain (in 2011) and France (in 2012) with almost half of the number. Moreover, the Spanish DPA conducted by far most inspections/audits (with a number of 5,389 in 2011), followed by Hungary (2,929 in 2012), France (458 in 2012) and Italy (447 in 2011). With regards to the number of sanctions again the Spanish supervisory authority (with 572 sanctions in 2011) took the top position ahead of Portugal (197) and Italy (170), both in the same year. Particularly interesting to look at are moreover the comparative figures on the overall annual amount of administrative fines issued by supervisory authorities. With an overall sum of 19.5 million euros again the Spanish DPA issued clearly the highest overall amount of fines, followed by the UK Information Commissioner (3.12 million euros) and the Italian supervisory authority (1.5 million euros).[34] Surprisingly – with a view to the global level – US-American supervisory authorities, mainly the FTC, dominated by far the list of top fines worldwide for data protection violations in the pre-GDPR era, occupying rank 1 to 15, except for the UK at 10th place (cf. Table 3).[35]

Table 3: Top 15 fines for data protection violations worldwide from 1999 to 2014

Rank	Fined entity	Amount of fines and penalties	Year	Country	Privacy principles violated
1	Apple	$32.5M	2014	U.S.	Choice and Consent
2	Google	$22.5M	2012	U.S.	Collection
3	Google	$17M	2013	U.S.	Collection and Notice
4	ChoicePoint	$15M	2006	U.S.	Security
5	Hewlett-Packard	$14.5M	2006	U.S.	Collection
6	LifeLock	$12M	2010	U.S.	Accuracy, Security
7	TJ Maxx	$9.8M	2009	U.S.	Security
8	Dish Network	$6M	2009	U.S.	Choice and Consent
9	DirecTV	$5.3M	2005	U.S.	Choice and Consent
10	HSBC*	$5M	2009	UK	Security
11	US Bancorp	$5M	1999-2000	U.S.	Disclosure
12	Craftmatic	$4.4M	2007	U.S.	Choice and Consent
13	Cignet Health	$4.3M	2011	U.S.	Access

[34] However, the research and figures of *Mind Your Privacy* and Pols have several shortcomings that reduce the value and significance of deriving conclusions. First, a variety of EU countries (altogether six), such as Germany, Austria or Finland, are missing from the analysis. Second, the data was collected in different years, making a meaningful comparison much more difficult. Third, DPAs' activities are not further defined or described, resulting in simplifications and a lack of necessary differentiation (e.g. between audits and inspections) as well as uncertainty, for example, as to what is meant by sanction (does the term include administrative fines, orders and/or further criminal sanctions?).

[35] In comparison, the highest single DPA fine in Germany (and one of the highest in Europe due to no or only modest DPA fining powers) in the pre-GDPR period amounted to €1.3M levied on an insurance company (Debeka) in 2014.

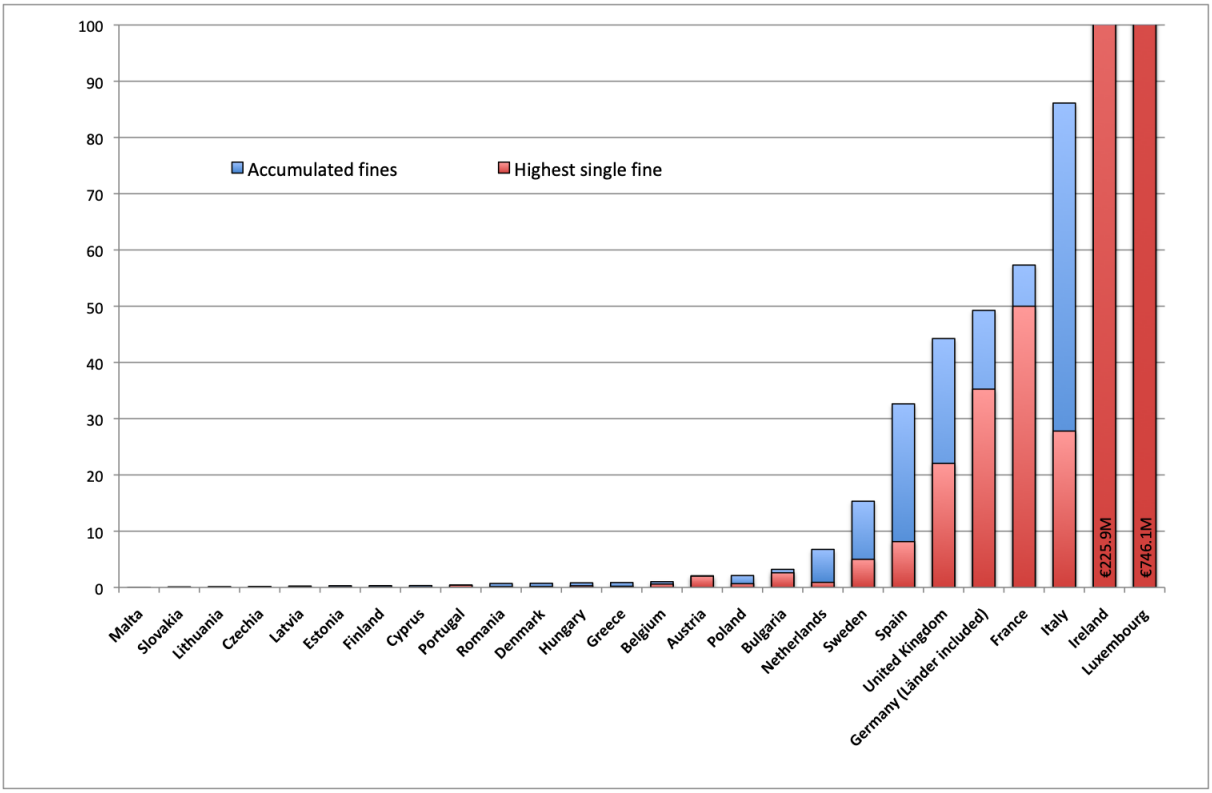
14	Barclays Bank	$3.8M	2013	U.S.	Use and Retention
15	Certegy Check Services	$3.5M	2013	U.S.	Accuracy

