Journal of Cybersecurity, 2024, pp. 1–18

doi: tbc
Accepted Manuscript
Paper

PAPER

GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved?

Gerard Buckley[1,*] Tristan Caulfield[1] and Ingolf Becker[2]

[1]Department of Computer Science, UCL, Gower Street, London, UK and [2]Department of Security & Crime Science, UCL, Gower Street, London, UK
[*]Corresponding author. gerard.buckley.18@ucl.ac.uk
Received on 18 January 2024; revised on 28 May 2024; accepted on 25 July 2024

Abstract

Data protection regulations like the GDPR are increasingly important in securing individuals' privacy as society goes digital. The success of any regulation, however good, ultimately depends on how well it is executed. Existing literature fails to answer what good execution means in this context. We research what practitioners think are the objectives of data protection regulators and how they evaluate their effectiveness. We explore novel ways to assess regulator performance more systematically. We surveyed 70 Chief Information Security Officers (CISO) and conducted 23 structured interviews. The interviewees included informed business executives, lawyers, digital rights activists and 4 national regulators. We supplement it with an analysis of diverse enforcement databases. Our findings indicate a mismatch between the broad presumed objectives attributed to regulators and the narrow criteria used to judge them in practice. Perception of the regulator's effectiveness is subjective, sanctions-focused and influenced by one's role and responsibilities. Moreover, the independence of regulators, intentionally designed to insulate them from daily politics, raises serious questions of accountability. We examine the historical, cultural and organisational motivations behind the current byzantine complexity of the GDPR regime. Lastly, we contribute a series of key performance indicators and make structural suggestions around centralised and standardised reporting of cases to deliver improved learning, legitimacy, transparency and comparability. We believe our findings have important implications for the future development of regulator assessment and accountability in Europe and in the growing number of GDPR-like regimes outside Europe.

Key words: GDPR, data protection, privacy, regulation, regulator effectiveness

1. Introduction

Regulation is critical to the working of society. Just as important is how regulators implement it. As society becomes increasingly digitised, privacy regulation and the effectiveness of the regulators executing it will become more pressing.

The European Union (EU) General Data Protection Regulation (GDPR) is regarded as the strongest privacy and security law in the world (even though the word 'privacy' never appears in its text). Although widely studied as a benchmark and blueprint by policymakers when considering a similar regulation beyond the EU, rather less attention has been paid to the actions of the GDPR regulators. Such regulators, known as Data Protection Authorities (DPA), operationalise it in the 27 EU member states, the 3 European Free Trade Association (EFTA) states and the United Kingdom (UK).

Performance measurement of regulators is challenging due to the indirect nature of their involvement. Their desired outcomes, such as consumer or environmental protection, are not theirs to deliver but are realised by the organisations they oversee. Many external factors can be beyond regulators' control, and outcomes often do not become evident for several years. Assessing the performance of GDPR regulators, where the very concept of privacy is contestable, brings added complexity. Differences in national laws, administrative processes and historical engagement with industry mean DPAs come to GDPR from different starting points. Differences in human and financial resources mean that DPAs have varying organisational capacities. And differences in political influences mean DPAs' self-confidence and understanding of their role may differ significantly between European countries. All these factors contribute to the noticeably different implementations of the GDPR. Metrics, where available, are often defined differently and make comparative analysis problematic. Such complexity may explain the surprising scarcity of prior research.

Nonetheless, if we are to hold data protection regulators accountable and to learn best practices, an assessment framework, however imperfect, is required to score their effectiveness individually and relative to their peers. We investigate the perspectives of those stakeholders closely involved in the regulatory process, such as CISOs, business executives, consumer digital rights advocates and regulators. This has not been attempted before in the security community.

Thus, we ask:

RQ1: How is the effectiveness of the GDPR regulator judged by involved stakeholders?

RQ2: How could we better measure the performance of the GDPR regulator?

We supplement the qualitative analysis with data on national budgets, headcount, complaints, investigations and fines from published EU and DPA annual reports.

It is important to note that data protection and privacy are technically different concepts, explained in more detail in Section 2.2. However, all participants and much of the related literature used these terms interchangeably, and we use them as reported. Data protection originates from the right to privacy. The law and terminology vary outside Europe. For example, in the United States, agencies enforce privacy or data privacy laws. In Europe, DPAs enforce data protection rights. Due to the colloquial conflation of these concepts, DPAs are often informally referred to as "privacy regulators".

Our contributions are:

- We interview and survey a hard-to-reach population of industry practitioners and regulators and thematically analyse how they perceive the role of a regulator and how it informs their evaluation of them in practice.
- We offer a series of KPIs and structural suggestions that we believe may enhance the future development of regulator assessment and accountability in the EU and GPDR-like regimes outside Europe.

The paper is structured as follows: Section 2 is a literature review, and Section 3 describes the methodology. We report our findings in Section 4 and show how five broad themes but narrow criteria emerge in answer to RQ1 and discuss ten potential performance indicators in answer to RQ2. Section 5 discusses the findings, and Section 6 concludes the paper.

2. Background Literature

Regulation studies is a vast field encompassing political science, economics, law, sociology and psychology. We are engineers and computer scientists. Our focus is on the effectiveness of privacy regulators which is why we limit our literature review to a high-level overview to the theories of regulation, the role of the regulator and models of performance measurement. We study how these theories apply to privacy, security and the GDPR. We show that weak performance measurement of regulators is a common issue and draw inspiration from management theory on scorecard frameworks.

2.1. The Theory of Regulation

We examine the importance of regulation, the logic behind it and how it is administered.

According to the OECD, regulation is indispensable to the proper functioning of economies and societies (69). It is a key tool for governments to achieve their economic, social or environmental policy objectives. A classic definition of regulation is the "sustained and focused attempt to alter the behaviour of others according to standards or goals with the intention of producing a broadly identified outcome or outcomes" (10). The UK National Audit Office describes it as using incentives or interventions to drive behaviour change in individuals and organisations outside of government's direct oversight (64).

Governments regulate for many reasons. A non-technical motivation might be linked to political philosophy or populism. For example, it is not unknown for political parties to regulate or deregulate an industry for reasons connected to their re-election. The technical justification for regulation is that it addresses market failures that are not in accordance with the public interest (13; 71; 62; 53). Baldwin and Cave (5) cite well-recognised reasons commonly given for regulating such as monopolies and natural monopolies, windfall profits, externalities, information inadequacies, continuity and availability of services, anti-competitive behaviour and predatory pricing etc. They do not occur in a mutually exclusive fashion, and often the case for regulating will be based on a combination of rationales.

There are three broad modes of regulation (21): technology-based, which is prescriptive and often has strict auditable standards; management-based, where business design their own compliance plan but where the capacity to assess it externally is difficult; and incentive or performance-based, where business design their own plan and where it can be assessed externally against regulatory targets.

The theory of enforcement broadly splits along hard and soft lines (1). Hard Deterrence (or Command and Control) enforcement assumes businesses will try to evade regulations. It tends to be rules-based and a companion to the technology-based mode of regulation. Soft Persuasive (or Cooperative) enforcement assumes business will try to comply. It tends to be more principles or risk-based and a companion to management or performance-based mode of regulation. Gaming studies (73) suggest the cooperative approach improves the chances of low-cost compliance in the long run. If a firm evades, the government can use enforcement, "tit for tat" (79), or it can employ "responsive regulation" (4), otherwise known as the "walk softly and carry many sticks". Critics (2) question this since it assumes the regulator has perfect information, perfect discretion, knows the right proportionate response, suffers no turf wars and can credibly commit to using the strongest enforcement mechanism when necessary.

Compliance is driven by external and internal influences that generate its "social license" (50). External pressure may come from company shareholders, NGOs and customers. These actors, in effect, give companies their "social license to operate," and pressure can revoke that license. Internal pressure may come from the employees in trust and management-based regulation. Compliance requires buy-in from the company and is related to deep commitment, routinization, professionalization (7). This is why naming and shaming can sometimes be effective.

2.2. The Practice of GDPR Regulation

We examine the evolution of the GDPR and how it is implemented in practice.

Identifying the motivations behind the GDPR is not simple since it is derived from years-long negotiations between EU member states and not one government. What is clear is that the roots of the GDPR can be traced back to two concepts: privacy and data protection.

The European Convention on Human Rights (ECHR) (28; 29) signed in 1950, protects the right to respect for private and family life. By the 1970's, the spread of databanks and debate about abusive data collection led several European states to introduce their own personal data regulations (16; 44; 86). In Germany, the term informational self-determination (15; 75; 88) became key to understanding the German view of privacy after a constitutional case in 1983 ruled that *"the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others."* Norway, Sweden, France and the UK (44) enshrined the right to data protection as a *sui generis* (in a class by itself) right, but they did not adopt the German concept of self-determination. They saw data as a valuable resource and subject to competing interests.

The first EU-wide legislation, the Data Protection Directive (DPD) (42), adopted in 1995, sought to enhance the free flow of personal data and to safeguard *"fundamental rights and freedoms [. . .] in relation to the processing of personal data."* It was prompted by economic interests and EU market integration. The Charter of Fundamental Rights of the European Union (43), declared in 2000, elevated data protection to a distinct right (on par with other rights such as the right to free speech, for example) within the legal order of the EU.

The GDPR (37) in 2018 replaced and repealed the DPD. It talks to *"the protection of individuals with regard to the processing of personal data and on the free movement of such data."* This dual mandate is a mix of prohibition and permission. It is prohibitive because personal data cannot be processed unless certain conditions are satisfied, echoing informational self-determination and individual control. At the same time, it is permissive because personal data can be processed provided certain conditions are satisfied. This dual mandate balances interests, but it also underlies many of the critiques of the day-to-day operation of the GDPR.

In addition to the philosophical motivations, the GDPR addresses market failures in the data economy, such as market concentration and information asymmetries, which are classic technical justifications for such a regulation. The GDPR gives users the right to request the information stored about them, the right to have it corrected or deleted, and the right to move their data to another data controller. Consumers are often unaware that service personalization, recommender systems and targeted advertising use their personal data to affect their purchasing behaviour, the so-called surveillance capitalism society (91). The GDPR forces companies to be more open by requiring consent up-front.

The GDPR is a mix of the three modes of regulation but not in equal measure. Two of the NGOs interviewed want it to be more technology-based and issue fines for clear-cut violations like automated speeding tickets. Others want it to be more performance-based, but it is difficult to assess a company's privacy practices without entering their premises and observing them in detail. As a result, the GDPR is mostly management-based, with companies committing to implementing the appropriate people, processes, and technology to support compliance.