* not issued by the Information Commissioner's Office (the UK data protection watchdog), but by the Financial Services Authority (FSA), UK's supervisory authority for the financial service industry.
Source: Cline (2014).

While systematically aggregated, comparative data on DPA activities in the EU and globally are largely missing in the post GDPR era, there are much more attempts to get a quantitative grasp on monetary penalties under the GDPR (cf. e.g. Daigle 2020), such as provided by the international law firm CMS with its enforcement tracker website. The following diagrams are based on that data, kindly provided by CMS.[36]

Figure 6 shows the accumulated amount of fines as well as the highest single fine under the GDPR (both in million euros), issued by DPAs in EU Member States and in the UK from the beginning of the GDPR's implementation in May 2018 to mid September 2021 and sorted by the accumulated amount of issued fines in ascending order.

Figure 6: DPA fines (in €M) under the GDPR in the EU and UK from 2018 to 2021 (17th September)



The sample does not include the EU Member States Croatia and Slovenia. Source: own research based on data from CMS (2021).

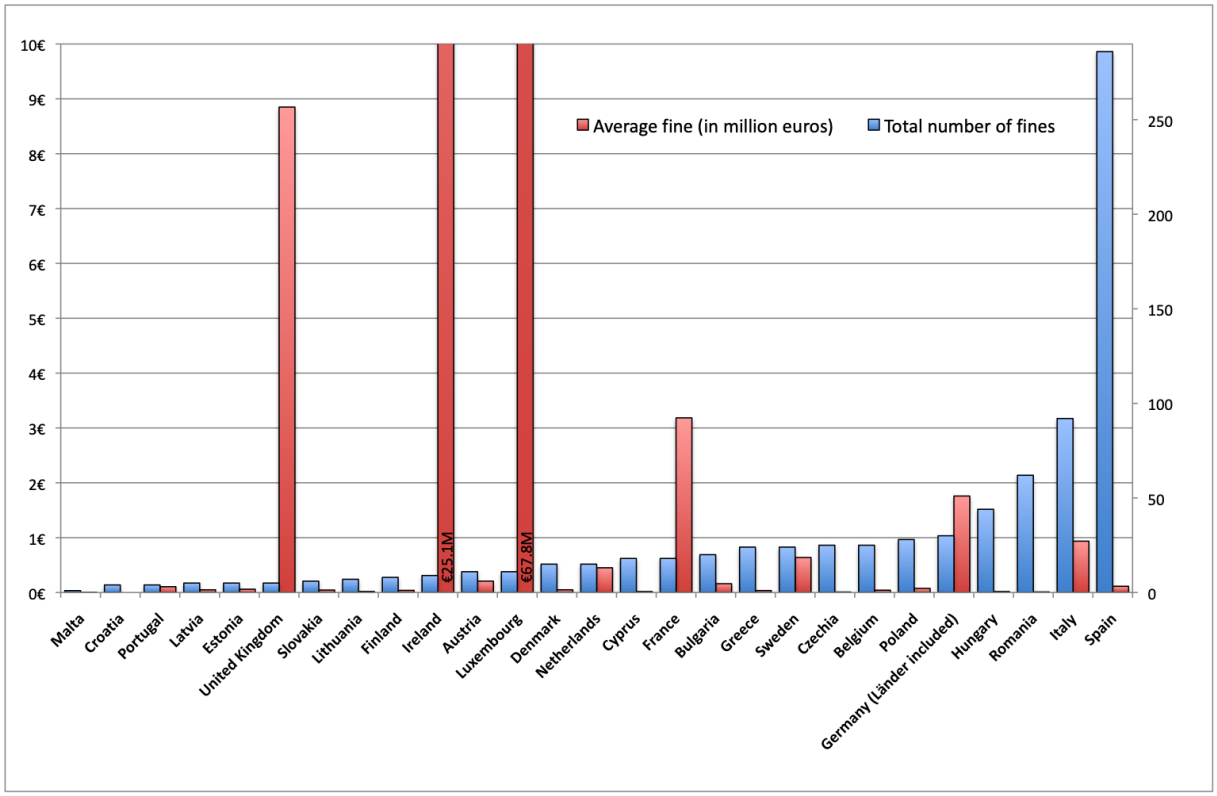
With respect to the highest overall amount of issued fines, only recently Luxembourg (€746.1M) and Ireland (€225.9M) have taken over the lead, outpacing the Italian DPA (86.2 €M), France

[36] It is important to keep in mind that the CMS data only comprise monetary penalties issued under the GDPR, not including fines for violations of data protection rules exclusively stipulated under national legislation, e.g. with regards to cookies (see table 4) or employee data, as well as annulled by the judiciary.

(€57.3M), Germany (€49.3M) – the German states are included – and the UK (€44.3M). Particularly in Luxembourg (€746M against Amazon) and Ireland (€225M against WhatsApp – though forced by the EDPB), but also in the rest of these countries a record-braking single fine (France: €50M against Google Inc.; Germany (Hamburg): €35.3M against H&M; Italy: €27.8M against Telcom Italia (TIM); UK: €22.1M against British Airways) makes up a significant part of the overall accumulated amount. DPAs in Spain (€32.6M) and Sweden (€15.3M) have so far issued monetary penalties in the low double-digit million range, whereas the Netherlands, Bulgaria, Poland, Austria and Belgium comprise a group that fined data controllers only an overall amount from a few to one million euros.[37] Supervisory authorities in the rest of the EU Member States did not make use of significant monetary penalties, so far.

In terms of the total number of fines issued (cf. Figure 7), Spain (286) leads by far the ranking, followed by Italy (92), Romania (62), Hungary (44) and Germany (30) – again Länder included. Taking a look at the average of monetary penalties issued, it becomes apparent that a large group of predominantly Eastern European countries (see also Daigle 2020: 10), i.e. Malta, Czechia, Romania, Cyprus, Slovakia, Hungary, Lithuania, Greece, Finland, Belgium, Slovakia, Latvia, Denmark, Estonia and Poland, does not yet make use of deterrent monetary penalties (average fine below €100k). In all other EU Member States average fines have significantly increased in comparison to the pre-GDPR period, ranging from €106k in Portugal and €114k in Spain to €1.8M in Germany (Länder included), €3.2M in France, €8.9M in the UK, €25.1M in Ireland and €67.8M in Luxembourg, of course sometimes biased by a very high single fine.

Figure 7: Total number and average of DPA fines under the GDPR in the EU and UK from 2018 to 2021 (17th September)



The sample does not include the EU Member State Slovenia. Source: own research based on data from CMS (2021).

[37] The bias of a major fine influencing the overall amount of fines is particularly strong in Luxembourg, Ireland, France and Bulgaria.

However, it is again worthwhile to look at the global level (see Table 4), where the United States have pushed financial punishments for data protection violations to yet another level in the post GDPR era. That way, Facebook had to pay a record-braking fine of $5bn for its severe data protection infringements surrounding the initially mentioned *Cambridge Analytica* scandal.[38] And also Equifax, a US-American consumer credit reporting agency, was forced to pay around $650M due to a massive data breach. With latest monetary penalties from DPAs in Luxembourg and Ireland more rigorous fining practices in the EU gain momentum, beginning to match those in the U.S.. And even more important, the development process of the latest fine against WhatsApp, in which the EDPB was able to force the responsible lead authority in Ireland to substantially increase the fine from initially €30-50 to €225 million, has clearly shown that GDPR's consistency mechanism is starting to work in practice, mitigating the risk of single national supervisory authorities undermining EU data protection standards.

Table 4: Top-15 fines worldwide related to data protection violations after GDPR (September 2021)

Rank	Fined entity	Amount of fines and penalties	Year	Country	Status
1	Facebook, Inc.	$5bn	2019	U.S.	settled
2	Amazon Europe Core S.à r.l.	€746M	2021	Luxembourg	issued
3	Equifax Inc.	$650M	2019	U.S.	settled
4	WhatsApp Ireland Limited	€225M	2021	Ireland	issued
5	Google LLC, YouTube LLC	£170M	2019	U.S.	settled
6	Uber Technologies, Inc.	$148M	2018	U.S.	settled
7	Google LLC, Google Ireland Limited	€100M	2020	France*	issued
8	Blue Global Media	$104M	2017	U.S.	suspended due to bankruptcy
9	Facebook, Inc.	$100M	2019	U.S.**	settled
10	Google LLC	€50M	2019	France	settled after judicial review
11	H&M	€35M	2020	Germany	settled
12	Amazon Europe Core S.à r.l.	€35M	2020	France*	issued
13	Yahoo!	$35M	2018	U.S.**	settled
14	Telecom Italia (TIM)	€27.8M	2020	Italy	issued
15	British Airways	€22.1M	2020	UK	settled

* not issued on the basis of the GDPR, but under national French cookie rules.
** not issued by the Federal Trade Commission, but by the Securities and Exchange Commission (SEC), the US-American supervisory authority for the financial service industry.