Enforcement of GDPR is a mixture of hard and soft regulation. The powers delegated to regulators are awe-inspiring, including the power to fine a company up to 4% of global revenue and/or the power to ban a company from processing certain data which could bring a company's operations to a halt. Whereas enforcement theorists stress a coercive strategy of monitoring and sanctions, management theorists embrace a problem-solving approach based on capacity building, rule interpretation, and transparency. Research suggests that enforcement and management mechanisms are most effective when combined in a "management-enforcement ladder" (83). Typically it escalates from (i) rule publicity to avoid inadvertent non-compliance (ii) enhanced monitoring (iii) legal proceedings and/or bargaining with violators (iv) sanctions or fines if non-compliance persists. As we shall see, regulators differ in how they interpret and exercise their powers.

2.3. The Role of a Regulator

We examine why we delegate authority to bureaucracies and how we hold them accountable whilst protecting their independence.

Governments delegate authority to bureaucracies for two reasons: competence and credible commitment (47). Bureaucracies have expertise that politicians lack, especially in complex policy and technological areas. This expertise can help reduce transaction costs and resolve disputes. Governments can also delegate authority to bureaucracies to tie their own hands and commit to stable policies. This can help prevent governments from taking expedient short-term measures that may be harmful in the long run (89; 58). To insulate senior officials from political interference, governments typically give them fixed terms of tenure, allow them to be fired only for cause, and remove them from direct executive control.

This independence can create its own issue, namely the principal-agent problem, where the agent (the bureaucracy) has more knowledge or policy expertise than the principal (the politicians) and can shirk or deviate from the principal's wishes. To mitigate this problem, governments can give agencies less authority when the issue is salient to the public (9; 74; 48; 81) and more authority when the issue is complex and requires expertise (8). Governments can also put in place monitoring agencies, administrative procedures, and policy evaluation tools to check on agencies and reduce the potential for bureaucratic drift.

De facto independence, or the ability of a bureaucracy to act without political interference, is achieved through a good reputation and autonomy (18). A good reputation is built on a history of competence, consistency, and flexibility. Autonomy is granted when "political authorities see it as in their interest to defer to agency action" (17). Together, these factors can protect a bureaucracy from political threats and meddling.

2.4. The Role of the GDPR Regulator

We examine the regulatory architecture behind the GDPR regulator and the light-touch accountability.

The EU has its own legislature (the European Parliament and the Council of Ministers) and executive (the European Commission (EC) and the European Council), as well as an independent judiciary and a central bank. These are supported and complemented by a set of institutions and bodies, including inter alia the European Ombudsman (EO), the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS).

The EDPB (36) is *"an independent body of the Union"* (recital 139) with legal personality that contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between supervisory authorities. The EDPB comprises the heads of the supervisory authorities (SA) and the EDPS, which provides secretariat services. It can provide general guidance (including guidelines, opinions, recommendations and best practices), advise the EC on new proposed legislation relating to data protection, make binding decisions addressed to the supervisory authorities in member states, and promote cooperation and the effective exchange of information and best practice between them (40). The EC has the right to participate in the activities and meetings of the Board without voting rights. The Chair of the EDPB communicates to the EC the activities of the EDPB.

The SAs (A.K.A the DPAs) are the national data protection regulators. Each member state must appoint one (or more) (31), and they must be independent (32) and "free from external influence." Member states are required to furnish them with adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of their tasks and exercise of their powers. Member States are required to appoint staff by means of a transparent procedure (by their parliament, government, head of State, or an independent body), for a fixed term only dismissable in cases of serious misconduct.

Regarding national oversight, each member state must ensure that each SA is 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. In terms of European oversight, the GDPR has very little to say other than Article 59 (35) and Activity Reports *"Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2) (34). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and the Board."* Accountability is defined in three sentences.

2.5. Regulator Performance Assessment

According to the OECD Best Practice Principles on the Governance of Regulators, a well-designed performance framework serves multiple goals: demonstrating the effectiveness of the regulator, building confidence in the regulatory system and driving improvements (69). Performance assessment is a critical ingredient for maintaining accountability and fostering transparency, and public bodies are often required to report on results and enable scrutiny of their performance. Data on the performance of both the regulator and the regulated sector are an important ingredient of economic regulators' performance assessment frameworks. The results can also be part of organisational learning, providing inputs into decision-making.

The theory of performance assessment of regulators has evolved over time. Early approaches focused on compliance monitoring. Ogus (70) identified the shift from command and control to more flexible and performance-based approaches that incentivize industries to improve their performance. Output-based regulation (57) focuses on regulating outputs rather than inputs, while outcome-based regulation (51) sets specific, measurable goals for the industry and evaluates their progress towards these goals. Risk-based regulation (5) assesses the likelihood and potential impact of risks associated with complex industries with significant uncertainty. More recently, Coglianese (20) argues regulatory performance should be measured by evaluating the impact of regulation and regulatory policy on society, including how well regulations achieve their intended goals, how much they cost, and how they affect different groups of people.

In recent years, governments like the UK (63) have turned to Key Performance Indicators (KPIs) and Balanced Scorecards (BSCs) to assess their regulators. The BSC is a strategic management tool that tracks and manages performance across four dimensions: financial, customer, internal processes, and learning and growth. For regulatory authorities, this framework can be used to measure factors such as budget utilization, cost savings, customer satisfaction, stakeholder engagement, regulatory decision-making, industry compliance, employee training, innovation, and technology adoption.

2.6. GDPR Regulator Performance Assessment

There is no standard performance assessment framework for the GDPR DPAs. The EC published a report in 2019 on the application of GDPR (38). The next one is due in 2024. The EDPB has published two reports (25; 26) that do contain some KPIs for some DPAs. Due to historic definitional and administrative differences, the KPIs are not entirely comparable and the second report does not include all the EU GDPR regulators. The DPAs publish their own annual reports, they are formatted differently and they can vary significantly in length. For example, the Irish DPA 2021 annual report (85) is 119 pages compared to the 2022 report, which is 46 pages (23).

The European Ombudsman (EO) is an independent and impartial body that holds EU institutions accountable for their actions. The Ombudsman investigates complaints about maladministration by EU institutions and bodies. In 2021, a complaint (77) was made to the EO that the EC was not collecting enough information to monitor the enforcement of the GDPR, particularly in Ireland. The outcome was an agreement that the EC would require a bi-monthly report from the Irish DPA (27), which the EDPB expanded into a requirement for all member state DPAs to report on large-scale cross-border investigations (59).

2.7. Motivation

The GDPR regulator's mission is to safeguard data protection rights, which involves upholding individuals' information rights and data privacy. What does that mean in practice, and how do we know if they are doing a good job? Governments and the EU have struggled to answer this question, and it is a gap in the existing literature. It is important because regulators are key to achieving policy objectives. Hence, we are interested in how practitioners perceive regulators' effectiveness now and explore if there are better ways to measure it and thereby improve accountability and comparability going forward.

3. Methodology

We used a mix of qualitative and quantitative research approaches based on semi-structured interviews, surveys, and publicly available data to understand, describe and explain how practitioners perceive the success of privacy regulators. We seek to uncover how practitioners conceive what regulators do or should do in terms that are meaningful and that offer rich insight (6). Qualitative research techniques and interpretive analysis have an acknowledged tradition within information systems research (87). An inductive approach of applied thematic analysis (49) was used for the interviews. Quantitative supplemental data was drawn from multiple sources to help contextualise the reported activity of regulators.

3.1. Qualitative Data Collection & Analysis

Our research findings are based on 23 semi-structured one-to-one interviews and 70 survey responses. The study's guiding research questions were "How is the effectiveness of the GDPR regulator judged by involved stakeholders?" and "How could we better measure the performance of the GDPR regulator?" The questions were deliberately broad given the exploratory nature of the study and the absence of previous findings on this subject.

The interview structure underwent two phases before we settled on a protocol to operationalise the RQs. In the initial three interviews, we found that if you led with questions about regulators, participants referred back to the regulation. And if you led with the regulation, participants either claimed unfamiliarity with the legal text or felt that it depended on the regulator. We also found that we had too many questions. Ultimately, to avoid going around in circles, we found that leading with "In your opinion, what are the objectives of the regulator" stimulated practitioners to think holistically about the topic and put them in the right frame of mind for RQ1. We then reflected back to them their answers and asked how they judged or measured regulator effectiveness against their stated objectives.

To answer RQ2, we initially asked participants to suggest other measures. This was not productive. Participants either repeated their answers to RQ1 or went off on tangents. Instead, we discovered we could better focus the interview by presenting them with 10 generic KPIs and inviting them to discuss and rank them in importance. If they didn't volunteer it in conversation, we invited them to create, merge or omit our KPIs to address RQ2 to their satisfaction. The interview protocol can be found in Table 9 in the Appendix.

To generate the KPIs in the absence of an official EU KPI scorecard, we looked for inspiration in the earlier-referenced literature in Section 2. Ideally, if the objective of regulation is to enable governments to drive behaviour change to achieve policy objectives (10; 64), this meant we needed metrics that evaluated the success of the DPA's in meeting the technical goals set out in the GDPR and the more intangible expectations of society in general (which is a tall order). We needed to be practical and choose indicators that were measurable and accessible. We also required a range of metrics to track performance across several dimensions. Starting with the theory of input-based regulation (70), we use regulator financial budgets and human resources, accessible in the DPA's annual reports, as an input metric. Adequate resources are generally regarded as an essential prerequisite to good regulation infrastructure. Leaning on the theory of output-based regulation (57), we chose activity metrics such as the number of investigations, complaints and fines as most regulators publish them, and they are meaningful to consumers and businesspeople alike. It is not straightforward to apply outcome or risk-based regulation theory (51; 5) in this context since confidence in the regulator and the system is difficult to encapsulate. Although less quantifiable, we chose impact measures such as the media impact of fines and the deterrence effect of large fines on business as they capture the longer-term effects. As perception metrics, we chose public awareness and understanding of GDPR rights and feelings of improved personal data control as key stakeholder measures. Similarly, we chose business perception of good guidance and outreach as the other key stakeholder measure. Together, they follow Coglianese's recent works (20) on measuring regulatory performance by evaluating the impact on society and how they affect different groups of people.