[38] According to Facebook shareholders, the record-braking fine was mostly accomplished due to the fact that the company's board allowed to overpay on its fine in order to shield CEO Mark Zuckerberg from personal liability (Nylen 2021).

Source: own research.

It is crucial to note here that most of the US-American monetary penalties are part of a directly applicable settlement with the infringing party, whereas fines issued by DPAs in Europe are normally not part of a deal and thus become increasingly subject to judicial review or DPAs' anticipatory obedience in expecting judicial review.[39] For example, while the Highest Administrative Court in France upheld the €50M-fine against Google in 2020, German courts substantially slashed the monetary penalty against 1&1 (a German telecommunications provider) by 90 per cent (from €9.6M to just €900,000) or even annulled the fine of €14.5M of the Berlin DPA against German property company Deutsche Wohnen. In Austria, the record-braking fine of €18M against the Austrian Post was also overturned by the Federal Administrative Court because of infringements of procedural requirements and other more peculiar cases involve the significant reduction of fines against British Airways (from £184M to £20M) and Marriot International (from £99M to £14.4M) by the ICO, apparently due to the COVID-19 pandemic and associated economic crisis of these companies.

Briefly summarised, comparative data on regulatory actions by DPAs in the EU and globally are largely missing. With respect to one out of many enforcement tools, namely issuing monetary penalties, there is more and more systematically aggregated, quantitative data. In the U.S., supervisory authorities clearly make use of *de facto* deterring financial sanctions. Whereas a small group of DPAs (especially in Luxembourg, France and Ireland, but also Germany, Italy and the UK) is trying to impose more rigorous monetary penalties (yet often still on a different scale as in the U.S.), supervisory authorities of most of the other Member States have not yet exercised their newly acquired fining powers for significant monetary penalties.

One of the key problems is, however, that some EU Member States seem to have adopted the role to function as data protection (as well as tax) havens, attracting most of the leading IT industry players. Despite recent efforts in massively increasing resources (cf. section 5.4) as well as establishing more rigorous fining practices, these DPAs are overrun by cross-border complaints not being able to react in a timely manner. This is particularly the case for Ireland, where – even after the enormous fine against WhatsApp – 98 per cent of major cross-border complaints remain unresolved (Irish Council for Civil Liberties 2021:3). That way – even if well-intentioned and pushed by EDPB decisions – the Irish DPA becomes a crucial bottleneck, significantly slowing down an effective regulation EU-wide.

[39] As opposed to the pre-GDPR period, the trend of challenging DPA fines in court will manifest itself in Europe since it seems worthwhile for fined data controllers to at least attempt to get a reduction in their financial sanction.

6 Concluding Remarks

What we have learned so far is that the topic of data protection authorities – despite its regulatory and societal relevance – is still massively under-researched, particularly from a social science perspective, lacking systematically aggregated qualitative as well as quantitative data.

There are more than 130 privacy and data protection authorities worldwide with a very large part of them (about 60) located in Europe. With the enactment of the GDPR in 2018 the EU set new standards in data protection worldwide. The GDPR perpetuates the process of policy convergence as well as significant improvements in the legal set up of supervisory authorities for an effective regulation, such as DPAs' independence, resources, tasks and powers.

With respect to the complete independence requirement, particularly the absence of rules addressing the highly significant selection processes of DPA decision-makers prior to the actual appointment as well as the obligatory involvement of a branch of government (other than the executive), such as parliament, in nomination and appointment procedures remains problematic.

While the GDPR clearly foresees DPAs to be provided with adequate human, technical and financial resources (including appropriate premises and infrastructure), the reality of many DPAs in the EU is quite different, posing enormous challenges in the attempt to fulfil the wide range of different functions. Regarding regulatory tasks and powers of DPAs, the GDPR heralds indeed a new era of *de facto* enforceability of data protection law. Before that, many DPAs in Europe suffered from a lack of investigative and corrective powers (including authorisation, ordering and fining powers). However, with a view to regulatory and particularly fining practices, the majority of supervisory authorities in the EU acts so far rather reserved, while other struggle with the sheer number of cases to be assessed or the actual execution of their monetary penalties in court.

In that respect, it is crucial to bear in mind that the debate on effective means of enforcement must not be restricted to easily quantifiable and publicly presentable monetary penalties, which only comprise one tool out of many and are often exclusively directed towards private-sector data controllers. Furthermore, the long-term effectiveness of financial sanctions can be called into question (cf. Serwin 2011: 856), since even the largest corporate fines in world history in cases of environmental pollution (20.8bn against BP for the Deepwater Horizon oil spill in 2010) and financial fraud ($16.7bn against Bank of America for its role in the subprime loan crisis) have not led to a complete reorientation of these companies, significantly reducing the risk of large corporations harming individuals and/or society at large. Instead, a mixture of soft and hard regulatory tools seems to be most promising, including educating and raising awareness with the general public as well as organisations (e.g. through mandatory full-time data protection officers), but also ordering the immediate cessation of the processing or transfer of personal data, and as a last resort ensuring personal liability and/or criminal prosecutions against relevant decision-makers (e.g. single chief executive officers). Eventually, it is worthwhile to take a closer look in that context at the interplay of data protection and competition law. New and more aggressive regulatory approaches in antitrust politics in the EU but also in the US (cf. e.g. Khan 2017), including discussions on forced break-ups, could help to put additional pressure on Big Tech to really change business practices also with regards to data protection.

Drawing on theoretical and methodological approaches of research on IRAs has proven to be quite helpful, though the analytical scope has to be broaden in order to be able to explain regulatory outputs of DPAs. Due to the increasing convergence of data protection legislation (at least with regards to liberal democracies worldwide), also spawned by GDPR's external effects to function as the new gold standard, future research on DPAs should not so much concentrate on *de*

jure features but rather *de facto* practices. The presented empirical findings show considerable differences in regulatory practices of DPAs in Europe (at least with regards to fining practices), contradicting to a certain extent Bignami's (2011) observation of converging regulatory styles for the time being. Also litigation plays an increasingly relevant role mostly due to more significant fines and associated incentives to challenge them in court. But GDPR's establishment of the right to compensation and liability (article 82) in cases of data protection violations, coupled with new opportunities e.g. for NGOs to file class action suits, will also result in more judicial decisions on claims of compensation.[40]

The lowest common denominator in the understanding of DPAs' regulatory role in society is certainly the clarification of the ECJ (2010) that DPAs shall act as "the guardian of those fundamental rights and freedoms" with respect to the processing of personal data (ibid.: recital 23), striving for a fair balance between observance of the fundamental right to private life and the interests requiring free movement of personal data (ibid.: recital 24). The GDPR provides an adequate legal framework for the fulfilment of these tasks. However, it is up to DPA decision-makers to live up to that role with all necessary means the GDPR provides them with, not only individually at the national, but also together at the European level or even worldwide. Further research on DPAs should critically scrutinise and accompany those developments.

[40] However, actual payments of compensation in privacy/data protection litigation in the EU remain low (to non-existent), particularly compared with those in the U.S., where companies are regularly forced to make significant compensation payments, e.g. only recently Facebook had to pay $650 million to 1.6 million users due to the illegal processing of facial recognition data.

7 List of Figures

8 List of Tables

9 References

Article 29 Working Party (2013): *Fourteenth Annual Report of the Article 29 Working Party on Data Protection. Covering the year 2010*. Article 29 Working Party, Dictorate-General for Justice, European Commission. Available here.

Article 29 Working Party (2016): *Seventeenth Annual Report of the Article 29 Working Party on Data Protection. Covering the year 2013*. Article 29 Working Party, Dictorate-General for Justice and Consumers, European Commission. Available here.

AIE & CLD (2017): *Global Right to Information Rating. Country Data*. Programme founded by Access Info Europe (AIE) and the Centre for Law and Democracy (CLD). Available here.

Banisar, D. & S. Davies (1999–2000): 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments'. In: John Marshall Journal of Computer and Information Law 18, pages 1–112. Available here.

Banisar, D. (2006): *Freedom of Information Around the World 2006. A Global Survey of Access to Government Information Laws*. Global Campaign for Free Expression. London: Privacy International/ARTICLE 19. Available here.

Barnard-Wills, D. (2017): 'The technology foresight activities of European Union data protection authorities'. In: *Technological Forecasting and Social Change* 116, pages 142–150.

Bennett, C. J. (1992): *Regulating privacy: data protection and public policy in Europe and the United States*. Ithaca: Cornell University press.

Bennett, C. J. & C. D. Raab (2006): *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd. Cambridge (Mass.) and London: MIT Press.

Bennett, C. and C. Raab (2020). "Revisiting the governance of privacy: Contemporary policy instruments in a global perspective." Regulation & Governance 14 (3): 447-64.

Bignami F. (2011). "Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy." American Journal of Comparative Law 59 (2): 411-61. Available here.

Bieker F. (2017). "Enforcing Data Protection Law – The Role of the Supervisory Authorities in Theory and Practice" in Lehmann, A., Whitehouse, D., Fischer-Hübner, S., Fritsch, L. and Raab, C. (eds.) Privacy and Identity Management: Facing Up to Next Steps. (11th IFIP WG 9.2, 9.5, 96/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School) Karlstad, Sweden, August 21-26, 2016, Revised Selected Papers, Springer: 125-139. Available here.

Bröhmer, J., C. Hill, M. Spitzkatz & S. Wahiduddin (ed.) (2012): *60 Years German Basic Law: The German Constitution and its Court. Landmark Decisions of the Federal Constitutional Court of Germany in the Area of Fundamental Rights*. 2nd edition. Konrad-Adenauer-Stiftung e.V. Ampang (Malaysia): The Malaysian Current Law Journal Sdn Bhd. Available here.

Busch, A. (2010): *Coping with innovation: The political regulation of personal information in comparative perspective: Full Research Report ESRC End of Award Report*. RES-062-23-0536-A. Swindon: ESRC.

Busch, A. (2011): 'The regulation of privacy'. In: *Handbook on the politics of regulation*. Edited by D. Levi-Faur. Cheltenham, UK; Northampton, MA, USA: Edward Elgar.