Interviews were conducted and recorded over Microsoft Teams as recommended by our organisation's ethics and data protection policies. After transcription, recordings were deleted. The interviews took between 30 minutes and 110 minutes, with an average of 50 minutes. One participant preferred not to be recorded, and two were interviewed in person rather than over Teams, and their data was collected via note-taking. The NVivo 1.7.1 platform was used to code and analyse the text. The analysis was informed by the Braun and Clarke (11) six-step process, the Ryan and Bernard (76) techniques on theme identification and the Williams and Moser (90) art of coding and thematic exploration. The authors followed an open-axial-selective coding process. It involved both deductive and inductive approaches, where the former produced a set of a-priori codes while the latter produced the final set of themes that we present in the results section. The a-priori codes comprised 10 KPIs and a handful of generic themes for regulator objectives and judgment criteria. All a-priori codes were general and did not include loaded terms. Analysis of the interview transcripts expanded the number of codes, yielding altogether 76 regulator objective codes, 74 judgment criteria codes and 24 KPI codes. Each code had between 1 to 30 snippets of interview text behind it. Through an iterative process, the authors amalgamated similar codes and clustered codes until the final themes began to surface. We do not report inter-rater agreement scores, as they are inappropriate in reflexive TA (12). The final codebook can be found in Appendix A.

The survey of the 70 CISOs was conducted over Mentimeter, an audience engagement platform. After a short introduction by one of the authors, the presentation screen switched to the Menti screen. The survey consisted simply of four questions: "What are

the objectives of a privacy regulator, in your opinion?" and "How do you judge the effectiveness/success of a privacy regulator?" The audience could input their answers via their mobile phones or laptops into a dynamic word cloud and see everyone else's answers as well. The third question presented them with our ten potential KPIs and asked them to rank them. This live and instant polling feature meant they could see the cumulative ranking in real-time. Finally, the fourth question asked "What other KPI measures might be better?" which allowed them to suggest alternative KPIs onto the word cloud. In this way, we collected their input for analysis.

3.2. Sample Characteristics

We aimed to recruit a diverse range of stakeholders for our privacy and security study, with a particular focus on chief information security officers (CISOs). One of the authors was invited to speak at a confidential invitation-only information security industry meeting organised by a Big 4 consultancy firm for their high-value clients. Under Chatham-House rules, we were allowed to mass-test our research questions and KPIs using the Mentimeter presentation and real-time voting platform. We began recruiting for interviews and successfully brought in CISOs, former CISOs, management consultants, and privacy partners from law firms. We contacted NGOs, receiving valuable help and introductions to academics, national regulators, and EU contacts. These introductions proved more effective than approaching the data protection regulators directly. Networking and snowball sampling helped us recruit sales, marketing, data protection and general management professionals from SMEs and international companies, ensuring a diverse perspective. In total, we surveyed 70 CISOs at the private industry meeting and had face-to-face interviews with 16 business people, 3 NGOs and 4 data protection regulators. We categorized them for analysis: Legal (in-house and external lawyers), Executive (non-legal business individuals and consultants), NGO (European and US organizations), and Regulator (EU and EFTA regulators).

Table 1. Interviewees P1–P23 & Conference Survey C1–C70

Group	**Labels**	**Male/Female**
CISO	P1 to P6	5/1
Executive	P7 to P10	2/2
Legal	P11 to P16	2/4
NGO	P17 to P19	2/1
Regulator	P20 to P23	4/0
CISO Conference	C1 to C70	64/6

It is worth noting that we did not include consumers in our sample because we wanted to interview individuals who were involved in the regulatory process. Earlier work by the authors (14) found inter alia that the UK data protection regulator registered modest name recognition with a UK-based sample. Ordinary people do not spend time thinking about our research question topics. For this reason, we felt recruiting NGO's who were full-time consumer digital rights advocates would be more productive in capturing the user perspective.

3.3. Quantitative Data Collection & Analysis

There is no one central database of GDPR regulator activity. Instead, one has to sew together information from diverse sources.

The EDPB publishes a register containing decisions taken by national supervisory authorities following the One-Stop-Shop cooperation procedure (Art. 60 GDPR) on its website. This is a small subset of all decisions. The EDPB has also published two overviews of resources made available by Member States to the DPAs (25; 26). These contain data on financial and human resources and enforcement statistics. The 2022 overview is shorter than the 2021 overview and is light on detail. Nevertheless, these two documents are useful.

The NGO, noyb, maintains a GDPRhub Decision Database (66). Volunteers collect summaries of decisions by national DPAs and courts in English. It is incomplete because not every DPA issues its reports publicly. This is a limitation of this analysis. The European law firm CMA maintains a database (19), Enforcement Tracker, which tracks similar data.

The EDPB, EDPS and the DPAs all publish annual reports. There is no standardised format. They are all different. There are no harmonised definitions for cases or decisions which make comparative analysis problematic. Despite these limitations, we use the data from the referenced sources to complement and augment the qualitative analysis.

3.4. Ethical Considerations

The study was approved by the authors' departmental Research Ethics Committee and is designed to follow the principles of pseudonymity, confidentiality and informed consent. Individual participants are not identified and were not compensated. The participants were aware of the research's purpose, the researchers involved, and their role in it.

4. Results

Section 4.1 is an overview of the financial, human resources and activity data of the GDPR regulators. Although incomplete, it sets the scene for appreciating the five themes that arose when participants were asked how they currently judge the effectiveness of a privacy regulator in Section 4.2 and appreciating the relevance of the KPIs that were discussed as potentially better measures of performance in Section 4.3.

4.1. Regulator Data

As discussed in Section 3.3, regulator data is not centralised. Table 2 has been assembled from multiple sources with differing time cut-offs. We did request data up to the 5th anniversary of GDPR from all 31 DPAs but only 13 had replied after six weeks (5 referred to us their out-of-date and/or incomplete websites, 5 sent acknowledgements with no follow-up, and 3 supplied full answers).

Germany and the UK have the biggest budgets and headcounts but are not the biggest finers by number or value. At least ten DPAs still have budgets under €2m. The Irish DPC is the "lead" authority for Google (including YouTube), Meta (including Facebook, Instagram, WhatsApp), Apple, TikTok, and Microsoft (including Linkedin, Xbox, etc.) across the EU, because these firms have their European headquarters in Ireland. This explains why it is the lead enforcer in terms of fine value and cross-border cases (46). Its budget is not the biggest, but it is in the top 5 and almost level with France. The world's fourth technology firm by market capitalisation, Amazon, is based in Luxembourg. After a recent decision, its regulator is now the second-highest finer by value. The Spanish regulator, by far and away, remains the most active enforcer as measured by the number of fines, followed by Italy and Romania.

Table 2. GDPR Statistics

Country	Budget[α β]	FTEs [β]	Cases[γ]	Complaints[γ]	Investigate[γ]	Fine Num[δ]	Fine Val €[ϵ]
Austria[ζ]	4.6m	45	1940	1822	337	20	25m
Belgium	9.7m	62	1370	1368	2	39	1.8m
Bulgaria	1.9m	87	274	445	133	24	3.7m
Croatia[η]	1.39m	34				20	2.8m
Rep of Cyprus	0.8m	23	19	9	3	37	1.36m
Czech Rep	6.4m	113	916	687	45	26	0.17m
Denmark	7.8m	80	5726	1328	100	25	2.4m
Estonia	0.9m	21	511	416	28	6	0.3m
Finland	4.5m	52		1527	22	18	2.6m
France	23.9m	263	3630	5830	162	35	298m
Germany[κ θ]	114m	1155	17616	8089		149	55m
Greece	2.5m	51	519	428	6	57	30.6m
Hungary	4m	111	174	50	10	68	2.3m
Ireland	23.2m	257	7400	1700	5	24	1310m
Italy[θ]	44.6m	139	4896		10	265	123m
Latvia	1.4m	34	462	449		15	0.2m
Lithuania	1.6m	56	3214	555	16	9	0.25m
Luxembourg	8.3m	54	18	176	18	31	746m
Malta	0.6m	14	37	229	1	11	0.36m
Netherlands	28.7m	167	6740	1090	8	22	14.7m
Poland	9.1m	260	4755	3902	31	50	3.4m
Portugal[θ]	2.5m	26				7	6.1m
Romania	1m	34	288	1733	133	138	0.7m
Slovakia	1.7m	45	352	568	9	9	0.13m
Slovenia	2.5m	49	666	257	37	0	0
Spain	16.8m	185	11212	4910	2	646	59.5m
Sweden	11.9m	122	24	943	24	22	14.7m
Iceland	2.2m	19	145	51	6	9	0.2m
Liechtenstein	1.2m	7	30	28	2	1	0.04m
Norway[θ]	7.5m	62	3200			50	10.4m
UK[ι]	66m	823	36343		474	13	75m

Notes: [α] All budgets in € except the UK (£). [β] Budgets and FTE sourced from EDPB Report 5th September 2022 (26) and UK ICO Annual Report 2021/22 (84). [γ] Cumulative cases, complaints and ex officio investigations sourced from EDPB Report August 2021 (25). [δ] Cumulative number of publicly available fines up to 16th May 2023 sourced from CMS GDPR Enforcement (19). [ϵ] Cumulative value of known fines (which does not include all fines as some DPAs do not identify the controller or quantify the fines) up to 16th May 2023 sourced from CMS GDPR Enforcement (19). [ζ] Austrian data replicated from 2020 as there was no data for the 2021 report. [η] Croatia's GDPR did not formally come into force until January 2023. [θ] Data is missing from EDPB report. [ι] UK budget figure is not exclusive to GDPR duties and cases include complaints and data breaches. [κ] German records are only available from some of their regional SAs.

4.2. RQ1: 'How is the effectiveness of the GDPR regulator judged by involved stakeholders?'

As described in the Methods section, we broke this into two parts. First, we asked 'What are the objectives of the privacy regulator, in your opinion?' because practitioners tied themselves in knots pondering the purpose of the regulation. Unsurprisingly, apart from a subset of legally trained participants, most practitioners were unaware that the purpose of the GDPR is clearly described in its text in Article 1 (30), and the role and responsibilities of supervisory authorities are described in Article 57 (33). Next, once they were focussed on how they construct the purpose of the regulator in their own minds, we followed up with, 'How do you judge the effectiveness/success of the privacy regulator?'