Busch, A. (2013): 'The regulation of transborder data traffic: Disputes across the Atlantic'. In: *Security and Human Rights* 23.4, pages 313–330.

Busch, A. (2015): 'Internet and Privacy'. In: *International Encyclopedia of the Social & Behavioral Sciences*. Edited by James D. Wright. 2nd edition. Volume 12. Oxford: Elsevier, pages 593–599.

BVerfG (1983): *Volkszählungsurteil (Census decision). Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden*. Available here (for an English translation see Bröhmer et al. (p. 150ff.) in this bibliography).

BVerfG (1984): *Urteil vom 20.06.1984 zur Überwachung des Brief- und Telefonverkehrs - 1 BvR 1494/78*. Available here.

BVerfG (1987): *Beschluss vom 24.09.1987 – 1 BvR 970/87*. Available here.

Cline, J. (2014): 'U.S. takes the gold in doling out privacy fines'. In: *Computerworld*. Available here.

Daigle B. and Khan M. (2020). "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities." Journal of International Commerce and Economics, May 2020.

De Hert, P., Kloza, D. und Makowski, P. (ed.) (2015): Enforcing Privacy: Lessons from Current Implementations and Perspectives for the Future. Warszawa: Wydawnictwo Sejmowe. Available here.

ECJ (2010): *Judgment of the Court (Grand Chamber) of 9 March 2010. European Commission v Federal Republic of Germany. Failure of a Member State to fulfil obligations — Directive 95/46/EC — Protection of individuals with regard to the processing of personal data and the free movement of such data — Article 28(1) — National supervisory authorities — Independence — Administrative scrutiny of those authorities*. Case C-518/07. Available here.

ECJ (2012): *Judgment of the Court (Grand Chamber) of 16 October 2012. European Commission v Republic of Austria. Failure of a Member State to fulfil obligations — Directive 95/46/EC — Processing of personal data and free movement of such data — Protection of natural persons — Article 28(1) — National supervisory authority — Independence — Supervisory authority and the Federal Chancellery — Personal and organisational links*. Case C-614/10. Available here.

ECJ (2014): *Judgment of the Court (Grand Chamber) of 8 April 2014 — European Commission v Hungary. Failure of a Member State to fulfil obligations — Directive 95/46/EC — Protection of individuals with regard to the processing of personal data and the free movement of such data — Article 28(1) — National supervisory authorities — Independence — National legislation prematurely bringing to an end the term served by the supervisory authority — Creation of a new supervisory authority and appointment of another person as head of that authority.* Case C-288/12. Available here.

ECJ (2021): Judgment of the Court (Grand Chamber) of 15 June 2021 (request for a preliminary ruling from the Hof van beroep te Brussel – Belgium) – Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA v Gegevensbeschermingsautoriteit. C-645/19. Available here.

EU Commission (2003): *REPORT FROM THE COMMISSION - First report on the implementation of the Data Protection Directive (95/46/EC)*. European Commission. Available here.

EU Commission. (2020). Communication from the Commission to the European Parliament and the Council – Data protection as pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the GDPR." COM(2020) 264 final. Available here.

EU Parliament (2013): ****I Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 - 0025/2012 – 2012/0011 (COD))*. Edited by Rapporteur: Jan Philipp Albrecht. Available here.

EDPB (2020): *Contribution of the EDPB to the evaluation of the GDPR under article 97*. European Data Protection Board. Available here.

EDPS (2017): *European Conferences*. Available here.

Eurostat (2021a): *Population on 1 January – persons*. Online data code: TPS00001. Available here.

Eurostat (2021b): *Total general government expenditure - % of GDP*. Online data code: TEC00023. Available here.

Finn, R., D. Wright, A. Donavan, L. Jacques & P. De Hert (2014): *Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations*. Final Report (commissioned by the Directorate-General Enterprise and Industries). Brussels: EU Commission. Available here.

Flaherty, D. H. (1989): *Protecting privacy in surveillance societies: The federal Republic of Germany, Sweden, France, Canada, and United States*. Chapel Hilland; London: University of North Carolina Press.

FRA (2009): *Thematic legal study on data protection in the European Union: the role of national data protection authorities*. Country reports (EU-27); updated 2014. Vienna. Available here.

FRA (2010): *Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*. Luxembourg: European Union Agency for Fundamental Rights (FRA). Available here.

Garstka, H. (2008): 'Der Mensch als Datenzuträger. Was Sie schon immer über Ihren Nachbarn wissen wollten'. In: *Wissen als Begleiter!? Das Individuum als lebenslanger Lerner*. Edited by Rita Herwig, Jens Uhlig & Johannes Küstner. Münster: LIT Verlag, pages 133–138.

Gilardi, F. & M. Maggetti (2011): 'The Independence of Regulatory Authorities'. In: *Handbook on the Politics of Regulation*. Edited by D. Levi-Faur. Cheltenham (UK); Northampton, MA (USA): Edward Elgar Publishing, pages 201– 214.

GPA (2019): *Website of the Global Privacy Assembly (GPA)*. Available here.

Greenleaf, G. (2012a): 'Independence of data privacy authorities (Part I): International standards'. In: *Computer Law & Security Review* 28.1, pages 3–13.

Greenleaf, G. (2012b): 'Independence of data privacy authorities (Part II): Asia-Pacific experience'. In: *Computer Law & Security Review* 28.2, pages 121–129.

González-Fuster, G., P. De Hert & D. Kloza (2015): *Deliverable 1.1: State-of-the-art report on teaching privacy and personal data protection at schools in the European Union*. Workstream 1: Preparing the two-day seminar for teachers (Call: JUST/2013/FRC/AG Agreement number: JUST/2013/FRAC/AG/6132). ARCADES (Introducing dAta pRoteCtion and privacy issuEs at schoolS in the European Union) project. Available here.

Gutwirth, S. (2002): *Privacy and the information age*. Lanham/Boulder/New York/Oxford: Rowman & Littlefield Publishers.

Hijmans, H. (2016): 'The European Union as a constitutional guardian of internet privacy and data protection'. PhD thesis. Faculty of Law (Amsterdam). Available here.

Hustinx, P. (2009): 'The Role of Data Protection Authorities'. In: *Reinventing Data Protection?* Edited by S. Gutwirth, Y. Poullet, P. Hert, C. Terwangne & S. Nouwt. Dodrecht: Springer, pages 131–137.

IAPP (2011): *Data Protection Authorities 2011 Global Survey*. International Association of Privacy Professionals (IAPP).

Irish Council for Civil Liberties (2021): Europe's enforcement paralysis. ICCL's 2021 report on the enforcement capacity of data protection authorities. Available here.

Jordana, J & D. Levi-Faur (2004): 'The politics of regulation in the age of governance'. In: *The Politics of Regulation. Institutions and Regulatory Reforms for the Age of Governance*. Edited by J. Jordana & D. Levi-Faur. Cheltenham (UK); Northampton, MA (USA): Edward Elgar Publishing, pages 1–28.

Jóri, A. (2013): 'The end of independent data protection supervision in Hungary – a case study'. English. In: *European data protection coming of age*. Edited by Serge Gutwirth, Ronald Leenes, Paul De Hert & Yves Poullet. Dordrecht; New York: Springer.

Karaboga, Murat (forthcoming): *Die Entstehung der Datenschutz-Grundverordnung*.

Khan, Lina M. (2017): 'Amazon's Antitrust Paradox'. In: Yale Law Journal 126.3, pages 564–907. Available here.

Kloza, D. & A. Galetta (2015): "Towards effcient cooperation between supervisory authorities in the area of data privacy law". In: *Enforcing Privacy: Lessons from current Implementations and Perspectives for the Future*. Edited by P. De Hert, D. Kloza & P. Makowski. Warszawa: Wydawnictwo Sejmowe, pages 77– 108. Available here.

Korff, D. (1998): *Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons*. European Commission. Available here.

Korff, D. (2002): *EC Study on Implementation of Data Protection Directive 95/46/EC*. Study Contract ETD/2001/B5-3001/A/49. European Commission. Available here.

Korff, D., I. Brown, P. Blume, G. Greenleaf, C. Hoofnagle, L. Mitrou, F. Pospisil, H. Svatosova, M. Tichy, R. Anderson, C. Bowden, K. Nyman-Metcalf & P. Whitehouse (2010): *Comparative study on different approaches to new privacy challenges in particular in the light of technological developments*. Final report Contract Nr: JLS/2008/C4/011 – 30-CE-0219363/00-28. European Commission. Directorate-General Justice, Freedom and Security. Available here.

Kress C., R. van Eijk & G. Zanfir-Fortuna. (2020). "New Decade, New Priorities: a summary of twelve European data protection authorities' strategic and operational plans for 2020 and beyond." Future of Privacy Forum. Available here.

Mayer-Schönberger, V. (1998): 'Generational development of data protection in Europe'. In: *Technology and Privacy: The New Landscape*. Edited by Philip E. Agre & Marc Rotenberg. Cambridge, MA, USA: MIT Press, pages 219–241.

Mind Your Privacy (2014): *European Privacy Overview (1890-2014) Infography. Privacy Enforcers in the EU: a Comparative Study of National Data Protection Agencies' (DPAs) Annual Reports (Latest Available)*. Mind Your Privacy (consultancy). Available here.

Newman, A. L. (2008): 'Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive'. In: *International Organization* 62.1, pages 103–30.

Nylen, L (2021): Facebook paid billions extra to the FTC to spare Zuckerberg in data suit, shareholders allege. In: *Politico* (21.09.2021). Available here.

Pols, A. (2014): 'Spain is responsible for 80% of European Data Protection fines'. In: *Privacy Laws & Business* 128, pages 22–24.

Quintyn, M. (2009): 'Independent agencies: more than a cheap copy of independent central banks?' In: *Constitutional Political Economy* 20.3-4, pages 267–295.