In summary, our research has identified five themes that capture how practitioners perceive the role of a privacy regulator and how it informs their subsequent evaluation thereof. The first two refer to a collection of related perceptions that we have clustered under the portmanteau of Lofty Views and Cynical Views. The other three are Enforcement, Clear Guidance for Business and Consumer Protector. We find judgement is very much in the eye of the beholder, depending on the expertise and background of interviewees. Each group (CISO, NGO etc.) had a different mental scorecard for evaluating regulators. We also find that the criteria they use in practice are a small subset of the many objectives they cited for the first part of RQ1.

The following sections will discuss each theme and how practitioners evaluate them to answer both parts of RQ1. The codebook for each theme can be found in the appendix A.

4.2.1. Lofty View

The lofty or idealistic view is that the regulator is there to be a change agent and execute many of the technical justifications outlined in Section 2.1. Thus, the regulator was there to ensure the regulation was a priority in organisations, that executives took responsibility and that it resulted in *"ex-ante good behaviour rather than ex-post fines"* (P9). Without using the words 'market failure', practitioners instinctively saw the regulator as there to make the rules for everyone and *"create a trustworthy market"* (C7). A common presumption was that the regulator should be independent, impartial and proportionate.

How practitioners evaluated this aspiration, however, was indeterminate. Success was judged by intangibles such as leadership, vision, and being seen to take a balanced multi-stakeholder approach to issues. Appearances that showed they were monitoring and in control were important. Being accessible and an organisation capable of learning were also quoted as good markers of effectiveness.

4.2.2. Cynical View

There is a sceptical or cynical view that the regulator is there to appear to be in control. *"If you don't control and you're not seen to control, then what's the point"* (P6)? Non-regulator participants believed the regulators' organisational agenda was to look good and always plead insufficient resources. NGOs believed regulators were complicit in *"compliance theatre"* (P18). One regulator accused a fellow regulator of *"indulging in procedural rather substantive activities"* (P22). He felt his fellow regulators *"were deliberately secretive as a group"* (P22). This chimed with another pan-European regulator's observation that *"We have KPIs but the definitions are not consistent. We have reports but not from all member state regulators"* (P23). The personal agenda of staff was assumed to be to gain experience or serve a term and then parachute into a better-paying job in a corporate or a consultancy.

This negative view coloured how participants evaluated regulators in practice. For some, the measure of success was *"a reduction in the number of data breaches"* (C3) or *"a lack of news about breaches"* (P8) or *"a lack of enforcements"* (P8). Expressed slightly differently it was *"less fines, but without consumers complaining"* (C7). That latter sarcastic standard was rationalised as evidence that regulators had succeeded in changing the behaviour of organisations. More prosaically, one participant saw success as eliminating *"people cold call calling you"* and *"spam"* (P7).

4.2.3. Enforcer

The enforcement theme emerged as the key role of the regulator. The purpose of a regulator is *"to enforce the law"* (C3) and *"investigate reported data breaches"* (C5). The GDPR was seen to have given regulators *"real teeth"* (P2) to punish companies. Many expressed fear of the reputational impact as much as the financial impact on their company. In fact,

> *"naming and shaming is considered an additional sanction on top of fines by regulators in some EU jurisdictions e.g. Germany."* (P22)

When practitioners think about enforcement, they think in numbers: *"by total fines issued"* (C8), *"on the number/value of enforcement activity"* (C3), *"the number of complaints"* (P22), *"number of investigations, number of decision, number of corrective measures"* (P19) and *"how many companies have DPOs"* (P1)? When invited to distinguish between their personal and business perspectives, participants see fines as the consummation of consumer protection.

A few thought fines were the wrong thing to focus on and could be counter-productive. Far better to quietly reprimand a company *"rather than putting a head on a spike"* (P5). Some thought fines were a bad measure since an uptick could mean many things: for example, a deterioration in compliance, an increase in regulator resources, a new focus by the regulator or a knock-on effect from events in another country. Some thought fines should be graded in severity depending on whether they were *"sins of omission or commission"* (P4). One CISO felt business was more the victim than the villain since consumers get compensated if they suffer a loss from a data breach whereas the company gets fined and then has to find the funds to improve their information security infrastructure. NGO's, on the other hand, felt fines were not enough to stop certain practices. It is *"the sanctioning power that matters, it's the ability to ban processing. [...] You're selling this data on really. Stop doing that"* (P18).

4.2.4. Guide

Education and awareness-raising were cited by all participants, including the regulators themselves. Clear guidance was seen by business people, legal counsel and management consultancies as the primary task of the regulator. Certainty was seen as a shield against inadvertent non-compliance by an organisation.

Judgement of their performance depended on one's interaction and point of view. According to the privacy practice leader at a leading law firm:

> *"the key ingredients are clear expectations through good guidance [. . .] having a dialogue and relationship [. . .] guidance which matches the real world problems and anticipates where the tension points are going to be."* (P15)

The educational and informational role was judged by CISOs and DPOs by the visibility of the regulator at industry events and the quality of the information, such as case studies, opinions, codes of practice and FAQs on their website. CISOs, in particular, wanted to see the regulator as a 'collaborator' (P6) and 'partner' and staffed with high-calibre professionals who are *"not just making knee-jerk decisions"* (P2). A management consultant said *"We rely totally on the ICO"* (P9), but certainty is fragile. When Equifax successfully challenged the ICOs ruling in an appeals tribunal, it introduced *"a new level of uncertainty [concerning the solidity of their guidance]. One got to look behind the curtain of the Wizard of Oz"* (P15). When the ICO announced a £180m+ fine on BA but later settled for a fraction of that, a lawyer opined *"they should have gone for something smaller but more solid because any climbdown just makes people believe less that it really does have a big stick"* (P15).

4.2.5. Protector

The consumer protection role meant most participants saw the regulator as the backstop, the helper, the adviser, the educator, the body that empowered the consumer, that responded to complaints and launched investigations and protected our privacy. It did not come up in the interviews, but it is worth noting the protection role is also vital for people beyond just consumers (e.g. workers, students, citizens, refugees, etc),

This expectation of the regulator suffered the same lack of follow-through as the lofty view. Participants spoke generically about the regulator helping the public if they had concerns but failed to quote anything tangible. Complaint metrics were mentioned by a few but in a dismissive way. One NGO was more interested in decisions and corrective actions, as complaint volumes could be shaped as much by awareness as by a lack of awareness and was deemed meaningless. A regulator quoted Article 57 1(f), which refers to the compliant reporting guidelines for regulators, and commented that every regulator did it differently regarding transparency, thresholds, backlogs and case count criteria.

Finally, even the research question itself threw up strange reactions. More than one participant admitted it had never occurred to them to think the question, whilst two legal participants thought it almost bad manners 'to judge the judges'. One NGO joked that the legal profession was so obsessed with ticking boxes that asking them for an opinion about its value was akin to *"asking cattle farmers about veganism"* (P18).

4.3. RQ2: 'How could we better measure the performance of the GDPR regulator?'

We found early participants struggled to move beyond their answers to RQ1 or went off on tangents about the regulation itself. To bring better focus to the interviews, we devised a balanced scorecard of ten KPIs that we adapted from work in related fields (20; 63). We invited participants to discuss them, rank them in importance and suggest alternatives. Separately, we invited CISO's at an information security conference to rank the KPIs. Their ranking was similar with the proviso that the interviewees emphasised the importance of financial and human resources. This section reports the findings under each KPI, suggested alternative KPIs and the two ranking exercises.

4.3.1. Secured adequate financial and human resources

Most participants were unsympathetic. *"I'm a bit cynical [. . .] I don't have the right budget and human resources, but I'm still expected to do my job"* (P11). Another opined, *"It's the human default in business to try and get more money and more people to make everyone's life easier"* (P8). In contrast, a regulator said *"75 to 85% of regulators do not have sufficient resources and are forced to prioritise"* (P22). This tallies with the EDPB's 2021& 2022 overview on resources made available by member states (25; 26), which showed 82% and 77% respectively of regulators felt they had insufficient allocated budgets and 86% and 87% insufficient human resources to carry out their tasks. To put numbers to this, the combined budget of EEA DPAs (UK excluded) has grown since 2016, from €167.1 million to €337.6 million in 2022 (55).

Quality of staff was mentioned often. One CISO, who had been an expert witness in a case, likened it to watching undergraduate regulator staff up against PhD-calibre corporate opponents (P4). There was sympathy for *"overstretched"* (P16) resources although pragmatism ruled

> *"you are probably never gonna have the level of resources to undertake the volume of investigations, complaints and fines that you possibly could get involved with. And so I think you have to pick and choose."* (P5)

However, as the interviews progressed, participants admitted that *"if you want it to be done right, then you have to spend the money"* (P7) and one needs *"adequate financial resources because everything else does come off that"* (P15). In fact, one interviewee took comfort that public statements from the Irish regulator demonstrated they were *"tooling themselves up to have the right resources"* (P11). Regulators have a more nuanced perspective. One thought it was a good KPI because it was a measure of the success of *"shouting or lobbying"* (P22) by a regulator to secure adequate funding, whilst another recognised that the complicating factor of independence meant that *"it's very difficult to make to budget allocation policy-neutral"* (P21).

4.3.2. Public perception of improved personal data control

The 70 survey respondents thought this was the most important KPI. Many felt it should be combined or paired with the awareness & understanding KPI as they were intertwined. One regulator liked the emphasis on public stakeholder KPIs. After all, *"DPAs are there for the people"* and *"we are not working for ourselves"* (P22). Active visible enforcement was seen as vital.

> *"I would say that for the perception to be real, it does need some element of public enforcement and a sort of lived experience of the regulator intervening effectively to dissuade the infractions."* (P15)

While there was consensus about the outcome, there was less agreement about the calculation.

> *"If we can contribute to them getting better control of their personal data or personal information, I think we play a good role. How measurable is this is extremely difficult."* (P21)

A second regulator was even more scathing:

> *"Perceptions of it can be your perception of it [...] or the regulated organization's perception of it or the general public's perception of it, and what you will measure there will depend on the year when you're doing the survey."* (P20)

A DPO described it as *"a hygiene factor. People's feelings are not a reliable measure"* (P10).

4.3.3. Business perception of good guidance and outreach

When interviewees were asked their views as private citizens, the improved personal control KPI was most important. As business people, however, the relationship with the regulator was more important, as was the perception that it should be there as a partner and collaborator and performing not just a *"auditing policing role [...] but actually contributing and helping you"* (P2). Many felt this was a good measure as business is an important stakeholder and a *"good judge of character"* (P3). There was generalised grumbling about generic versus specific advice by the legal participants. *"For us, it's clear guidance. So, when we ask a question, we want an answer. We don't want an obfuscation"* (P9). At least two complimented the UK regulator, the ICO, for clear guidance and an informative website. Certainty is key for the advisory profession. *"The purpose of good regulation is to create guard rails"* (P9) so that they can advise their clients on how to operate lawfully. The regulators also have their own reasons for issuing clear guidance. Any room for misinterpretation could undermine *"robust enforcement decisions"* (P20). This tension was characterised as follows:

> *"It's a very complex relationship between a regulator and a company. We want to work together. We both want to achieve the same goal. But at the end of the day businesses are accountable for what they do, and [...] we are controlling them, we are supervising them, so the relationship is not balanced."* (P21)

Another regulator observed *"Most businesses want to comply"* (P22) which is why this metric is important for governance regimes that rely on cooperation.

4.3.4. Media impact of fines and regulator leadership

There was unanimous agreement on two aspects: *"the media impact draws attention to the fact that the regulators are taking action"* (P14) and that companies are *"more worried about the public reputational impact than the actual number"* (P2). Even when the fine appears high, *"it's in the headline rather than the bottom line"* (P2). This attitude is probably conditioned by the size of the fines levied historically being small compared to the profits of large multinationals. One NGO wryly characterised the financial pain of €100m+ fines on Meta as equivalent to mere *"parking tickets"* (P18). (This interview took place before the Irish DPC levied a €1.2Bn fine on Meta in May 2023 - the first and only fine to date to breach the Bn threshold).

Public fining of well-known companies in the same industry does however have wider effects and *"everybody will sit up and take note"* (P7). Quite a few believed that the media impact was linked to the size of the fine. If the press fails to pick up on it and report it, then *"we all know that nothing happens unless there's some media outrage"* (P8). A regulator saw the media impact *"as a means to an end and not the goal itself"* (P22). Another regulator felt fines are enormously important for the perception of their authority that they will *"impose fines on a regular basis when people or when companies or organizations are infringing the law"* (P21). Large fines and associated publicity were seen as important *"game changers"* (P20) because they set an important precedent *"not only at the national level but also possibly at European or global level"* (P20). Leadership was referenced by only one NGO with decades of experience dealing with regulators, and they felt the importance of the *"vision"* (P17) of the CEO was undervalued.

4.3.5. Perception regulator is independent of the government

The initial reaction of non-regulators and regulators alike was that it was not a priority. A fairly typical reaction was summed up by one CFO: *"most people would not know or care"* (P8). All the regulators thought it was a non-issue. For example: *"there's a lot of assurance, at least in the privacy world that the regulator is independent of the government. This is enshrined in the texts and at least in many EU countries, there's a long history of independent regulators"* (P20). When pressed on why it was so unimportant, some commercial participants rewound their initial dismissal. Independence from the government in power is important to business because business doesn't want *"surprises"* or suffer *"collateral damage"* (P2) if regulatory change becomes *"politically expedient"* (P7). In a UK context, some felt the new draft Data Protection Bill showed the ICO wanted to be *"more closely aligned to the government"* (P14) and that concerns *"might bubble up more post-Brexit if the UK [...] is playing footloose with your data because they are going after the commercial big bucks"* (P2). In a slightly backhanded compliment, one executive

drew comfort that the ICO was more independent than longer established regulators such as telecoms because it was not as well *"connected"* (P5) to business.

4.3.6. Good public awareness & understanding of GDPR rights

Everybody interviewed, apart from one DPO, thought awareness of GDPR was high. Some questioned *"if the awareness translates into an understanding of the rights"* (P11). For example

> *"subject access requests are a nuisance for lots of organizations. Sometimes they're a nuisance because people request stuff they're not entitled to, which is an education thing."* (P5)

Awareness was regarded as important *"because if you haven't made society aware of what you're doing and taking them with you so that you're working with them, then I think that's a failure"* (P2) as was understanding since *"I think it's paired because if those two are pulled apart, that would be a regulatory failure"* (P2). Education was seen as a key function of a DPA by a DPA because *"better citizen awareness will affect policymaking"* (P22).

4.3.7. Fines issued on a scale that deter

A typical endorsement of the deterrence effect is that large fines *"build confidence in the public that actually these guys have teeth. And there's a crossover between fines and the media impact"* (P7). As a DPO put it *"if a parking fine were £1, people would park everywhere"* (P10). For the same DPO, the bigger the headline fine, the better the attention it commanded *"this is the one thing we can hold up [to the board] and say, You know what, if you don't do this, this is what this is the bad thing that can happen"* (P1). Some participants quibbled the fines in the UK were not re-invested, that strict compliance could put the UK at a competitive disadvantage to China, that large fines could cripple the UK economy, that companies weigh up the fines against the commercial benefit of non-compliance, that fines should be commensurate with the harm and that the focus should be less on the stick and more on clearer guidance. The NGOs felt *"the sanctioning power that matters is the ability to ban processing"* (P18).

4.3.8. Number of investigations

Regulators were the biggest fans of this metric:

> *"You want to show your performance [. . .] These are things that [. . .] we systematically put forward in the annual report because they're key numbers. Those tables over time that you can easily measure do not depend on the people surveyed and things like that."* (P20)

Business people were less convinced. They felt they were *"too open to manipulation"* (P8) and *"more about the performance of the regulator as opposed to whether they are effectively regulating, which is a different question"* (P16).

The NGO's were even more cynical. They regard the metric per se as very important, but they derided regulator-initiated ex-officio investigation metrics. They claimed most were driven by them and by their threats to embarrass the regulators' inaction in the press. *"These people have procedure, political will, resources. Who knows? Some DPAs are definitely quicker than others and we know which ones now after five years if we want a quick decision"* (P19).

4.3.9. Number of complaints

The reaction to this metric fell between nice-to-know and downright misleading. A few felt it acted as a good statistical barometer, particularly if it was accompanied by contextual information to add colour. A strong majority questioned its meaningfulness:

> *"I don't know if she's making that sound like it's a positive thing that we've had more complaints or you could actually say that that's because there's greater public awareness. [. . .] I don't think the number of complaints is a particularly helpful metric, because what's that really showing?"* (P11)

Some accused dissatisfied consumers or disgruntled employees of being opportunistic *"ambulance chasers"* (P2) and using SARs as to further their grievances. One regulator admitted *"it's actually quite tricky to compare the annual reports"* (P21) because *"the notion of complaint, although it is written down in the GDPR is nevertheless not interpreted the same way in every country"* (P21). For example, some regulators are required by national law to respond by letter to every complaint, some push people towards information requests for mediation etc. to stay out of the formal complaint rule process, and others have the discretion to pick and choose what they follow up. One regulator (P22) felt the number of complaints speaks more to awareness of rights and a culture of compliance. If people know their rights, more will complain. The complaints may be justified. Alternatively, people may misunderstand their rights and still make complaints. Different countries will have different thresholds for reaching out and trusting their authorities. For example, he believes that data breaches are over-reported in certain countries. By contrast, in other countries, the complaint procedure can be formal and complex. Thus *"this metric could be about how easy it is to lodge a complaint"* (P22).

4.3.10. Number of fines

This was controversial. Regulators like this metric: *"You will focus [. . .] on the things you can measure [. . .] it's important for our own work as a KPI"* (P20). There was broad agreement among regulators that the desired outcome, i.e. behavior change, was more important than the fine per se. One lawyer applauded the ICO shift to *"naming and shaming as they were in slapping people with big fines"* (P16). Another lawyer liked *"more regulators showing their teeth [. . .] particularly in Europe, you're seeing Spanish, Italian DPA's issuing a lot of fines, but small amounts not sufficient to deter, but maybe to make people think*

twice" (P14). However, many were sceptical of the integrity of the metric since it was generated by the regulators themselves. Liking it to the boundaries of hospital waiting times or flight times being changed to meet a scheduled target, more than one cynic felt regulators would *"spin the number to suit the argument"* (P7). One regulator even accused another of being guilty of that gamesmanship rather than focusing on substance.

4.4. KPI Rankings

Table 3. Average Ranking scores of KPIs for Interviews (I) and CISO Menti (M) responses. The lower the rank (the darker the colour), the more important.

KPI	I	M
Secured adequate financial and human resources	2.7	6.3
Public perception of improved personal data control	2.8	2.7
Business perception of good guidance and outreach	1.8	4.5
Media impact of fines and regulator leadership	3.9	6.9
Perception regulator is independent of the government	4.5	5.3
Good public awareness & understanding of GDPR rights	2.7	3.4
Fines issued on a scale that deter	4.8	6.5
Number of investigations	5.1	5.1
Number of complaints	5.8	6.8
Number of fines	5.4	7.4

Table 3 shows the interview results in one column and the Menti survey results in the other. At the end of each interview, participants were asked to rank the KPIs in importance. When their votes were aggregated, they ranked business guidance as the most important evaluation KPI (which may be influenced by the business majority of the sample). The two public perception metrics combined with budgetary sufficiency were ranked collectively in second place. Separately, the Menti rankings were collected from attendees on the Mentimeter survey platform after our presentation at an information security conference. They show the two public perception KPIs as preeminent and then business guidance KPI. The slight difference in ranking may be due to the discretion interviewees took to cluster KPIs, whereas the survey platform enforced a strict individual KPI ranking on the Menti voters. It may also be due to the interviewees' freedom to discuss a topic such as budgets, whereas the conference attendees did not have that interactive option. Nonetheless, the top three KPIs are the same in both surveys.

4.5. Alternative KPIs

The two most common alternative KPI themes were regulator responsiveness and regulator accountability. Annual reports were characterised as backwards-looking:

> *"If they set forward-looking goals and targets and then had to report back on whether they achieved those. I think it would make them more accountable."* (P11)

The NGOs wanted more granular data on the pipeline of cases, the stage of each case, and the turnaround times for a decision (68; 41). They wanted transparency of the in-and-outflow balance of cases to reveal backlogs and a measure of powers exercised, such as decisions, ex officio investigations, dawn raids, and stop orders. One regulator volunteered that one KPI should be about how DPAs proactively investigate risks invisible to the common man, such as invasive ad tech or privacy-destroying AI. To counter the objection that measuring a Hidden Risks KPI may be impracticable, he suggested *"a possible proxy there would be, what about NGOs, expert organizations and bodies? How they perceive the state of play?"* (P22) as part of a stakeholder perception measure. Other ideas included having comparative benchmarks across Europe, a root cause repetition metric to measure recurring systematic violations, and a class action and civil claims metric that was an adjunct to the formal complaint metric.

5. Discussion

In this section, we will explore why the indefinable effectiveness of privacy regulators is tied up with the difficulty practitioners have in specifying the regulator's raison d'etre in the first place and how that affects their instinctual evaluations of their performance. We examine the independence and accountability conundrum that is common to many regulators and how it is made worse by the national definitional and procedural differences for a supposedly common regulation like the GDPR across Europe. We identify some basic systems and informational infrastructure that would support enhanced reporting before finally fleshing out a series of KPIs that could form the basis of a framework for individual and cross-country regulator performance assessment.

5.1. The Indefinable Effectiveness Paradox

We term it a paradox because just as the privacy paradox (82; 3) is the observed phenomenon that describes the discrepancy between users' expressed concern and actual behaviour regarding online privacy practices, our research indicates there is an analogous paradox that describes the discrepancy between the expressed objectives and the actual criteria practitioners use to

judge the effectiveness of privacy regulators. The results of RQ1 show that practitioners hold a wide spectrum of expectations of a regulator spanning the five themes but only have tangible output measures for a narrow subset of those expectations to judge them in practice (i.e. the Enforcer expectation). The results of RQ2 show practitioners revert to higher level goals when given more information and time to consider a range of KPIs. We surmise it is partly due to definitional difficulty and partly due to one's point of view. In political science, it might be characterised as "where you stand depends on where you sit".

Trying to pin down the concept of privacy has challenged philosophers and scholars for millennia (52; 80; 65). As one regulator put it *"privacy is a fluffy, immeasurable objective"* (P18), which means assessing their effectiveness is problematic if attainment resists definition. As the EDPS puts it "The notion of data protection originates from the right to privacy and both are instrumental in preserving and promoting fundamental rights and values".

Lacking well-defined objectives, practitioners ascribe goals based on their personal motivations and experience. Thus, consumers think about complaint handling, high-profile data breaches and fines, whereas business people think about the clarity of guidance they receive and the calibre of personnel they encounter at the regulator. NGOs prioritise evidence of activity and responsiveness, whereas regulators stress consumer awareness and treasure their independence.

This mismatch has practical implications for regulators around how they frame and communicate their role, prioritise their workload, and thereby demonstrate their value and effectiveness.

5.2. The Independence-Accountability Enigma

In Sections 2.3 and 2.4 we summarised the importance of protecting regulator independence. Our research confirms that the SAs believe they enjoy a high degree of autonomy and business does not see it as a concern. In the course of our interviews, we learnt firsthand of instances where regulators 'lean' on a fellow regulator at EDPB meetings if they think they are being too lenient, for example, but accountability is mainly restricted to an annual report to parliament or to an annual hearing or meeting with the government minister that has administrative responsibility. Whilst an obvious lever, politicians are careful not to be seen to use budgetary decisions as indirect accountability instruments. The EC has started to require bimonthly reports on cross-border cases (39), but that is the limit of scrutiny. Meanwhile, in June 2023, the Irish Parliament has introduced a new law (92; 72, Section 26A which modifies the 2018 DPA Act) that prohibits the disclosure of confidential information which the DPC justifies as protecting the integrity of their decision-making process but which the NGOs characterize as a gagging order (78; 67; 54). There is no provision in Section 26 that allows a third party to audit if the imposition of this new power by the DPC is proportionate or justified. In effect, GDPR regulators continue to mark their homework. Apart from longer-term court challenges, the feedback loop with society seems weak if regulators are immune from pushback.

5.3. Practical Steps to Better Accountability

In political science, it is contested that regulators generally face a legitimisation and democratic deficit problem (60). Trade-offs exist concerning the simultaneous delivery of autonomy, performance and accountability. Although we make no claim to legal expertise, two alternative sources of legitimacy emerge from our research: the positive evaluation of regulatory performance by all stakeholders (consumers, business and expert organisations) and a procedural component in formalising how GDPR regulators peer-review one another.

To enable this evaluation, one needs a level playing field. A surprising finding was that there exists no central database. At the very least, a common platform seems like a sine qua non to enable analysis. A second surprising finding was the lack of similarity in reporting styles. Harmonising the format of the DPA annual reports seems an easy win. Given our research revealed a high degree of cynicism regarding 'spin' in annual reports, there may be a role for an EU third-party to audit the data. A third surprising finding was that there exists no EU-wide agreement on what constitutes a final complaint decision nor how to account for or link cases. Harmonising definitions and registrations seem an obvious means to achieve better transparency and comparability. Knowing how many complaints are being lodged, and what occurs to them, is crucial to assess and improve GDPR enforcement. There is no shortage of ideas from NGOs and academia about how to 'fix' the problem (45; 68; 61; 41).

As regards procedural changes, administrative law and a recent legislative proposal (22; 39; 46) may address this issue. This is beyond the remit of this paper.

5.4. Practical KPIs to Measure Regulator Effectiveness

Effectiveness and efficiency are often used interchangeably. They are different. As Peter Drucker (24) put it: *"effectiveness is doing the right things, while efficiency is doing things right."* Effectiveness is about achieving strategic goals or outcomes. Efficiency is about achieving them with the minimum time, money or effort.

The regulators favoured hard metrics such as the number of complaints, investigations and fines because they are measurable and comparable from year to year (which is ironic since they are difficult to find and compare objectively by the public). The NGOs liked them because they were a tool for making comparisons and substantiating complaints against regulators they judged unresponsive. These are arguably as much a measure of efficiency as effectiveness.

Non-regulators favoured the softer metrics surrounding the public perception of improved control & understanding of rights and the business perception of clear guidance on compliant implementations. Regulators didn't like them because they were too subjective and regarded them as only having contextual significance. This may be missing the point. Article 1 of the GDPR states its objective is *"the protection of the fundamental right of natural persons and in particular their right to the protection of personal data."* The perception of stakeholders that privacy has improved and the regulation is implementable is a key desired outcome of the GDPR. Annual standardised sentiment or satisfaction surveys of both interest groups (and possibly NGOs) would reveal trends and inter-country differences without compromising the independence of regulators.

Enforcement in the form of large fines that deter and the media attention they attract were both seen as important and intertwined. Assessing whether a regulator is levying a proportionate fine amount could be related to the size of the country, industry, or non-compliant company turnover.

Assessing media impact is trickier. Different regulators carry different portfolios of responsibilities, which will impact the number of press releases they issue each year. Nevertheless, national regulators could easily identify in their annual report the number of GDPR-related press releases and the number of hits from it in the media.

Public perception could be measured by selectively borrowing marketing companies' techniques to measure brand value. For example, they use surveys and polls for quantitative analysis and focus groups and interviews for qualitative analysis. They use media analysis to monitor and analyze the coverage and sentiment of an organization in the media, and social media analysis to monitor and analyze the engagement and sentiment of an organization on social media platforms. All of these methods can help measure awareness, attitudes, opinions, satisfaction, behaviour, perceptions, motivations, emotions, experiences, likes, shares, comments, mentions, reviews, and ratings related to an organization. Obviously, the key challenge would be ensuring standardizing them for trans-European comparison purposes.

The budget KPI is an enabler. Regulators are not shy about complaining that they lack sufficient resources. A method to judge if their special pleading is justified would be to accompany their finances with comparable standardised benchmarks with other countries: the number of investigators, lawyers, and IT staff, for example.

The independence of a regulator from its government is a KPI that participants do not consider a priority at present. In the UK, there is a new data bill going through parliament. How far that will compromise its independence and imperil the UK's adequacy status is a subject of debate (56).

Taken together, a standardised set of KPIs and standardised annual reports would significantly improve organisational learning, transparency, accountability, comparability and legitimacy of regulators.

5.5. Limitations & Future Work

Most of the participants interviewed and surveyed were based in the UK, whereas the regulators were drawn from across Europe and did not include the UK regulator (who declined the invitation). The UK is no longer in the EU, but the EU deems its GDPR to have an equivalent adequacy status. The lead GDPR regulator, the Irish DPC, also declined to participate. Taken together, these three factors may affect the generalizability of the findings. In mitigation, while the business interviewees were heavily drawn from the UK (apart from one Irish company), all the regulators and NGOs had an international perspective, and most of the CISOs and executives worked in multinational companies with EU-based offices. Future work would benefit from a larger sample of interviewees and regulators Europe-wide. A logical next step would be to put numbers to the KPIs with the cooperation of the national regulators to enable in-country analysis and cross-country comparison.

6. Conclusion

Data protection regulations like the GDPR are increasingly important in securing individuals' privacy as society goes digital. The success of any regulation, however good, ultimately depends on how well it is executed. Existing literature fails to answer what good execution means in this context. We research what practitioners think are the objectives of data protection and privacy regulators and how they evaluate their effectiveness. We also explore novel methods for systematically assessing regulator performance in the future. Our findings indicate there is a gap between how practitioners judge regulators day to day and how they judge them when given a chance to discuss it in the round. The contrast between participants' initial criteria and their later ranking of the KPIs confirms this gap. Perception of the regulator's effectiveness is subjective, sanctions-focused and influenced by one's role and responsibilities. Regulators are designed to be independent of short-term political interference, but this raises serious questions of longer-term accountability. We examine the historical, cultural and organisational motivations behind the current byzantine complexity of the GDPR regime. Lastly, we contribute a series of key performance indicators and make structural suggestions around centralised and standardised reporting of cases to deliver improved learning, legitimacy, transparency and comparability. We believe our findings have important implications for the future development of regulator assessment and accountability in Europe and GDPR-like regimes outside Europe.

Funding statement

Gerard Buckley is supported by UK EPSRC grant no. EP/S022503/1. Ingolf Becker is supported by UK EPSRC grant no. EP/W032368/1. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Kenneth W. Abbott and Duncan Snidal. Hard and Soft Law in International Governance. *International Organization*, 54(3):421–456, 2000. Publisher: [MIT Press, University of Wisconsin Press, Cambridge University Press, International Organization Foundation]. URL: `https://www.jstor.org/stable/2601340`.
2. Kenneth W. Abbott and Duncan Snidal. Taking responsive regulation transnational: Strategies for international organizations. *Regulation & Governance*, 7(1):95–113, 2013. `doi:10.1111/j.1748-5991.2012.01167.x`.

3. Alessandro Acquisti. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce*, pages 21–29, New York NY USA, May 2004. ACM. doi:10.1145/988772.988777.
4. Ian Ayres and John Braithwaite. *Responsive Regulation: Transcending the Deregulation Debate*. Oxford University Press, 1992.
5. Robert Baldwin, Martin Cave, and Martin Lodge. *Understanding regulation: theory, strategy, and practice*. Oxford University Press, New York, 2nd ed edition, 2012.
6. Marcus Banks. *Using Visual Data in Qualitative Research*. SAGE, September 2018.
7. Jeb Barnes and Thomas F. Burke. Making Way: Legal Mobilization, Organizational Response, and Wheelchair Access. *Law & Society Review*, 46(1):167–198, 2012. doi:10.1111/j.1540-5893.2012.00476.x.
8. Kathleen Bawn. Political Control Versus Expertise: Congressional Choices about Administrative Procedures. *American Political Science Review*, 89(1):62–73, March 1995. Publisher: Cambridge University Press. doi:10.2307/2083075.
9. Kathleen Bawn. Choosing Strategies to Control the Bureaucracy: Statutory Constraints, Oversight, and the Committee System. *The Journal of Law, Economics, and Organization*, 13(1):101–126, April 1997. doi:10.1093/oxfordjournals.jleo.a023375.
10. Julia Black and Smith Dimity Kingsford. Critical reflections on regulation [Plus a reply by Dimity Kingsford Smith.]. *Australasian Journal of Legal Philosophy*, 27(2002):1–46, 2002. Publisher: Copyright Agency. doi:10.3316/ielapa.200206927.
11. Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, January 2006. doi:10.1191/1478088706qp063oa.
12. Virginia Braun and Victoria Clarke. One size fits all? what counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology*, 18(3):328–352, 2021. doi:10.1080/14780887.2020.1769238.
13. Stephen Breyer. *Regulation and Its Reform*. Harvard University Press, 1982.
14. Gerard Buckley, Tristan Caulfield, and Ingolf Becker. Gdpr: Is it worth it? perceptions of workers who have experienced its implementation, 2024. arXiv:2405.10225.
15. 1 Senat Bundesverfassungsgericht. Federal Constitutional Court - Decisions - On the constitutionality of the 1983 Census Act, December 1983. Archive Location: de Publisher: Bundesverfassungsgericht. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html.
16. Lee A. Bygrave. Data Protection Law. *Data Protection Law*, pages 1–458, 2002. Publisher: Wolters Kluwer. URL: https://www.torrossa.com/en/resources/an/5392241.
17. Daniel Carpenter. The Political Foundations of Bureaucratic Autonomy: A Response to Kernell. *Studies in American Political Development*, 15(1):113–122, 2001. Publisher: Cambridge University Press. doi:10.1017/S0898588X01010069.
18. Daniel P. Carpenter and George A. Krause. Reputation and Public Administration. *Public Administration Review*, 72(1):26–32, 2012. doi:10.1111/j.1540-6210.2011.02506.x.
19. CMS Germany. GDPR Enforcement Tracker - list of GDPR fines, May 2023. URL: https://www.enforcementtracker.com.
20. Cary Coglianese. Measuring Regulatory Performance: Evaluating the impact of regulation and regulatory policy. Technical report, OECD, 2012. URL: https://www.oecd.org/regreform/regulatory-policy/1_coglianese%20web.pdf.
21. Cary Coglianese and David Lazer. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals. *Law & Society Review*, 37(4):691–730, 2003. doi:10.1046/j.0023-9216.2003.03703001.x.
22. Dan Cooper, Anna Meneses, and Sam Choi. European Commission Plans to Improve Cooperation Between Supervisory Authorities in Cross-Border GDPR Cases, February 2023. URL: https://www.insideprivacy.com/gdpr/european-commission-plans-to-improve-cooperation-between-supervisory-authorities-in-cross-border-gdpr-cases/.
23. DPC. Data Protection Commission Annual Report 2022, March 2023. URL: https://www.dataprotection.ie/sites/default/files/uploads/2023-03/DPC%20AR%20English_web.pdf.
24. Peter F. Drucker. *The effective executive: the definitive guide to getting the right things done*. Harper Business, New York, NY, 1967.
25. EDPB. Report 2021 Overview on resources and enforcement. Technical report, August 2021. URL: https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf.
26. EDPB. Report 2022 Overview on resources and enforcement. Technical report, September 2022. URL: https://edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstatestosas2022_en.pdf.
27. EO. Decision on whether the European Commission collects sufficient information to monitor Ireland's implementation of the EU's General Data Protection Regulation (GDPR) (Case 97/2022/PB) | Decision | European Ombudsman, December 2022. URL: https://www.ombudsman.europa.eu/en/decision/en/164337.
28. Equality and Human Right Commission. What is the European Convention on Human Rights? | Equality and Human Rights Commission, April 2017. URL: https://www.equalityhumanrights.com/en/what-european-convention-human-rights.
29. Equality and Human Right Commission. Article 8: Respect for your private and family life | Equality and Human Rights Commission, June 2021. URL: https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life.
30. EU. Art. 1 GDPR – Subject-matter and objectives, May 2018. URL: https://gdpr-info.eu/art-1-gdpr/.
31. EU. Art. 51 GDPR – Supervisory authority, May 2018. URL: https://gdpr-info.eu/art-51-gdpr/.
32. EU. Art. 52 GDPR – Independence, May 2018. URL: https://gdpr-info.eu/art-52-gdpr/.
33. EU. Art. 57 GDPR – Tasks, May 2018. URL: https://gdpr-info.eu/art-57-gdpr/.
34. EU. Art. 58 GDPR – Powers, May 2018. URL: https://gdpr-info.eu/art-58-gdpr/.
35. EU. Art. 59 GDPR – Activity reports, May 2018. URL: https://gdpr-info.eu/art-59-gdpr/.
36. EU. Art. 68 GDPR – European Data Protection Board, May 2018. URL: https://gdpr-info.eu/art-68-gdpr/.
37. EU. General Data Protection Regulation (GDPR) – Official Legal Text, May 2018. URL: https://gdpr-info.eu/.

38. European Commission. General Data Protection Regulation one year on. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2956.
39. European Commission. Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation - Have your say, March 2023. URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en.
40. European Data Protection Board. EDPB Work Programme 2023/2024, February 2023. URL: https://edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf.
41. European Digital Rights. EDRI LETER TO EDPB, September 2022. URL: https://noyb.eu/sites/default/files/2022-09/EDRI_LETER_TO_EDPB.pdf.
42. European Union. Data Protection Directive. *Official Journal L 281 , 23/11/1995 P. 0031 - 0050;*, November 1995. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3AEN%3AHTML.
43. European Union. Charter of Fundamental Rights of the European Union (2000/C 364/01), December 2000. URL: https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
44. Gloria González Fuster. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer Science & Business, April 2014.
45. Gloria González Fuster, Jef Ausloos, Damian Bons, Lee A Bygrave, Laura Drechsler, Olga Gkotsopoulou, Christopher Hristov, Kristina Irion, Charlotte Kroese, Orla Lynskey, and Maria Magierska. The right to lodge a data protection complaint: ok, but then what?: an empirical study of current practices under the GDPR. *European University Institute*, June 2022. URL: https://cadmus.eui.eu/bitstream/handle/1814/74899/The_right_to_lodge_a_data_protection_complaint_2022.pdf?sequence=1&isAllowed=y.
46. Giulia Gentile and Orla Lynskey. Deficient by design? the transnational enforcement of the GDPR. *International & Comparative Law Quarterly*, 71(4):799–830, October 2022. Publisher: Cambridge University Press. doi:10.1017/S0020589322000355.
47. Fabrizio Gilardi. Policy credibility and delegation to independent regulatory agencies: a comparative empirical analysis. *Journal of European Public Policy*, 9(6):873–893, January 2002. doi:10.1080/1350176022000046409.
48. William T. Gormley. Regulatory Issue Networks in a Federal System. *Polity*, 18(4):595–620, June 1986. Publisher: The University of Chicago Press. doi:10.2307/3234884.
49. Greg Guest, Kathleen M. MacQueen, and Emily E. Namey. *Applied Thematic Analysis*. SAGE Publications, October 2011.
50. Neil Gunningham, Robert A. Kagan, and Dorothy Thornton. Social License and Environmental Protection: Why Businesses Go Beyond Compliance. *Law & Social Inquiry*, 29(2):307–341, 2004. doi:10.1111/j.1747-4469.2004.tb00338.x.
51. Robert W. Hahn and Patrick M. Dudley. How Well Does the Government Do Cost-Benefit Analysis?, January 2004. doi:10.2139/ssrn.495462.
52. Jan Holvast. History of privacy. In Karl De Leeuw and Jan Bergstra, editors, *The History of Information Security*, pages 737–769. Elsevier Science B.V., Amsterdam, January 2007. doi:10.1016/B978-044451608-4/50028-6.
53. Information Commissioners Office. The public interest test, May 2023. Publisher: ICO. URL: https://ico.org.uk/for-organisations/foi-eir-and-access-to-information/freedom-of-information-and-environmental-information-regulations/the-public-interest-test/.
54. Amnesty International. Ireland: Draconian law to make data protection procedures confidential, June 2023. URL: https://www.amnesty.org/en/latest/news/2023/06/ireland-draconian-law-to-make-data-protection-procedures-confidential/.
55. Irish Council for Civil Liberties. 5-years: GDPR's crisis point. Technical report, 2023. URL: https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf.
56. Johnny Ryan. Ryan to Reynders re UK adequacy, 2023. URL: https://www.iccl.ie/wp-content/uploads/2023/05/Ryan-to-Reynders-re-UK-adequacy.pdf.
57. Paul L. Joskow and Nancy L. Rose. Chapter 25 The effects of economic regulation. In *Handbook of Industrial Organization*, volume 2, pages 1449–1506. Elsevier, January 1989. doi:10.1016/S1573-448X(89)02013-3.
58. Philip Keefer and David Stasavage. Checks and Balances, Private Information, and the Credibility of Monetary Commitments. *International Organization*, 56(4):751–774, 2002. Publisher: Cambridge University Press. doi:10.1162/002081802760403766.
59. Natasha Lomas. Big changes coming for GDPR enforcement on Big Tech in Europe? *TechCrunch*, January 2023. URL: https://techcrunch.com/2023/01/31/gdpr-enforcement-reform-dpa-oversight/.
60. Martino Maggetti. Legitimacy and Accountability of Independent Regulatory Agencies: A Critical Review. November 2010. URL: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/cis-dam/CIS_DAM_2015/WorkingPapers/Living_Reviews_Democracy/Maggetti.pdf.
61. Estelle Masse. Four Years Under The EU GDPR: How To Fix Its Enforcement. Technical report, 2022. URL: https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-4-year-report-2022.pdf.
62. Mitnick, Barry M. *The political economy of regulation: Creating, designing, and removing regulatory forms*. New York: Columbia University Press, 1980.
63. National Audit Office. Performance measurement by regulators. Technical report, November 2016. URL: https://www.nao.org.uk/wp-content/uploads/2016/11/Performance-measurement-by-regulators.pdf.
64. National Audit Office. Good practice guidance Principles of effective regulation. *Design*, May 2021.
65. Helen Nissenbaum. Privacy in Context: Technology, Policy, and the Integrity of Social Life. In *Privacy in Context*. Stanford University Press, November 2009. doi:10.1515/9780804772891.
66. NOYB. GDPRhub, June 2023. URL: https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub.
67. noyb. Ireland: Corrupt GDPR procedures now "confidential", June 2023. URL: https://noyb.eu/en/ireland-corrupt-gdpr-procedures-now-confidential.

68. nyob. Data Protection Day: 41 Years of "Compliance on Paper"?!, January 2022. URL: https://noyb.eu/en/data-protection-day-41-years-compliance-paper.
69. OECD. Setting the scene: The importance of regulatory policy. Technical report, OECD, Paris, November 2011. doi:10.1787/9789264116573-4-en.
70. Anthony Ogus. *Comparing regulatory systems: institutions, processes and legal forms in industrialised countries*. Edward Elgar Publishing, 2004. URL: https://www.elgaronline.com/display/9781843764823.00016.xml.
71. Anthony I. Ogus. *Regulation: Legal Form and Economic Theory*. Bloomsbury Publishing, October 2004.
72. Houses of the Oireachtas. Courts and Civil Law (Miscellaneous Provisions) Bill 2022: From the Seanad – Dáil Éireann (33rd Dáil) – Wednesday, 28 Jun 2023 – Houses of the Oireachtas, June 2023. URL: https://www.oireachtas.ie/en/debates/debate/dail/2023-06-28/26.
73. Matthew Potoski and Aseem Prakash. The Regulation Dilemma: Cooperation and Conflict in Environmental Governance. *Public Administration Review*, 64(2):152–163, 2004. doi:10.1111/j.1540-6210.2004.00357.x.
74. Randall L. Calvert, Mathew D. McCubbins, and Barry R. Weingast. A Theory of Political Control and Agency Discretion. August 1989. URL: https://www.jstor.org/stable/211F1064.
75. Antoinette Rouvroy and Yves Poullet. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. pages 45–76. January 2009. doi:10.1007/978-1-4020-9498-9_2.
76. Gery W. Ryan and H. Russell Bernard. Techniques to Identify Themes. *Field Methods*, 15(1):85–109, February 2003. Publisher: SAGE Publications Inc. doi:10.1177/1525822X02239569.
77. Johnny Ryan. ICCL launches European Ombudsman complaint against European Commission's failure to take Ireland to court over the GDPR., November 2021. URL: https://www.iccl.ie/news/iccl-launches-european-ombudsman-complaint-against-european-commissions-failure-to-take-ireland-to-court-over-the-gdpr/.
78. Paul Sawers. Irish government criticized over proposed law-change that would 'muzzle' Big Tech critics, June 2023. URL: https://techcrunch.com/2023/06/26/ireland-big-tech-gdpr-dpc-critics/.
79. John T. Scholz. Voluntary Compliance and Regulatory Enforcement. *Law & Policy*, 6(4):385–404, October 1984. doi:10.1111/j.1467-9930.1984.tb00334.x.
80. Daniel J. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3):477–564, 2006. doi:10.2307/40041279.
81. David B. Spence. Administrative Law and Agency Policy-Making: Rethinking the Positive Theory of Political Control. *Yale Journal on Regulation*, 14(2):407–450, 1997. URL: https://heinonline.org/HOL/P?h=hein.journals/yjor14&i=413.
82. Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 38–47, Tampa Florida USA, October 2001. ACM. doi:10.1145/501158.501163.
83. Jonas Tallberg. Paths to Compliance: Enforcement, Management, and the European Union. *International Organization*, 56(3):609–643, 2002. doi:10.1162/002081802760199908.
84. The Information Commissioners Office. ICO Annual report 2021-2022, July 2022. URL: https://ico.org.uk/media/about-the-ico/documents/4021039/ico-annual-report-2021-22.pdf.
85. The Irish Data Protection Commission. Data Protection Commission AR 2021. Technical report, February 2022. URL: https://www.dataprotection.ie/sites/default/files/uploads/2022-02/Data%20Protection%20Commision%20AR%202021%20English%20FINAL_0.pdf.
86. Brendan Van Alsenoy. Data Protection Law in the EU: Roles, Responsibilities and Liability. *Journal of Data Protection & Privacy*, 3(1):113–115, 2019. URL: https://econpapers.repec.org/article/azajdpp00/y_3a2019_3av_3a3_3ai_3a1_3ap_3a113-115.htm.
87. Geoff Walsham. Doing interpretive research. *European Journal of Information Systems*, 15(3):320–330, June 2006. doi:10.1057/palgrave.ejis.3000589.
88. Wikipedia. Informational self-determination, November 2022. Page Version ID: 1119834086. URL: https://en.wikipedia.org/w/index.php?title=Informational_self-determination&oldid=1119834086.
89. William Bernhard. A Political Explanation of Variations in Central Bank Independence | American Political Science Review | Cambridge Core, May 1998. URL: https://www.cambridge.org/core/journals/american-political-science-review/article/political-explanation-of-variations-in-central-bank-independence/DAE8837A0A6FC400EE483BF9392E868C.
90. Michael Williams and Tami Moser. The Art of Coding and Thematic Exploration in Qualitative Research. *International Management Review*, 15(1):45–55,71–72, 2019. Num Pages: 45-55,71-72 Place: Marietta, United States Publisher: American Scholars Press, Inc. URL: https://www.proquest.com/docview/2210886420/abstract/E00F3EF3D7CD4724PQ/1.
91. Shoshana Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019*. Profile Books, January 2019.
92. SEANAD ÉIREANN. COURTS AND CIVIL LAW (MISCELLANEOUS PROVISIONS) BILL 2022, June 2023. URL: https://data.oireachtas.ie/ie/oireachtas/bill/2022/84/seanad/3/amendment/numberedList/eng/b84b22d-scnl.pdf.

A. Codebook

The following tables show the codebook grouped by theme.

Table 4. Codes in the Cynical View theme

Appear to be in Control
Bad Manners to judge judges
Cases trump Investigations
Complexity of inconsistent systems
Cost Budget
Credibility of Regulator Authority
Cross Border cases are not that important
Decisions that stand up in Court
Duplicitous annual Reports
Fight it up to ECJ
Fines bad measure
Futile
Lack of central database
Lawyers act for plaintiffs
Never thought about it
Numbers only tell half the story
Perceptions are not enough
Scrutiny by court
Scrutiny by Gov
Success =Low or No Breaches
Success =Low number of fines
Success =No spam no cold calls
Success =No fines
Terminology complexity
Transparency
Transparency of Annual Reports
CNIL v Spanish v Irish
Data is not safer
Rubbish DPA Reports
Rubbish EDPB Reports
Compliance Theatre
Organisational agenda
Outcomes v Resources
Personal agenda of staff
Procedural v Substantive
Secretive behaviour

Table 5. Codes in the Lofty View theme

Accessible
Accountable
Appreciate value of data
Comparative benchmarks
Change Agents
Depends on Regulation Objectives
Leadership
Learning organisation
Metrics
View NGOs as helpers
Overall Compliance
Individual v corporate perspective
Proportionate
Reg Tech
Stakeholder Balance
Vision
A focus on fines is wrong
Global importance
Promote priority in companies
Spur to action
Behaviour change
Correct market failure
Create Trust
Individual Responsibility
Make the rules for everybody

Table 6. Codes in the Protector theme

Complaint Handling
Educate
NGOs as assessors
Number of complaints
Number of Decisions
Number of DPOs in country
Number of opinions followed by Legislators
Powers Used metric
Success=Nyob Metrics
Consumer Individual Orientated
Educate
Public Awareness
Empowerment of the Consumer
Investigate Complaints
Protect Privacy

Table 7. Codes in the Enforcer theme

Business Support
Business Guidence
Not a balance of Equals
Enforcement
Fines: Punishment
Fines: Counterproductive
Fines: Go after parent company
Fines: Graded in severity
Fines: Public Relations
Fines: Can be a pro-business PR-weapon
Fines: Sanction power
Fines: Sin of commission v omission
Investigations
Media impact
Monitoring
Pace of decision making
Stop Order
Compliance with Regs & Rules
Drive-up Accountability Responsibility Integrity
Drive-up & maintain standards
Investigate Data Breaches
Reputational Impact
Useful Stick

Table 8. Codes in the Guide theme

Business Communications
Business Support & Guidence
Breach Reports are useful
Case studies are useful
Certainty
Collaborative
Credible Staff
Good website
Relationships with Business
Victim or Villain
Partner
Educate Business
Raise Awareness
Obfuscation
Poor Guidance

Table 9. Interview Protocol

Participant information sheet check, Consent check, recording check.	
Double-check that the interviewee is familiar with the GDPR and has had some involvement with DPAs.	
1	What are the objectives of a GDPR privacy regulator?
2	You said the objectives were X, Y, and Z. Taking each in turn, what criteria do you use to judge their effectiveness in achieving those objectives? Ask
Imagine you are doing a DPA's annual performance review.	
Here are 10 KPIs with which to evaluate them.	
3	What do you think of each KPI 1 to 10?
4	How would you rank the KPIs in terms of importance and why?
5	Would you amalgamate or drop some KPIs?
6	If you took off your (business/regulator) hat, would that change your opinion of their importance? Why?
7	Can you think of alternative KPIs?