Raab, C. D. (2011): 'Networks for Regulation: Privacy Commissioners in a Changing World'. In: *Journal of Comparative Policy Analysis: Research and Practice* 13.2, pages 195–213.

Raab, C. D. & I. Szekely (2017): 'Data protection authorities and information technology'. In: *Computer Law & Security Review* 33, pages 421–433.

Regan, P. M. (2009): *Legislating privacy: technology, social values, and public policy.* Chapel Hill, NC (USA): The University of North Carolina Press.

Richardson, J. J., G. Gustafsson & G. Jordan (1982): 'The Concept of Policy Style'. In: *Policy styles in Western Europe*. Edited by J. J. Richardson. Allen & Unwin, pages 1–16.

Righettini, M. S. (2011): 'Institutionalization, Leadership, and Regulative Policy Style: A France/Italy Comparison of Data Protection Authorities'. In: *Journal of Comparative Policy Analysis: Research and Practice* 13.2, pages 143–164.

Roßnagel, A. (2009): 'Die Zukunft informationeller Selbstbestimmung: Datenschutz ins Grundgesetz und Modernisierung des Datenschutzkonzepts'. In: Verfassungsrecht und gesellschaftliche Realität. Dokumentation: Kongress „60 Jahre Grundgesetz: Fundamente der Freiheit stärken" der Bundestagsfraktion Bündnis 90/Die Grünen am 13./14. März 2009 in Berlin. Edited by Kritische Justiz. Baden-Baden: Nomos Verlag, pages 99–119.

Ryan, J. (2020): Europe's governments are failing the GDPR. Brave's 2020 report on the enforcement capacity of data protection authorities. Brave Software Inc.. Available here.

Schütz, P. (2012a): 'The Set Up of Data Protection Authorities as a New Regulatory Approach'. In: *European Data Protection: In Good Health?* Edited by S. Gutwirth, R. Leenes, P. De Hert & Y. Poullet. Dordrecht: Springer, pages 125–142.

Schütz, P. (2012b): 'Comparing formal independence of data protection authorities in selected EU Member States'. Conference Paper presented at the 4th Biennial ECPR Standing Group for Regulatory Governance Conference 2012, Exeter, UK. Available here.

Schütz, P. & M. Karaboga (2015): *Akteure, Interessenlagen und Regulierungspraxis im Datenschutz: Eine politikwissenschaftliche Perspektive*. Arbeitspapier. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Available here.

Schütz P. (2018): Zum Leben zu wenig, zum Sterben zu viel? Die finanzielle und personelle Ausstattung deutscher Datenschutzbehörden im Vergleich. In: Roßnagel, A.; Friedewald, M.; Hansen, M. (ed.): Die Fortentwicklung des Datenschutzes. DuD-Fachbeiträge. Wiesbaden: Springer Vieweg, pages 251-268.

Schütz, P. (forthcoming): Data Protection Authorities in Comparative Perspective. The Cases of the United Kingdom and the Federal Republic of Germany (working title).

Serwin, A. (2011): 'The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices'. In: *San Diego Law Review* 48, pages 809–856. Available here.

Simitis, S. (2014): 'Einleitung: Geschichte - Ziele - Prinzipien'. In: Bundesdatenschutzgesetz (Nomos Kommentar). Edited by Simitis, S.. 8th. Baden-Baden: Nomos, pages 81–196.

Simitis, S.; Hornung, G.; Spiecker gen. Döhmann, I.; Schiedermair, S.; Albrecht, J.-P.; (2019): Einleitung. In: Datenschutzrecht. DSGVO mit BDSG (Nomos Kommentar). Edited by Simitis, S.; Hornung, G.; Spiecker gen. Döhmann, I.. 1st. Baden-Baden: Nomos, pages 158-240.

Sivan-Sevilla, I. (forthcoming): 'Europeanization of Policy Implementation? A qualitative comparative analysis (QCA) of Data Protection Authorities' enforcement styles post-GDPR', Journal of European Public Policy.

Stewart, B. (2004): 'A comparative survey of data protection authorities - Part 1: Form and structure'. In: *Privacy Law and Policy Reporter 46* 11.2. Available here.

Taylor, C. (2020): ‚GDPR at risk of failing due to underfunding of regulators, study finds. Complaint filed over failure of EU member states to properly resource regulators', Irish Times (27.04.2020), Available here.

Vranaki, A. (2016): 'Cloud investigations by European data protection authorities: An empirical account'. In: *Research Handbook on Electronic Commerce Law*. Edited by John A. Rothchild. Cheltenham (UK); Northampton, MA (USA): Edward Elgar Publishing, pages 518–541.

Wippermann, G. (1994): 'Zur Frage der Unabhängigkeit der Datenschutzbeauftragten'. In: *Die Öffentliche Verwaltung (DÖV)* 47.22, pages 929–940.

Wright, D. & P. De Hert (ed.) (2016): *Enforcing Privacy*. Law, Governance and Technology Series 25. Cham ZG (Switzerland): Springer International Publishing.

Zuboff, S. (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

PROJEKTPARTNER

Fraunhofer

Natur
Technik
Kultur
Gesellschaft
UNIKASSEL
VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung