Centre for Information Policy Leadership
Hunton & Williams LLP

Regulating for Results

Strategies and Priorities for Leadership and Engagement

A Discussion Paper

25 September 2017

Contents

Ten Discussion Topics

Introduction & Summary

1. **The Purpose and Nature of This Paper**
    - **a. Benefits for Individuals**
    - **b. Benefits for DPAs**
    - **c. Benefits for Regulatees**
    - **d. Global Generally, Europe Specifically**
2. **The Functions of Data Protection Authorities**
3. **Meagre DPA Resources**
    - **a. Level of Resources**
    - **b. Additional Resources?**
4. **Effective Regulation**
    - **a. Key Themes**
    - **b. Law and Corporate Behaviour**
    - **c. Conclusions From Other Spheres of Regulation**
5. **A Results-based Approach for Regulating Data Protection**
    - **a. Effectiveness**
    - **b. Setting Strategic Priorities**
    - **c. Leadership and Engagement**
    - **d. Police Officer**
    - **e. Complaint-Handler**
    - **f. Authoriser**
6. **Constructive Engagement in Practice**
7. **Principles for a Results-based Approach**
8. **Possible Problems**
    - **a. Reluctance to Relegate Functions**
    - **b. Regulatory Capture**
    - **c. Regulatee Resistance**

Annex A – DPA Functions Under GDPR

Annex B – DPA Resources

Annex C – Basic Conclusions From "Law and Corporate Behaviour"

Annex D – First Draft of a Possible Protocol

Bibliography

Ten Questions for Discussion

"Regulating for Results" involves making difficult, but essential, choices about strategies and priorities. Data Protection Authorities (DPAs) simply cannot do everything, so strategic decisions are needed about what works best.

1. When the challenges and expectations of the digital age are so great—and especially when resources are limited—what are the most promising ways for DPAs (independently and with others) to ensure that the regulation of data protection will produce the best results?

2. Which ways should be explored for increasing DPA budgets to more realistic levels?

3. What can be learned from approaches which have been adopted around the world in many other spheres of regulation?

4. Can effectiveness be elaborated in terms of enabling people to flourish with dignity and autonomy in a digital world where unacceptable data uses which impair their privacy are prevented?

5. When the responsibilities of most DPAs are so numerous, what are the best ways to achieve overall effectiveness?

6. Does the Results-based Approach offer helpful ways to set strategic priorities and balance engagement, enforcement and complaint-handling?

7. Is it right to give top strategic priority to Leadership functions with strong emphasis on constructive engagement with regulated organisations?

8. What activities and techniques best promote constructive engagement in practice?

9. Will the bodies bringing DPAs together globally, regionally and operationally consider adopting the suggested Principles for a Results-based Approach?

10. How can the suggested Principles be improved?

Regulating for Results – Strategies and Priorities for Leadership and Engagement

Introduction & Summary

The ecosystem for regulating data protection and privacy is changing rapidly, and not just within the EU. For many years CIPL has championed the role of accountable organisations and the merits of a risk-based approach. We now turn to the "plumbing" of the system as a whole and consider how its component parts can best fit together.

The aim of this paper in particular is to stimulate discussion about how Data Protection Authorities[1] (DPAs) can maximise their effectiveness in the modern information age.

When functions are numerous, expectations are high and resources are limited. This paper asks whether and how conscious efforts should be made for the regulation[2] of data protection to become more "results-based". This involves making difficult, but essential, choices about strategies and priorities. DPAs simply cannot do everything.

The Results-based Approach is used by CIPL to mean DPAs—independently and co-operatively—maximising their effectiveness by adopting modern and strategic approaches to regulation that achieve best outcomes for the individuals, society and regulated organisations. In particular, this involves responsively engaging with, and supporting, those organisations, both in the private and public sectors, which are seeking to "get it right" while also dealing firmly with those who are not trying.

This paper suggests some high-level Principles to provide the foundation for a Results-based Approach. The Principles are intended to inform the setting of strategic priorities, including ranking different types of function, selecting the most appropriate tools and targeting particular sectors, activities or organisations.

Principles for a Results-based Approach

- Regulating for Results in the Digital World requires independent Data Protection Authorities (DPAs) to be strategic, effective, co-ordinated and transparent.
- The goal of a DPA should be to produce cost-effective outcomes, which effectively protect individuals in practice, promote responsible data use and facilitate prosperity and innovation.
- DPAs should give top priority to securing protection for individuals.

[1] "Data Protection Authorities", as used in this paper, equates to membership of the International Conference of Data Protection and Privacy Commissioners.
[2] "Regulation" is used in this paper in the sense of "control" or "supervision".

- Each independent DPA should be accountable for transparently spelling out the particular outcomes it is seeking and the priorities and approaches it will be adopting to achieve those outcomes in its regulatory work.

- The strategies of all DPAs should be as co-ordinated, consistent and complementary as possible.

- DPAs should treat regulated organisations in a consistent manner—adopting similar approaches across and within sectors, irrespective of the type or geographical reach of the organisation.

- Each DPA should adopt a risk-based approach to all its activities, basing priorities on conduct that creates the most harm to individuals or to democratic and social values.

- An approach of constructive engagement with the emphasis on leadership, information, advice, dialogue and support will be more effective than sole and excessive reliance upon deterrence and punishment.

- Emphasis on information and advice is especially important in the field of data protection, due to its broad impact on so many organisations and the nature of the requirements that are either not precise or are context driven, requiring judgement in individual cases.

- Open and constructive relationships with organisations handling personal information, based on honest dialogue and mutual co-operation, but without blurred responsibilities, will improve overall compliance outcomes.

- Regulated organisations should be assessed in particular by reference to demonstrable good faith and due diligence in their efforts to comply.

- Organisations trying to behave responsibly and to “get it right” should be encouraged to identify themselves, for example by transparently demonstrating their accountability, their privacy and risk management programmes, the influence of their DPOs and their use of seal / certification programmes, BCRs, CBPR and other accountability frameworks.

- Punitive sanctions should be mainly targeted on non-compliant activity that is deliberate, wilful, seriously negligent, repeated or particularly serious.

- Though the need to deal with individual complaints can be an important component of protecting individuals, handling high volumes is very resource-intensive and can impede wider strategic goals. Complaints should be tightly managed with clear criteria to determine the extent of investigation, also taking into account that complaints are a valuable source of intelligence.

The primary objective of this paper is to stimulate discussion within the data protection and privacy community (including regulators, regulated organisations, civil society, academics and experts).

While this paper seeks to provide insight on what a Results-based Approach for Data Protection might look like in practice, ultimately, it must be for the DPA community itself to decide whether and how it wishes to take this thinking forward. If the substance of these Principles is broadly acceptable, it is envisaged that a revised version could be adopted, promulgated and put into practice at four levels:

- Globally, by the International Conference of Data Protection and Privacy Commissioners (ICDPPC).[3] A suitable target date might be the 40th International Conference, which will take place in Brussels in October 2018.
- At EU level, by the European Data Protection Board.
- At Asia-Pacific level by the Asia-Pacific Privacy Authorities forum (APPA).
- At the operational level, by the Global Privacy Enforcement Network (GPEN) and the APEC Cross-border Privacy Enforcement Arrangement (CPEA).[4]

Structure of This Paper

Section 1 elaborates the purpose and nature of the paper, emphasising the need for a strategic approach to setting priorities which will deliver the best results. The section sets out the potential benefits for individuals, DPAs and regulatees. The paper is intended to be helpful for all DPAs globally, not least in encouraging maximum consistency for a global digital economy. There is a particular focus on the European Union where the GDPR will bring significant changes in the way EU DPAs work individually and together.

Section 2 examines the numerous functions placed upon the shoulders of DPAs by particular reference to those prescribed by the GDPR. From May 2018 this will shine an unprecedented spotlight upon DPAs across Europe. The GDPR envisages some 22 separate "tasks" and some 27 separate powers, but without a sense of strategic mission. To assist the dynamics of prioritisation, the functions have been grouped by reference to four types:

1. **"Leader"** – the functions which rely upon the expertise, authority and support of and information from the DPA;
2. **"Police Officer"** – where enforcement is available for infringement, especially deliberate or wilful non-compliance;
3. **"Complaint-Handler"** – where complaints may lead directly or indirectly to a sanction or to redress;

[3] www.icdppc.org.
[4] The CPEA, available at http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf, is an enforcement co-operation MOU for APEC-based privacy authorities. It envisions, among other things, that the participating authorities may prioritise their enforcement actions, both individually and collectively. *See* CPEA at Section 9.2.

4. **"Authoriser"** – where some form of prior authorisation is needed from the DPA.

Section 3 illustrates the meagreness of resources available to DPAs. Taking the EU as an example, some 26 million enterprises fall within the jurisdiction of EU DPAs. The latest comparable figures show that the budgets for DPAs in 26 EU countries averaged less than €0.41 per citizen and about €8 per business. Another study shows that only 9 of 19 DPAs had more than 40 full-time equivalent staff and six had fewer than 30 staff. The section concludes with a call for increased DPA budgets, suggesting that simply charging an annual fee of just €20 from each regulated entity in the EU could raise at least €500 million for EU DPAs.

Section 4 distils the evidence about effective regulation in other regulatory spheres. This draws heavily upon a range of recent studies, notably Prof Christopher Hodges's work on *Law and Corporate Behaviour*[5] which is a comprehensive survey of modern approaches to regulation, enforcement, compliance and ethics. It stresses that the optimum outcome for any regulatory system is to produce acceptable behaviour and to stop unacceptable behaviour. In practical terms, effective regulation means securing maximum compliance. Most organisations seek to "get it right" by complying with their responsibilities. This means that if regulators are serious about being effective, they must prioritise their support functions, with open and constructive relationships between regulators and those they regulate. Deterrence and punishment have limited effectiveness and should be targeted primarily against those who are deliberately or wilfully breaking the law.

Section 5 is the core of this discussion paper, seeking to apply these lessons to the regulation of privacy and data protection. It discusses what is actually meant by effectiveness and results. It suggests that, going beyond mere compliance with formal requirements, regulating data protection means aiming for a digital world where people flourish with dignity as autonomous individuals. The overall results which are sought could thus be developed on the following lines:

- The prevention of data uses which impair the quality of life for individuals by denying them the privacy to which they are entitled; and
- The promotion of a society where a good quality of life for individuals flows from genuine and widespread privacy where the use of data in a digital world is both universal and popular.

The section spells out, in the context of increasing functions and meagre resources, the need for strategic DPA priorities which pursue these outcomes. Although there is considerable overlapping, the four main types of function are grouped together and relate to the four main regulatory goals: **Predict - Prevent - Detect - Enforce**. The concept of a Results-based Approach for Data Protection is developed from this analysis and from evidence from other regulatory spheres. It is suggested in

[5] https://www.bloomsbury.com/in/law-and-corporate-behaviour-9781782255826/.

particular that the **Leadership** role, with maximum dialogue and **Constructive Engagement** with regulated entities, should be the top priority.

Section 6 outlines what Constructive Engagement means in practice and gives examples of activities and techniques which are likely to produce the best results. Emphasis is placed on transparency, consultation, frank exchanges and exploiting the tendency ("herd instinct") of organisations to follow the leader of the pack and peer and competition pressure.

Section 7 sets out a first draft of suggested Principles for a Results-based Approach and suggests how (after full debate and revision) they might be adopted and promulgated.

Section 8 addresses possible problems with the suggested approach. It answers concerns about the consequences of having to treat some functions with low priority, the risks of "regulatory capture" and fears that some regulatees may be reluctant to get too close to their regulators.

Questions for Discussion

This is a discussion paper. Therefore, key questions have been raised at the end of relevant sections. CIPL anticipates that, in due course, it will put these ten questions in open letters to the leaders of the International Conference, the Article 29 Working Party (WP29) / EDPB, the APPA forum, GPEN and the CPEA. For convenience the Ten Questions for Discussion are drawn together on page 4 above.

Acknowledgements

This discussion paper has developed as a dynamic process and its questions mean that many answers are still sought. Numerous people—including many currently and previously serving in a DPA capacity—have made contributions which have significantly improved the paper. Special mention must be made of the Secretariat of the International Conference of Data Protection and Privacy Commissioners for making available resource data from its recent DPA census.

DPA, industry and academic participants at the workshop which CIPL hosted in Dublin in June 2017 to review a draft of this paper agreed on the importance of this subject and also made invaluable suggestions, particularly articulating what "Constructive Engagement" looks like in practice.

CIPL is immensely grateful to everyone who has helped so willingly with this project.

1. The Purpose and Nature of This Paper

Data protection finds itself at a crossroads. With the fourth industrial revolution[6] and rapidly evolving information practices, as well as the new generation of data privacy laws and regulation, including the EU GDPR, the stakes have never been higher.

Each independent Data Protection Authority (DPA) has a crucial role to play in making a reality of data protection. Sometimes, however, the overall role of DPAs and their specific functions are taken for granted without much detailed analysis about how they should be discharged in practice.

The purpose of this discussion paper is to raise questions about how—in the face of numerous challenges and high expectations—the effectiveness of the regulatory framework can be maximised. It does this by seeking responses to a Results-based Approach in line with developments which have taken place in many other spheres of regulation. This involves adopting a strategic approach to setting priorities which will deliver the best results.

The full meaning and nature of a Results-based Approach for Data Protection are elaborated below. But first, setting out the benefits which this discussion is seeking is helpful. These can be grouped as follows:

a. Benefits for Individuals

The basic aim of data protection regulation must be to protect individuals whilst facilitating the free flow of data.[7] Data protection regulation promotes the trust which is essential for digital progress and growth, data innovation and beneficial data use.

The EU approach, and that of a number of other jurisdictions, expresses this in terms of upholding fundamental rights and freedoms. Elsewhere, the aim is seen more in terms of preventing harm to individuals. In all cases, there is also a wider "social good" context. Whatever language is used, any regulatory framework should give top priority to securing protection for people.

Any regulatory framework must be effective and effectiveness must be primarily assessed in terms of the impact on individuals. Are they being protected in practice, not just on paper? Are they getting the benefits to which they are entitled? Are people—consumers, citizens, employees—able to take maximum advantage of the digital society with confidence that their interests are being properly safeguarded? Can they expect that organisations will in reality handle their personal information correctly?

[6] As understood by the World Economic Forum.
[7] The European Court of Justice requires DPAs to establish "a fair balance between the protection of the right to private life and the free movement of personal data." (Case C-518/07 – para 30).

There are also balances to be drawn in terms of sensitivities to the needs and wishes of individuals when dealing with both commercial and public bodies. People generally do not have the power, knowledge or capability to safeguard their interests entirely by themselves. But the characteristics, attitudes and preferences of individuals vary considerably and the presumption must be that they should be the best judges of their own interests. Also, market and peer / competitor pressures can have a major impact on organisational reputations and behaviours. Any regulatory body must take great care to avoid suggesting that it "knows best" when it comes to deciding peoples' best interests. A modern approach gives precedence to protecting and empowering individuals, but does not patronise or disempower them.[8]

A focus on people is also vital for communicating in plain language with the media with the explicit aim of promoting public awareness and building popular support for data protection activities.[9] Unless individuals understand the importance of data protection, and can relate it to their own lives, it will never be fully effective.

b. Benefits for DPAs

DPAs are faced with many challenges. They have become de facto the principal regulators of the digital society and the data which is powering it. They are expected to exercise control over millions of organisations—large, medium and small, operating in private, public and third sectors and often across national borders. Innovative technology develops daily. Individuals are becoming increasingly vocal about their expectations of privacy and responsible data uses. DPAs must balance numerous tasks and potentially competing public policy goals—data protection, other fundamental rights (including free speech), free flows of information, innovation, societal benefits, security and so on.

Moreover, in absolute terms and in comparison to most other areas of regulation, DPAs are woefully under-resourced. A fundamental challenge for any DPA is how to maximise effectiveness when there is so much they could do and so little resource to do it. Resources may be increased in individual situations, but it is not controversial to state that resources will never be adequate. DPAs must also retain their credibility and their legitimacy. DPAs will never be able to do everything.

The search is therefore for approaches which increase the effectiveness and influence of DPAs and make the best possible use of available resources by concentrating on those regulatory activities which promise the best outcomes. Put another way, the credibility and even the legitimacy of DPAs may be called into question if they do not take active steps to maximise effectiveness.

[8] The EDPS Strategy contains a very welcome commitment to communicate even difficult concepts in clear and simple language.
[9] As made explicit in Art. 57(1)(b) GDPR.

The need for consistent approaches becomes even greater with demands for cross border co-operation and collaboration. The globalisation of data flows, and the need to protect individuals' rights globally, need to be matched by efforts to harmonise DPAs' duties and powers. Within the EU, this is envisaged by the GDPR.

For any such ambitions to work effectively, there will need to be maximum clarity about the strategies and priorities of all participating authorities. A results-based approach does not mean a standardised, one-size-fits-all approach. But it does mean at the least that the international community of DPAs must have confidence that they will be acting in ways which are complementary and converging. Even though DPAs operate in different legal systems and are part of different regulatory cultures, it is essential in the borderless digital world that DPAs' priorities are mutually consistent and as seamless as possible. This will also improve the efficient use of DPA resources.

Within the EU, these needs are even more evident. The co-operation and consistency mechanism introduced by the GDPR will need consistency of priorities and enforcement approaches as much as consistency of legislative interpretation.

International co-ordination has already demonstrated its potential with initiatives such as the Global Privacy Enforcement Network (GPEN) and the APEC Cross-border Privacy Enforcement Arrangement (CPEA), with co-ordinated investigations and an International Internet Sweep.

There have also been increased efforts to co-operate with consumer, competition, telecoms and other regulatory bodies. The EDPS has proposed the establishment of a Digital Clearinghouse to "bring together agencies from the areas of competition and consumer and data protection willing to share information and discuss how best to enforce rules in the interests of the individual". The first meeting of the clearinghouse took place in May 2017.[10]

c. Benefits for Regulatees

All organisations—large and small businesses, governments, public agencies, NGOs—are digitalising their activities, products and services; processing personal data; and being regulated to a greater or lesser extent by data protection laws. By their nature, the laws cannot always be clear-cut and are often principle based and contextual. Yet, regulatees need to know how to behave and what actions

[10] https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en.

they are expected to take to protect individuals and what behaviours they should avoid. All regulatees, large organisations, SMEs and start-ups need and are equally entitled to as much consistency and predictability as possible from regulatory bodies within and across national borders. This is especially important given the increasing speed of technology developments and modern data protection laws' placing ever greater weight on accountability and risk management.

An effective regulatory framework for the digital economy—with smooth and free, but well-ordered, data flows—is essential for promoting innovation, economic growth and prosperity. The framework should not, however, impose disproportionate burdens, especially where the costs get passed on as higher prices, lower wages or higher taxes.

d. Global Generally, Europe Specifically

DPAs around the world have far more in common than the detailed differences which may separate them. The analysis and suggestions of this paper are therefore intended to be helpful for all DPAs, not least in encouraging maximum consistency for a global digital economy.

At the same time, the activities of DPAs in the EU will very soon be significantly transformed by the GDPR. This will have major implications for them, but also for many other DPAs which will be directly or indirectly affected by GDPR. The recasting of DPA functions—and in particular the one-stop-shop with a lead DPA and the legally binding co-operation and consistency mechanisms—crystallises the need for maximum consensus about how to maximise effectiveness. All EU DPAs will need to reset their strategic priorities and do it consistently across the EU. As they rise to these challenges, CIPL hopes that the analysis and suggestions put forward in this paper will be especially helpful to such DPAs, to the WP29 and (in due course) to the EDPB.

It can be expected that the EU approach over the next few years will have a significant effect on the rest of the world. Although this paper accordingly illustrates many of its points by reference to GDPR, and anticipates that the EDPB could take a lead in taking forward its suggestions, it should be stressed that the overall approach is not intended to be confined to the European context.

2. The Functions of Data Protection Authorities

Although the details of specific DPA functions vary around the world, there are broad similarities. In 2001, the International Conference of Data Protection and Privacy Commissioners adopted formal processes and criteria for recognising the credentials of data protection authorities.[11]

Great weight has been attached to the genuine independence and autonomy of DPAs. They may be independent and autonomous, but they need to perform their tasks in the public interest. In the 2010 case of *Commission v. Germany*[12] the European Court of Justice emphasised how DPAs fit within the system of checks and balances in a democracy based on the rule of law.

DPAs can be seen as "hybrid" bodies, expected to ensure that organisations meet their obligations, that the rights of individuals are respected and (more generally) that high levels of privacy and data protection are maintained across society. Their strategic goal can be described in terms of balancing the protection of fundamental rights—or the prevention of harm—with the free flow and beneficial use of information. In the EU, the European Court of Justice described the essence of the DPA task as "establishing a fair balance between the protection of the right to private life and the free movement of personal data".[13] DPAs have been described as "authoritative champions".[14]

In the EU, DPAs have a constitutional status with the broad task of "controlling" or "supervising" the processing of personal data and ensuring compliance with the data protection rules.[15] Articles 57 and 58 of the GDPR set out the functions—some new—of each data protection supervisory authority. These can be seen as a mix of "sticks and carrots". These are divided into tasks and powers. Some 22 separate "tasks" can be identified, where the DPA "shall" undertake the prescribed activity. These are amplified by some 27 powers, of which 6 are "investigative", 11 are "corrective" and 10 (with some replication of mandatory tasks) are "authorisation and advisory".

In effect, the GDPR presents these 22 mandatory tasks and 27 powers as a shopping list with little or no attempt to prioritise or indicate how they relate to each other, nor any articulation about the overall mission of each DPA in terms of the outcomes it is supposed to achieve. Each function is explicable in isolation, and most are neither controversial nor surprising in themselves. Yet, critically, the GDPR does not set out any sense of overall strategy.

---

[11] https://icdppc.org/wp-content/uploads/2015/02/Criteria-and-Rules-for-Credentials-Committee-and-the-Accreditation-Principles.pdf.
[12] C-518/07 - para 41-43.
[13] C-518/07 - para 30.
[14] Bennett and Raab, *The Governance of Privacy*.
[15] Article 16(2) of the Treaty on European Union and Article 8(3) of the Charter of Fundamental Rights.

However, nothing in the GDPR, or in laws elsewhere in the world, prevents the development of a more strategic, results-based approach. It is also possible to identify different **types** of function—an essential element for any strategic thinking.

Although there are interlinkages and interdependencies, with no hard boundaries, Annex A of this discussion paper groups each of the GDPR functions into one of four broad types:

1. ***"Leader"*** *– the functions which rely upon the expertise, authority and support of and information from the DPA;*
2. ***"Police Officer"*** *– where enforcement is available for infringement, especially deliberate or wilful non-compliance;*
3. ***"Complaint-Handler"*** *– where complaints may lead directly or indirectly to a sanction or to redress;*
4. ***"Authoriser"*** *– where some form of prior authorisation is needed from the DPA.*

3. Meagre DPA Resources

Although they can never be adequate, the resources available to DPAs must be examined before exploring strategies and priorities for maximising the effectiveness of regulation.

a. Level of Resources

The most recent comparative survey of DPA budgets was carried out as a census by the ICDPPC in 2017.[16] Relevant data from the survey is set out and analysed in more detail in Annex B and set against some of the demands imposed on DPAs.[17]

The survey responses include resource data for 87 Data Protection Authorities from 58 countries. Of the countries which provided financial resource information, the total global DPA budget for 2016 was €887,320,351.

For 26 EU countries[18] the figures show a total budget in 2016 of €205,703,574 for a total population for that year of 507,471,970.[19] This would suggest, across these 26 countries as a whole, that the budget per citizen was less than €0.41.

Even more indicative of the demands upon each DPA is the need to relate resources to the number of regulated organisations. Eurostat estimates that "in 2014, the EU28's business economy was made up of around 26 million active enterprises".[20] Assuming that virtually all enterprises are now processing personal data, this suggests that DPAs have an average budget of only about €8 per business.

Staff numbers provide a further indication of resources and capability. The recent PHAEDRA study on *Enforcing Privacy*[21] found that only 12 DPAs in the European Union had more than 40 full-time staff in 2015, with the highest at 350 and the lowest at 14. Six of the EU DPAs had fewer than 30 staff.

The meagreness of resources is not new and is fully recognised by the DPAs themselves. A recent collective recognition of the problem is to be found in a Resolution[22] adopted at the European Data Protection Authorities' Conference in May 2015. Extracts from the preamble and substance of that Resolution are worth highlighting:

---

[16] The census data is available upon request from the International Conference of Data Protection and Privacy Commissioners Secretariat, https://icdppc.org/the-conference-and-executive-committee/icdppc-census/.

[17] CIPL is most grateful to the ICDPPC for making the survey data available for use in this paper ahead of its formal publication.

[18] Figures were not available for Austria or Croatia and the figure for Germany is lower than the actual value as only 7 out of 16 Länder provided data.

[19] Population figures for the 26 relevant EU countries were sourced from the World Bank on 27 July 2017, http://data.worldbank.org/indicator/SP.POP.TOTL.

[20] http://ec.europa.eu/eurostat/statistics-explained/index.php/Business_demography_statistics.

[21] http://www.phaedra-project.eu/wp-content/uploads/phaedra1_enforcing_privacy_final.pdf.

[22] https://edps.europa.eu/sites/edp/files/publication/15-05-20_manchester_resolution_1_en_0.pdf.

- "…European Data Protection Authorities are being confronted with many new challenges, with implications for the way in which they deliver their functions…".
- "…Data Protection Authorities are increasingly facing financial and other resource constraints whilst at the same time the demands on them are increasing".
- "…rights and obligations on paper must always be enforceable and deliverable or they are at best a delusion and at worst a deception on citizens".
- "[The Conference] calls upon the governments of European countries to ensure that the funding of Data Protection Authorities is sufficient to meet the ever increasing demands on them and to ensure that the requirements set by the law makers are duly followed in practice".

Despite the scale of responsibilities which the GDPR places on the shoulders of DPAs, it makes little attempt to increase the extremely limited financial and human resources which are available to them. Article 52(4) provides only in general terms that "[e]ach Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers…".

This is, however, little more than a general exhortation with more aspiration than precision or real obligation. It is not specific and will be difficult to enforce by legal, political or other means.[23] The European Commission is pressing Member States to provide adequate funding, but has not developed any criteria for assessing what is adequate or "necessary".

There is some evidence of actual and potential upward movement. The budget of the Irish Data Protection Commissioner has been increased substantially—the ICDPPC census reports an increase of more than 20 % for 2015-16 alone. In the Netherlands the Autoriteit Persoonsgegevens (AP) commissioned consultants to review what resources it will need to discharge its GDPR responsibilities. The consultants' report[24] concluded that the new situation will be completely different. It emphasised increased complaint and data breach volumes and responsibilities, the need for more systemic control and more investigations arising from EU co-operation mechanisms, the costs of promoting public and organisational awareness, the need for DPIA prior consultations and the costs associated with certification and accreditation arrangements. According to this scenario, this new reality could require a trebling of staff from 72 up to 185-270. The report is currently with the Ministry of Security and Justice and budgetary decisions are awaited.

[23] In the case of *Commission v. Austria* the CJEU did not even adopt the argument that a DPA should have its own separate budget.
[24] https://www.tweedekamer.nl/kamerstukken/detail?id=2017D15344&did=2017D15344.

Indications of actual or possible budget increases in Ireland, the Netherlands and elsewhere are welcome. Nevertheless, the overall picture does not yet appear to extend beyond incremental increases and remains very disturbing.

Finally, there has not been sufficient attention paid to the need for DPAs to recruit more technology, communication and other experts to go beyond the legal skills to be found within most DPAs.

b. Additional Resources?

Beyond doubt, whatever approaches European DPAs adopt, they will need additional resources. The PHAEDRA study[25] concluded that "[n]owadays – to ensure an appropriate level of protection of privacy and personal data and to investigate and prosecute violations, should they occur – these supervisory authorities face constraints by way of human and/or budgetary shortages…". It quotes the 2014 view of the European Union Agency for Fundamental Rights that "the problem of resources represents one of the greatest obstacles limiting their activity".

Resources lag far behind those available for competition / anti-trust authorities. A recent, but not comprehensive, exercise conducted by Politico concluded that "[s]tarving watchdogs lag in preparing for EU's biggest privacy law".[26] In March 2017, Isabelle Falque-Pierrotin on behalf of the WP29 sent a letter[27] to the Council of Ministers calling for increased resources to allow DPAs to "effectively perform their new tasks, train their own staff, upgrade their IT-systems, promote awareness and give guidance on the new rules".

The GDPR does not address possible sources of DPA funding, but leaves this to the Member States. There are roughly three possible sources:

- **Governmental funds** – Public funds, sourced from taxation or borrowing, have been the traditional budgetary source for most DPAs. But, with most governments facing economic challenges in an "age of austerity", one must ask how realistic is it, or likely, that national governments will provide any significant increase from public funds over the resources already available to DPAs. Also, where budgets depend upon governmental funding, especially where constitutional guarantees for sufficient budget are lacking, the possibility of a threat to independence always exists.

- **Fines** – The GDPR contemplates substantial fines for organisations which breach their obligations. But, any attempt to finance DPAs directly from

[25] At page 16.
[26] http://www.politico.eu/pro/starving-watchdogs-will-police-eu-biggest-privacy-law-general-data-protection-regulation-europe/?utm_source=POLITICO.EU&utm_campaign=edc4d71000-EMAIL_CAMPAIGN_2017_04_04&utm_medium=email&utm_term=0_10959edeb5-edc4d71000-189890157.
[27] http://ec.europa.eu/newsroom/document.cfm?doc_id=43668.

penalties which they themselves impose will be fiercely opposed as putting in place distorting incentives. Any such attempt will be highly controversial and open to ethical, political and legal challenge.

- **Regulatees** – The cost of regulation could be directly borne by those it regulates, whether through fees or other means. This "polluter pays" approach is increasingly common in other areas of regulation. Some DPAs already receive income from chargeable services, such as auditing, training and publications. The approach recognises that regulation benefits organisations by increasing public trust and confidence in their activities and it avoids burdening public funds. It can also be very administratively simple and cheap to collect. The GDPR would not prevent, for example, a Member State from introducing a bare requirement for every organisation which processes personal data to pay a modest online fee directly or indirectly to the competent DPA each year.

  Assuming again that virtually all enterprises are now processing personal data, a nominal fee of just €20 from the 26 million enterprises in the EU would generate a total budget of €520 million each year—a massive increase of resource. The total would be even greater if the fee were to be more for larger organisations.[28]

QUESTION FOR DISCUSSION

1. **Which ways should be explored for increasing DPA budgets to more realistic levels?**

[28] In the UK, over 400,000 data controllers are registered. The fee for larger organisations is £500.

4. Effective Regulation

The challenge of effectiveness is to get the best results from whatever resources are available. Data protection does not exist in a vacuum and there is much to be learned from experience in other regulatory spheres. Many studies of regulatory effectiveness have emerged in recent years—and the Bibliography mentions some of these. Unfortunately, however, such studies have largely bypassed data protection and, in turn, perhaps have not been taken sufficiently into account by the data protection community.

Before discussing what a Results-based Approach for regulating data protection might look like, therefore, this section draws upon a range of significant studies.

a. Key Themes

Although there is no single consensus about "what works best", and the regulatory pendulum swings to and fro, a number of key themes can be identified. These include:

- Regulatory practice—the behaviour of regulators—is just as important as the content of laws and regulations.
- Aiming for well-defined results—or "outcome-based" regulation—is now widely recognised as a high-level regulatory principle. In other words, any effective regulatory delivery model should focus, as far as possible, on outcomes, going wider than "law enforcement" and resisting pressures to seek compliance for its own sake or to impose excessive regulatory prescription.
- Effective regulators adopt a "risk-based approach". This means that the supervisory framework, including interpretation and enforcement, is targeted to manage the main risks to the regulatory objectives.[29]
- Effective regulators select the most appropriate approach from a wide range of compliance-producing tools, engaging with those they regulate and preferring "voluntary compliance" to enforcement where possible. This approach becomes even more relevant where regulatees are required or expected to be accountable.

[29] This is especially relevant to the risk-based provisions of the GDPR. See also "A Risk-based Approach to Privacy: Improving Effectiveness in Practice", CIPL 2014, available at http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf; and "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR", CIPL 2016, available at http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

- They also exploit a range of levers in addition to their own formal powers to ensure that standards are upheld. These levers include the influences which come from users, consumers and citizens (especially where they can make choices in a competitive marketplace and democratic arenas), from peer pressure amongst regulatees, from conventional and social media and from the political sphere.

b. Law and Corporate Behaviour

One of the most recent and comprehensive studies elaborates these themes and is worth citing in more detail. In his 2015 book, *Law and Corporate Behaviour*,[30] Prof Christopher Hodges, professor of justice systems at the University of Oxford, draws together some 800 pages of evidence and analysis to inform discussion about effective regulation. In the words of its subtitle, it is about "[i]ntegrating theories of regulation, enforcement, compliance and ethics".[31]

Prof Hodges has subsequently advanced the concept of "Ethical Business Regulation" (EBR), which, based on empirical data on why people observe or break rules and on how culture can support continuous improvement and innovation, aims to build commercial success on compliance with social values.[32]

Maximum Compliance

Hodges argues that regulation is fundamentally about behaviour. The optimum outcome is to produce acceptable behaviour and to stop unacceptable behaviour. In practical terms, effective regulation means securing maximum compliance.

A substantial body of evidence demonstrates how regulators in contemporary democracies should best seek to affect business behaviour in order to secure maximum compliance. This includes the findings of behavioural psychology and analysis of economic and cultural incentives. Regulation alone cannot achieve compliance, especially since it is heavily influenced by customer pressure, competitor behaviour, media comment and reputational considerations. Social norms, ethical values and peer pressure also play important parts. Enlightened self-interest—where compliance is seen as providing a route to increased profitability or fulfilment of other corporate goals—is very often a dominant factor.

Effective regulation involves harnessing these and similar forces, not resisting them or working in isolation from them.

---

[30] At page 8.

[31] An abbreviated summary of key points is available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/497539/16-113-ethical-business-regulation.pdf.

[32] *Ethical Business Regulation; Growing Empirical Evidence*, Christopher Hodges, Wolfson College, University of Oxford.

The Modern Approach to Regulation

The essence of a modern democracy is based on respect for others, not least expressed through support for fundamental human rights. Applying that political policy to a vibrant market economy produces the result that society supports honest business to improve the common good. Honest business and a harmonious society function on the basis of trust. Hence, a key purpose of regulation is to enable widespread trust in businesses, on the basis of which a healthy, sustainable and growing economy can exist, which in turn supports employment, social stability and innovation. This philosophy is equally applicable whether the regulatory objectives are primarily economic or social.

In line with this broad philosophy, most modern regulation has moved on from the historical model—where a powerful individual or organisation "commands and controls" the actions of inferiors, exercising authority through actual or feared harsh punishments on those who did not obey. It is now universally accepted—and usually legally enforceable—that, even if regulatory bodies hold significant power to enforce the law, they must act fairly and proportionately, follow due process and be accountable for their actions.

The modern approach inevitably also requires a good understanding about why organisations and people behave in particular ways and how they can be helped to improve.

Empirical research has found that people obey rules where:

a. the rules correspond to recognised value systems;

b. the rules have been made fairly; and

c. the rules are applied fairly.

Responsive Regulation

A great deal of research now endorses "responsive" regulation where the emphasis is on engagement through information, advice and support rather than deterrence and punishment. Research has covered a wide range of regulated activity, including occupational health and safety, water pollution, environmental protection, the mining industry, food processing, care for the elderly and civil aviation.

Outcomes, not Compliance

In response to stubbornly high accident rates on construction sites in the 1990s, the UK regulator (the Health & Safety Executive (HSE)) decided on a new approach—to make those involved *own* it as their problem. Instead of inspections on a site-by-site basis across tens of thousands of construction sites, the new approach involved leveraging influence in high-risk areas and engaging and forming partnerships with parties inside the industry able to effect widespread change.

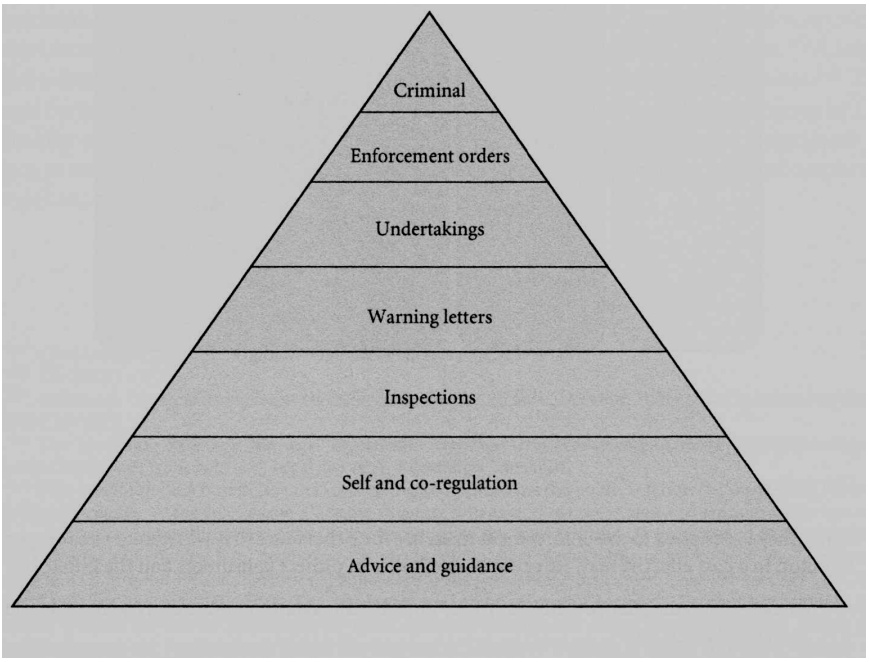
The approach was a significant success. From 2000-01 to 2012-13 the number of fatal and major injury accidents fell from 4,410 to 2,161 (49 %).

A study comparing the enforcement policies of various countries with the same laws illustrated clearly that the difference in effectiveness lies not in the rules, but in the approach of the authorities.[33] The UK's approach has permanently reduced the occurrence of serious safety incidents. The same approach was followed in Germany, with the same outcome. The approach in France, however, still relies on inspections and penalties for non-compliance with the rules. The "name of the game" is for businesses to pass inspections, not to make workplaces safe. The workplace safety record of France has remained one of the worst in Europe.[34]

Experience in these and other fields stresses the benefits of a culture where regulators adopt a positive and proactive approach towards ensuring compliance. This involves regulators carrying out their activities in ways that support and help those they regulate to comply. In particular, high priority should be given to ensuring that clear information, guidance and advice are available to help organisations meet their responsibilities. Such support is even more important for SMEs, where the research indicates that they often believe that they are complying with the law until a person they respect (e.g. a regulator or trade association) points out that they could improve, after which they usually follow the advice.

[33] F Blanc, *From Chasing Violations to Managing Risks. Origins, challenges and evolutions in regulatory inspections* (Edward Elgar, forthcoming).
[34] Ibid.

Responsive Regulation – the approach of the UK Civil Aviation Authority[35]



c. Conclusions From Other Spheres of Regulation

From the evidence and this analysis, Prof Hodges draws five basic conclusions[36]:

1. **A regulatory system is most effective where it is consistent and supports behaviours which are widely seen as fair, proportionate and ethical.**

2. **Organisations should be accountable for demonstrating, with evidence, their commitment to behaviour that will attract the trust of regulators, as well as their own management and staff, customers, suppliers, investors and other stakeholders.**

3. **Learning is fundamental and is encouraged by open and constructive engagement between regulators and regulated organisations, but is deterred by emphasis on "blame" and / or punishment.**

4. **Regulatory systems need to be based on dialogue and mutual co-operation which are explicitly directed at maximising compliance, prosperity and innovation.**

[35] CAA Regulatory Enforcement Policy, based on the "responsive" model of regulation developed by Prof John Braithwaite, as quoted in *Law and Corporate Behaviour*.
[36] These are enlarged in Annex C.

5. **Where organisations do break the rules, a proportionate response is needed, with the toughest penalties reserved for deliberate, repeated or wilful wrongdoing.**

QUESTION FOR DISCUSSION

1. What can be learnt from approaches which have been adopted around the world in other spheres of regulation?

5. A Results-based Approach for Regulating Data Protection

The evidence and analysis contained in various studies, as summarised above, is consistent with more subject-specific thinking that is starting to emerge within the data protection community. Both DPAs and regulated organisations increasingly understand that compliance is part of corporate responsibility and sustainability.

As our digital society transforms through the fourth industrial revolution, a new ecosystem for data protection is emerging—based on accountable organisations and effective and outcome-based regulators.

At the EU level, there is a growing recognition of the fundamental challenges for DPAs which can be summarised in simple terms:

- From May 2018, the functions of DPAs will enlarge substantially;
- DPA resources are meagre for existing functions and will be inadequate to fulfil the full range of tasks prescribed by the GDPR;
- There is little or no prospect of sufficient increases in governmental funding; and
- Even significant increases would not diminish the need for strategic approaches.

The foundation of organisational accountability as a driver for data privacy compliance, which CIPL articulated for many years and which was given authoritative recognition in the seminal WP29 Opinion on Accountability,[37] now lies at the heart of the GDPR. Accountability is also essential in the OECD Privacy Guidelines. Globally, privacy management programme guidance from the Canadian, Hong Kong and Australian privacy commissioners has been very well received and influential, as well as the references to accountability in Colombian and Mexican data protection laws.

In 2015, the European Data Protection Supervisor (EDPS) published his Opinion, *Towards a new digital ethics*,[38] which followed on from EDPS activities, encouraging synergies with consumer and competition law.[39] The 2015 Opinion envisages an effective data protection regime in terms of an "ecosystem" where all relevant players (but especially DPAs and controllers) act better together to reinforce rights.

The importance of enlightened self-interest as a driver of corporate behaviour has been explicitly explored by the former interim privacy commissioner for Canada. Chantal Bernier's discussion paper[40] outlines how the concept of "Social Licence to Operate" (SLO) could become the "ultimate enforcement of privacy law". This argues

[37] Opinion 3/2010 on the principle of accountability, WP 173.
[38] EDPS Opinion 4/2015.
[39] For example: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf
[40] The Concept of Social Licence to Operate: A Common Ground to Apply Privacy Law? - Dentons, Ottawa.

the case for treating social acceptability as the common ground between regulators and business, especially as individuals become more assertive in their expectations and businesses become more concerned about the impact of data-handling reputation on the bottom line.

Most recently, a report[41] published by the US Chamber of Commerce in February 2017 argued that the risks and challenges of data protection arising from the ubiquity and increasing value of data in the global economy make it imperative to understand how to regulate data protection effectively. A study of DPAs around the world demonstrates, however, that "their methodologies, practices and scope of authority vary greatly". The report goes on to conclude that "...the common thread among all DPAs is that truly effective DPAs treat those they regulate as partners instead of adversaries". With an approach that corresponds with the analysis and suggestions in this CIPL paper, the report identifies seven Key Attributes as the keys to effective data protection governance. They place strong emphasis on education, awareness, feedback, guidance and assistance.

a. Effectiveness

There is no settled consensus about what effectiveness means in the context of data protection. At the general level, there is frequent reference to such concepts as "upholding the fundamental rights of individuals", "achieving a high level of data protection" or "ensuring compliance with requirements". But such aspirations can be too hollow without more concrete objectives. Likewise, references to risks, priorities, targets and mantras such as "Selective to be Effective" are not sufficiently meaningful unless and until there is clarity and agreement about what is meant by being "Effective".

As a starting point, all effective regulators ask themselves:

- "What results are we trying to achieve?"
- "What does success look like?"
- "How will we know when we've done a good job?"

CIPL does not have the answers to these questions, which, in any case, are for DPAs to agree upon themselves, whether collectively or individually. The basic aim of protecting individuals in practice has already been mentioned, but, as with environmental protection, there is a wider "social good" dimension. At CIPL's Dublin workshop a broad consensus emerged about the importance of seeking and securing clearly articulated results, rather than compliance for its own sake. It was also recognised that fundamentally effective regulation involves monitoring and changing behaviours, and sometimes cultures, not just ensuring that the formalities and paperwork are in order.

[41] *Seeking Solutions*, US Chamber of Commerce, Feb. 2017, https://www.uschamber.com/sites/default/files/023052_dataprotectionhuntonpaper_fin.pdf.

Therefore, beyond mere compliance, regulating data protection means aiming for a digital world where people flourish with dignity as autonomous individuals. The overall results which are sought could thus be developed on the following lines:

- the prevention of data uses which impair the quality of life for individuals by denying them the privacy to which they are entitled; and
- the promotion of a society where a good quality of life for individuals flows from genuine and widespread privacy where the use of data in a digital world is both universal and popular.

We do stress, however, that it must be for DPAs themselves to articulate the outcomes they are seeking.

b. Setting Strategic Priorities

Any well-managed DPA will need to set clear priorities, usually in a transparent Strategic Plan. If priorities are not articulated explicitly, there will still be de facto prioritisation in the shape of work done and work left undone. The Conference Resolution mentioned above itself recognised the need for a targeted approach:

- "It is not though just a question of resources. It is also necessary for Data Protection Authorities to adopt a sustainable approach at national, EU and the wider European level to carrying out their functions, targeting their activities where the need to protect privacy is greatest…".

This is not straightforward. Using the familiar language of "targeting" or adopting a "risk-based approach" is relatively easy, but much more difficult is going beyond the rhetoric and developing meaningful criteria, principles or other measures to determine the priorities, the targets or the risks which should be tackled. This applies in at least two dimensions:

- How should functions (or tasks or activities) be ranked against each other?
- How should particular sectors, activities or organisations be targeted for attention within a particular function?

All regulatory bodies, in all sectors and in all jurisdictions face these questions. The evidence from other spheres of regulation, as summarised in the previous section, suggests how they are being answered. There are lessons to be learned for data protection. In particular, a considerable body of evidence now exists to guide the priority-setting processes.

The following construct may be helpful in answering these questions:

PREDICT - PREVENT - DETECT - ENFORCE

These are key goals for any regulator, but it is necessary to decide the balance between them and where to place priority. The evidence from other regulatory spheres suggests that “Prevent” should be paramount, backed up by “Enforce” when that is necessary. A strategy can then be developed by relating these goals to all the DPA functions.

A Results-based Approach to regulation involves maximum engagement with regulated organisations and, as this table demonstrates, Leadership is crucial for the effective fulfilment of all goals:

	Leader	**Authoriser**	**Police Officer**	**Complaint-Handler**
PREDICT	✓			
PREVENT	✓	✓		
DETECT	✓		✓	✓
ENFORCE	✓		✓	✓

This analysis also suggests a broad ranking of priorities:

1. **“Leader”** – where the emphasis is on the expertise, authority, influence of and information from the DPA.
2. **“Police Officer”** – where the emphasis is on enforcement in cases where there has been, or may have been, an infringement of the regulation.
3. **“Complaint-Handler”** – where the emphasis is on dealing with individuals’ complaints, which may lead directly or indirectly to a sanction or to redress.
4. **“Authoriser”** – where some form of prior authorisation from the DPA is needed.

c. Leadership and Engagement

“The guidance that DPAs provide today will produce the results they want tomorrow”.

It should be unarguable from this analysis that the Leadership role—guiding good practice—is the top strategic priority and can only grow in importance in the modern information age. It cuts across all the goals which need to be fulfilled.

Leadership embraces those functions which rely upon the expertise and authority of the DPA. An effective DPA will want to be, and be seen to be, the leader in making clear the outcomes and behaviours which it expects. This involves understanding the technological, commercial and political environments, anticipating issues, interpreting the law and providing guidance that is forward thinking, practical and strategic. Although they have a part to play here, this is not a role that can be delegated to lawyers, consultants or other advisers, nor left in the hands of regulatees themselves. It is fundamental that DPAs should ***engage*** directly in dialogue and take the lead in providing the information, advice and support which will make a practical reality of data protection. DPAs can leverage informed input from inside regulated organisations—in private and public sectors—to help fulfil their mission.

Engagement requires mutual trust and reinforces the GDPR's Accountability principle. It is a two-way process—with accountable organisations willing and able to demonstrate their compliance, to be transparent about their own activities and to share insights into general technological and behavioural trends and innovations. Although leadership must primarily involve dialogue with regulatees, information, advice and awareness-raising for members of the public also have parts to play here.

Examples of DPA Engagement

- The WP29 has taken the very welcome initiative of consulting on draft Opinions and Guidelines before they are adopted. Recent examples include lead authorities, data portability and DPOs.

- A number of DPAs have discussed Artificial Intelligence (AI) issues with relevant businesses and are now recognising that an approach which calls for "transparency of algorithms" may be less productive than emphasis on "AI accountability & specific checks".

- The "FabLabs", organised by the WP29 to discuss GDPR implementation, have been much appreciated.

- The EDPS has a structured programme of high-level visits to the EU institutions which it supervises. These often result in an agreed road map to "voluntary" compliance which avoids the need for formal enforcement.[42]

- The EDPS also regularly consults DPOs on draft Guidelines.

[42] See successive EDPS Annual Reports.

- The *Pack de conformité* initiative from the CNIL has invited companies from a given sector to jointly define with the CNIL best data protection practices for this sector and to simplify administrative formalities.

- The US FTC conducts regular thematic workshops and consultations, on specific technological developments or forward-thinking topics, to solicit input and exchange learnings with key practitioners, experts, academics and leaders.

- DPAs taking part in APPA's biannual meetings regularly invite representatives from the regulated organisations to exchange insights on key topics of interest for the regulators.

Increasingly, DPAs are recognising the benefits of engagement and co-operation with regulated organisations—especially those organisations pursuing a responsible approach to compliance. Although there are of course many "shades of grey", it is widely recognised that few organisations are actively seeking to avoid compliance. Though many, especially SMEs, struggle through ignorance, the majority of regulatees accept that they should fulfil their legal obligations. Many of the larger organisations have adopted elaborate privacy management programmes to provide effective self-assurance or "earned recognition", moving beyond the more traditional syndrome of "privacy paperwork" where efforts rarely went beyond policies collecting dust on a shelf. These trends are supported in the GDPR with its emphasis on Accountability and Risk Management and its encouragement of Certification and seal schemes. At the very least, a comprehensive privacy programme should provide evidence of serious attempts to achieve compliance.

A further part of the DPAs' leadership role is to encourage organisations to adopt accountability frameworks and incentivise good behaviours. This can be done by formally providing mitigations for those organisations that are able to demonstrate sustained accountability, or simply showcasing examples of best practice to create market momentum and peer pressure for others to follow. For example, the Singapore PDPC, at the occasion of the large international conference and Singapore DP week in 2016, distributed a user-friendly booklet showcasing best practices of over half a dozen organisations in Singapore, ranging from large multinational companies to public sector organisations and local start-ups.

At the same time, DPAs need to be sophisticated in their approach. For example they should understand the principles and logic of risk management and continuous improvement of compliance policies and procedures and not use it to evidence weaknesses, which organisations have openly acknowledged but justifiably treated as low priority. Equally, guidance from DPAs on low risk or *de minimis* activities is likely to be welcomed as part of a risk-based approach.

d. Police Officer

The Police Officer role—investigating, threatening or taking enforcement action against non-compliant organisations—is important, but—if widespread behavioural results are seriously sought—it should not be the top priority and should not be a first port of call for any DPA. The evidence summarised in section 4 above suggests that such an attitude would be both ineffective and counterproductive. There are significant risks that regulatees will adopt defensive, secretive or openly hostile attitudes which are most unlikely to improve outcomes for those who are supposed to be protected. Scarce resources could easily end up being diverted into fighting lengthy battles in the courts. No regulator can expect to be effective if its first-choice approach is to rule by fear.

This is not to deny a due role for enforcement. DPAs around the world have been given significantly sharper teeth in recent years, most notably by the GDPR which introduces fines up to 20 million euros or 4 % of annual worldwide turnover. Such sanctions increase credibility and legitimacy and concentrate minds. The possibility of enforcement and stronger sanctions will undoubtedly influence many organisations, especially where commercial or reputational damage follows. DPAs will have to exercise their enforcement powers from time to time for them to be meaningful, of course with due respect to considerations of proportionality. Where decisive action is taken, especially where an eye-catching penalty is involved, attention is easy to attract (not least via media and political channels).

Certain breaches may be so serious that a sanction is inevitable. However, clearly the main targets for enforcement activity (preferably set out as an explicit goal) should be those organisations which are engaging in deliberate, wilful, repeated or seriously negligent non-compliance with the law. This approach is consistent with the GDPR which includes multiple factors to be taken into account when deciding both whether to fine and the amount. These include the gravity of the infringement, its intentional or negligent character and any relevant previous infringements.[43] In most cases, some form of warning would be desirable, to both alert the organisation and make it easier for the DPA to show intent or negligence. If a DPA is to succeed as a Leader, use of the “stick” is not unreasonable, especially in situations where warnings of non-compliant behaviour have been ignored and a real risk of harm to individuals exists.

e. Complaint-Handler

Although EU law treats the complaint mechanism as an important element of the individual’s right to data protection and complaint handling is also included in some data protection laws around the globe, it is unusual in other spheres of regulation for a regulatory body also to have complaint-handling functions.

[43] GDPR, Article 83(2).

In the EU, the GDPR makes it mandatory for a DPA to "handle" complaints. This is not new and, under current EU law, complaints must be dealt with with due diligence, an issue which lay at the heart of the *Schrems* case.[44]

Serious problems and threats to effectiveness may emerge, however, if the Complaint-Handler role is given excessive priority or not tightly managed. Firstly, this role is demand-led—outside the control of DPAs—and can be very resource-intensive, to the detriment of the other functions. Unless cases are chosen very carefully, it can distract from more strategic activity and (however well-performed) bulk complaint-handling will rarely achieve desired behavioural outcomes across a sector. Rather than focusing on redress for select, or numerous (but relatively few), individuals, regulators should concentrate on protecting rights more universally before any wrong happens. There are real risks of creating an environment of public disappointment or disillusionment—whether through backlogs or unwelcome outcomes—and jeopardising the popular support which DPAs need.

This is not to say that the Complaint-Handler role should—or could—be ignored altogether. The GDPR imposes a duty on DPAs to "handle and investigate" complaints. But this implies a wide discretion. "Handle" is a flexible concept which is not elaborated on. Article 57(1)(f) of the GDPR requires the investigation to be "to the extent appropriate", which certainly allows triage arrangements, distinctions between different types of complaint, priority for the most serious cases and referral elsewhere where appropriate.

A Results-based Approach should involve various elements in respect of complaints:

- the Complaint-Handling role be well-managed to avoid the swamping of a DPA;
- DPAs should be aware of the risks to overall effectiveness from diverted and inefficient use of resources;
- the value of complaints as a source of intelligence should be stressed;
- information requests should be separated from genuine complaints;
- objective criteria should be developed for determining which complaints are to be "handled and investigated" beyond initial acknowledgment and monitoring;
- robust triage arrangements should be introduced to ensure the criteria are applied consistently and fairly;
- DPAs should quickly identify abusive, frivolous or vexatious complaints;
- complainants should be encouraged (or, where possible, directed) to approach Alternative Dispute Resolution (ADR)[45] schemes which can provide remedies;
- complainants should be encouraged to address a complaint initially to the organisation concerned, which, as an accountable organisation, should have

[44] Case C-362/14, Schrems, EU:C:2015:650.
[45] See also the relatively new EU framework for Consumer Alternative Dispute Resolution (CADR).

complaint handling policies and procedures and be able to deal with the complaint effectively; and
- certification and seal programmes should be encouraged to provide third-party dispute resolution arrangements.

All these would alleviate the burdens on DPAs of handling large numbers of complaints that might be better resolved at source or through ADR mechanisms. This would enable DPAs to concentrate on more serious complaints or those that were not resolved by the organisation concerned.

DPAs should, in any event, publish their policies towards the receipt of complaints. With such an approach, and in line with the principles of "appropriate extent" and "due diligence", detailed attention can then be reserved, for example, for those complaints which:

1. cumulatively suggest widespread non-compliance affecting many people;
2. suggest particularly serious detriment for the complainant;
3. allege serious ongoing non-compliance;
4. could lead to essential improvements in organisational behaviour; or
5. suggest that an important point of principle needs to be addressed.

An approach on these lines is an efficient use of scarce resources which also treats complaints as an important source of intelligence to complement and support other—more important—functions. At the same time, it makes clear that DPAs must not allow themselves to be distracted into providing a high-volume, demand-led complaint resolution service.

One objection to the approach outlined above may be its potential impact on the individual's right to an effective remedy. The right to data protection is a right which individuals should be able to exercise effectively. CIPL suggests, however, greater focus on improving organisational conduct. This would, in fact, enhance the substance of this right by improving the effectiveness of data protection law generally (as the CJEU emphasised in Costeja).[46] It is important to recall that data protection law is often viewed, like environmental protection, as a public good which benefits everyone. In a more strategic environment, other methods of redress may also have an important role to play in securing an effective remedy for the individual.

Due Diligence in the EU context

In *Schrems,*[47] the EU Court of Justice decided that DPAs must examine claims of individuals concerning their right to data protection "with all due diligence". Although the meaning of due diligence is not fully clear, it can be argued that "due diligence"

[46] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*.
[47] Case C-362/14, Schrems, EU:C:2015:650, at 63.

requires that all complaints must be investigated by a DPA, in a manner appropriate to the complaint. The requirement of due diligence is essentially a compromise between a wide margin of discretion available to DPAs and the protection of complainants. DPAs, having limited resources, must ensure a high level of protection, but also provide for a legal remedy for those who claim that in their individual case the law is infringed. Due diligence could function as a compromise, provided it is not interpreted as an obligation to dedicate resources to investigate all complaints. The added value of an independent DPA is not only its wide range of tasks, but also its capacity to perform these tasks in a manner it considers most effective.

f. Authoriser

The DPAs' Authoriser role is also largely demand-led and potentially resource-intensive and non-strategic.

It covers those situations where some form of formal consultation, prior authorisation or approval is needed from the DPA. This *ex ante* approach means that the affected activities cannot take place at all without such authorisation. Examples in the GDPR include BCR approvals, ad hoc contracts for data transfers, prior consultation in case of DPIAs where risk cannot be mitigated, codes of conduct, etc. The actual processes of authorisation may not necessarily contribute much to effectiveness in terms of achieving high standards of behaviour. Although volumes are difficult to predict, this could be a significantly resource-intensive function, especially if each application is treated individually and examined in depth.

As with complaint-handling, the function itself and its rationale cannot be ignored. However, there is scope for DPAs to consider how to simplify and discharge this function most effectively, especially where it relates to cross-border processing falling within the one-stop-shop and consistency procedures. The EDPB could play a leading role here, by issuing guidelines, recommendations and best practices as foreseen in Article 70(1) of the GDPR, thereby also engaging with DPAs outside the EU.

Again, a strategic and co-operative approach is needed. The use of some form of "class-based" approval for certain prescribed types of activity, perhaps coupled with appropriate conditions, may be promising.[48] For each case where authorisation is needed, this could easily be given on the basis of published criteria for the activity. Compliance with the criteria and any conditions would lead to routine and automatic authorisation unless the activity involved unusual or exceptional features. This could be linked with the "Comply or Declare" approach increasingly adopted in other areas of regulation. As the DPA-as-Leader becomes more engaged with

[48] This could evolve in a similar way to "category exemptions" under EU competition law.

responsible regulatees, considerable scope for consultation exists about the substance and application of the criteria and even for self-certification mechanisms, which can be checked post facto by DPAs or accredited third parties. Obviously, this does not replace prior approval where specifically required by the law, but it significantly alleviates the process.

QUESTIONS FOR DISCUSSION

1. **When the challenges and expectations of the digital age are so great - and especially when resources are limited – what are the most promising ways for DPAs to work (independently and with others) to ensure that the regulation of data protection will produce the best results?**

2. **Can effectiveness be elaborated in terms of enabling people to flourish with dignity and autonomy in a digital world where unacceptable data uses which impair their privacy are prevented?**

3. **When the responsibilities of most DPAs are so numerous, what are the best ways to achieve overall effectiveness?**

4. **Does the Results-based Approach offer helpful ways to set strategic priorities and balance engagement, enforcement and complaint-handling?**

5. **Is it right to give top strategic priority to Leadership functions with strong emphasis on constructive engagement with regulated organisations?**

6. Constructive Engagement in Practice

The analysis in the previous section suggests that the Leadership functions of DPAs should be treated as the top strategic priority, with as much constructive engagement as possible between DPAs and those they regulate. In the EU this brings to life Article 57(1)(d) of GDPR which implicitly recognises that both sides could do much to assist the other to bring about optimum regulatory outcomes.

This central conclusion was supported at the workshop hosted in Dublin by CIPL in June 2017, which also stressed the mutual interest of regulators and regulated entities in securing real data privacy regulation alongside data innovation and the growth of the digital economy. In other words, effective and results-based regulators and accountable organisations can work more alongside each other as two essential pillars of modern data protection.

> "If businesses show us [a DPA] they are investing in self-compliance, we will relax—unless we see a smoking gun."
>
> "It's all about trust. Regulators and regulatees should have the same aims."
>
> "It makes a huge difference—and the subject gets taken seriously at the top—when regulators openly recognise good efforts and data protection successes."
>
> "We already work with businesses to improve their behaviours. We got 100,000 calls from SMEs last year."
>
> Participants at CIPL Dublin workshop

The workshop went on to consider what constructive engagement actually involves in practice. A welcome and growing trend towards constructive engagement on the part of many DPAs around the world has already begun and this can be built upon. Many activities and techniques (both current and prospective) can be identified:

- **Maximum Transparency** – DPAs should be transparent in setting out their priorities, expectations and working methods, which will help DPAs be effective and help organisations to "get it right the first time". In the same way, organisations must be ready to be transparent when engaging with DPAs, without fear or the threat of self-incrimination.
- **Practical Guidance** – Usually web-based, guidance is on the interpretation and application of regulatory requirements, which is also open for consultation and response by regulated organisations. The best guidance is in plain language, with plenty of examples and segmented for maximum ease of use by each target audience—e.g. small businesses, medium enterprises, multinationals, specific business sectors, public bodies etc.

- **Active Participation** – In open and closed meetings, to communicate both concerns and expectations, participation can be just as important to also find out about uncertainties, trends, commercial and technology developments etc.
- **"Regulated Self-Assurance"** – Places full reliance upon DPOs, codes of conduct, certification schemes, the ability to demonstrate accountability etc. to promote trustworthy self-compliance and reduce pressures on DPAs.
- **Maximum Consultation,** with a "No Surprises" approach, for example seeks views on draft guidance or getting feedback on a proposed strategic plan before its final adoption. Such dialogue is especially beneficial where there are new requirements or no common views on what is the "right thing" to comply, or even what should be prevented.
- **Frank Exchanges** – a willingness to participate in confidential discussions, often with a market leader, about the implications and acceptability—or otherwise—of a technological innovation.
- **Exploiting Herd Instinct** – Increasingly, DPAs are recognising that organisations tend to follow a leader of the pack. If one or two businesses prominently receive some form of regulatory endorsement or clearance to follow a desirable course of action, competitors, peers and many others (especially SMEs) will follow the benchmark and do likewise. There is considerable scope for DPAs to exploit this tendency—promoting best-in-class behaviours, highlighting successful transparency, DPIA and other templates, showcasing best practices of accountable organisations (training or awareness campaigns, DPO leadership etc.), deliberately influencing key legal and other advisers and highlighting examples of online good practice.
- **Incentives** – Corporate leadership will take data protection and privacy more seriously if DPAs can create and communicate incentives for good faith privacy and compliance programmes. These incentives can include the ability to share data across borders, to engage more broadly in big data and machine learning activities and, crucially, mitigation in case of enforcement.
- **Creating Space for Responsible Innovation** – There is considerable scope for building compliance solutions co-operatively. The Regulatory Sandbox (see below) offers one possibility. "Design Thinking" where data privacy requirements and compliance challenges can be made scalable and developed bottom-up by multifunctional teams may provide other opportunities for regulatory participation and engagement with regulated organisations and experts from other areas (behavioural economists, user-centric designers, technology engineers, marketing and customer relationship experts).[49]
- **Reiterative and Dynamic Compliance** – Just like with technology and software development, it would be helpful if both DPAs and regulated organisations approached compliance as a journey and a reiterative, dynamic

[49] One current example of a responsible innovation initiative is Facebook's "design jam" initiative seeking new approaches and solutions for transparency and individual control.

process, as opposed to a one-off event. Dynamic compliance is particularly suited for data protection, given the speed of technological developments and adoption of digital solutions. It enables improvements, based on user feedback, internal and external developments and learnings from industry and regulators. Organisations should be encouraged to adopt dynamic compliance and DPAs should not punish those that actively try to get it right over time.

- **Performance Indicators** are essential for measuring and demonstrating DPA success in directly influencing the spread of good practice, preferably with common and/or comparable metrics.

The Regulatory Sandbox – Space for Responsible Innovation

Constructive engagement includes creating space for responsible innovation by accountable organisations. How might this be achieved?

The "Regulatory Sandbox" model being developed by the UK's Financial Conduct Authority[50] may prove an interesting way to enable regulated companies to experiment and innovate in a "safe haven" overseen by the regulatory body.

The regulatory sandbox allows businesses to test innovative products, services, business models and delivery mechanisms in the real market, with real consumers.

The sandbox is a "supervised space" that is claimed to provide organisations with:

- reduced time-to-market at potentially lower cost; and
- appropriate consumer protection safeguards built in to new products and services.

The sandbox offers tools such as restricted authorisation, individual guidance, waivers and no enforcement action letters. The FCA closely oversees trials using a customised regulatory environment for each pilot.

Sandbox tests are expected to have a clear objective (e.g. reducing costs to consumers) and to be conducted on a small scale, so firms will test their innovation for a limited duration with a limited number of customers. It is arguable that technical innovation is impacting on data protection to an even greater extent than financial services. This model may be particularly well suited and well received in the data protection community, where there is increasing recognition that compliance has to be treated as an iterative process.

The possible use of the sandbox model in this context was raised by the former Secretary-General of the CNIL in an article in *Les Echos* in early 2017.[51]

[50] https://www.fca.org.uk/firms/regulatory-sandbox.
[51] https://urldefense.proofpoint.com/v2/url?u=https-3A__www.lesechos.fr_idees-2Ddebats_cercle_cercle-2D165613-2Dlinnovation-2Dlautre-2Darme-2Ddu-2Dbrexit-2D2061519.php&d=DwIFAw&c=jxhwBfk-KSV6FFIot0PGng&r=Fk3CDN4QpXmXZZ7F2MuwcJTW5M0wnTw0gqFJV2no8r8&m=Yd8qNquweow

More recently, in July 2017, it was announced that the Singapore PDPC is prepared to work with accountable companies to create regulatory sandboxes to test proposed legislative changes and enable companies to continue to be innovative and competitive.[52]

Constructive dialogue must be a two-way process, with a great deal of trust, commitment and mutual respect between DPAs and accountable organisations. Unless organisations are positive about helping DPAs to develop a better understanding of the landscape they regulate, they cannot expect DPAs to be open and comprehending. Regulated businesses and public bodies have to be ready and willing to engage constructively with DPAs. This means coming forward—both proactively and reactively—with an approach which is as open and frank as possible. Business and governmental organisations need to be able to explain and demonstrate as transparently as possible their processes and technology solutions and be ready to explain and demonstrate business models. This is also a matter of Enlightened Self-Interest and is especially promising in an environment where more and more responsible entities pride themselves on their accountability. Where an obviously innovatory or controversial proposal is being developed, dialogue is particularly valuable for identifying in advance any modifications which will ensure acceptability—far better than challenge after launch. In the EU, the innovative mechanisms in the GDPR of the one-stop-shop, lead DPA, as well as the co-operation and consistency procedures, should encourage this two-way dialogue, which is more transparent and based on mutual trust and respect.

"We need regulators to be independent, just as we need judges and referees to be independent. However, independence cannot come at the price of accountability or engagement and regulators need to keep their fingers on the pulse of the market through interaction with industry and consumers…. In a nutshell, regulators must be engaged but not enmeshed, insulated but not insular."[53]

CIPL's Dublin workshop also emphasised that constructive engagement must extend beyond the direct regulator / regulatee relationship. Apart from the obvious importance of interacting with the individuals who are the beneficiaries of data protection, there are many other players and forces which can be harnessed in pursuit of the desired regulatory outcomes. As already mentioned, DPOs, third-party certification bodies and redress schemes can be used to reinforce DPAs' Leadership

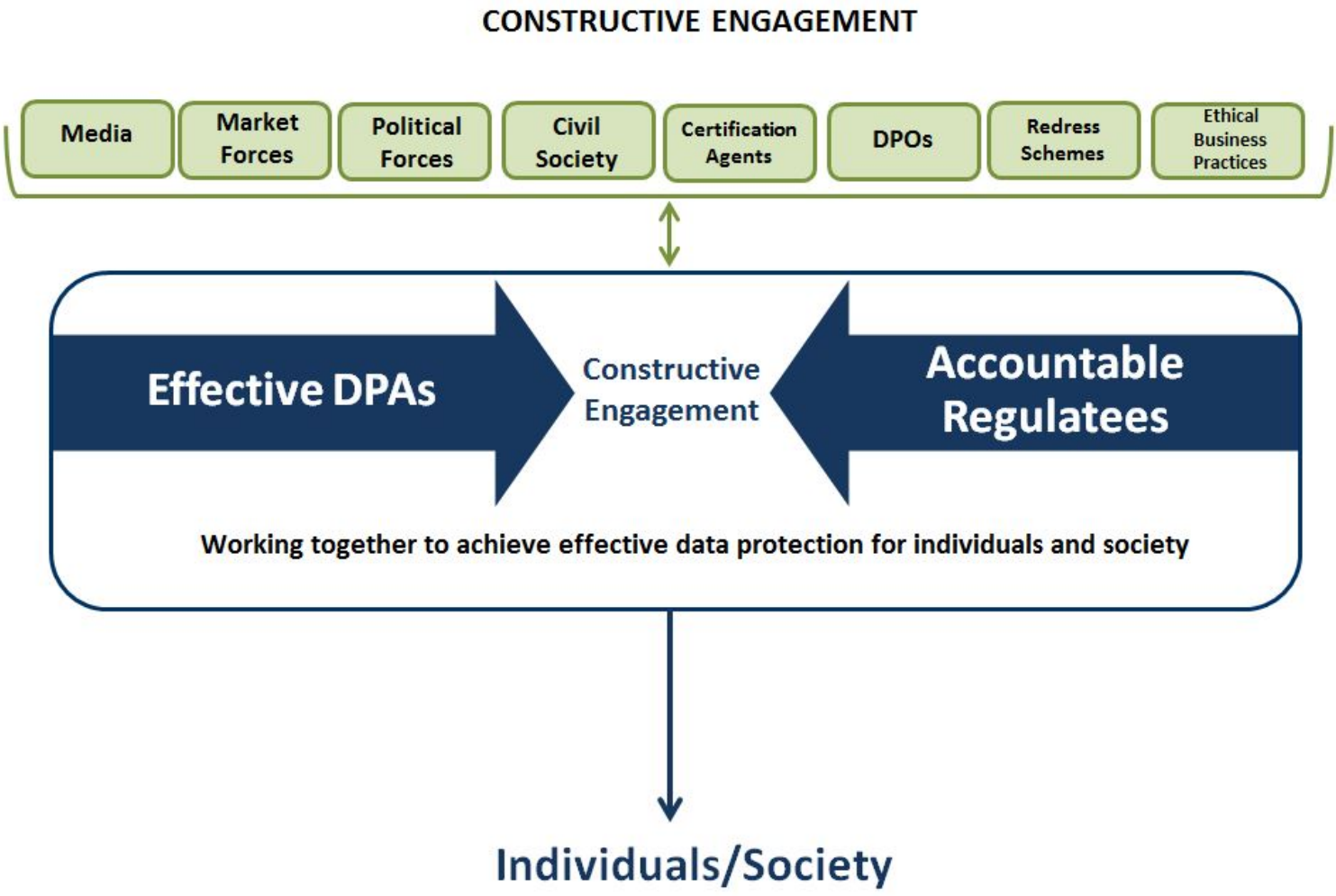
j_8BlDbM5Ljgl43DBuw5ZitB6SZdhk7E&s=UHTdvy5zVo0ee3dA1N5JRiq8X9UDsOY4hU1BgUuAcUc&e.

[52] https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2017/7/personal-data-protection-seminar-2017.

[53] 'Are regulators the new *Men in Black*?' Cavassini, Naru & Below, in *Risk & Regulation* (LSE, 2016) citing OECD, Being an Independent Regulator.

role. Harnessing media and political forces is vital for getting messages across. The pressures of a competitive marketplace, where organisations place enormous value on reputation, likewise need to be fully understood and taken advantage of.

Constructive engagement can be characterised as operating within a "Framework" which captures the contributions of this rich network of stakeholders. The Framework diagram on the next page illustrates the scope for DPAs to engage directly with those regulatees, but also work with a wide range of other organisations and forces.



QUESTION FOR DISCUSSION

1. **What activities and techniques best promote constructive engagement in practice?**

7. Principles for a Results-based Approach

A strategic approach to setting priorities and making hard choices is essential for the effectiveness of DPAs. This applies to each individual DPA, but—as the need for global co-ordination and consistency increases inexorably—there also needs to be the fullest discussion and consensus about how best to maximise effectiveness.

From both the general evidence about effective regulation summarised in section 4, and the more specific analysis of priorities for data protection in section 5, it is possible to draw the threads together and suggest a first draft for discussion of high-level Principles to provide the foundation for a Results-based Approach. The suggested Principles put forward below are in line with approaches already adopted by some DPAs. The Principles, suggested for discussion at this stage, are intended to assist with the setting of priorities—both in terms of ranking functions against each other and for the targeting of particular sectors, activities or organisations.

As well as primarily providing a framework for a Results-based Approach, the draft Principles are intended to promote maximum consistency of strategy amongst DPAs. The Principles have therefore been drafted to have wide application for data protection and privacy regulators on a worldwide and regional basis. The importance of working together to ensure compliance across borders has already been mentioned. But there has to be consistency of strategy as well as information-sharing and pooling of resources.

If their substance is broadly acceptable, it is therefore envisaged that a revised version of the Principles could be adopted and promulgated at four levels:

- Globally, by the International Conference of Data Protection and Privacy Commissioners. A suitable target date might be the International Conference, scheduled for autumn 2018.
- At EU level, by the WP29 and, in due course, by the European Data Protection Board. Ideally this should be done before the GDPR start date of May 2018.
- At Asia-Pacific level by APPA.
- At the operational level by the Global Privacy Enforcement Network (GPEN) and the APEC Cross-border Privacy Enforcement Arrangement (CPEA).

Principles for a Results-based Approach

- *Regulating for Results in the Digital World requires independent Data Protection Authorities (DPAs) to be strategic, effective, co-ordinated and transparent.*

- *The goal of a DPA should be to produce cost-effective outcomes which protect individuals in practice, promote responsible data use and facilitate prosperity and innovation.*

- *DPAs should give top priority to securing protection for individuals.*

- *Each independent DPA should be accountable for transparently spelling out the particular outcomes it is seeking and the priorities and approaches it will be adopting in its regulatory work.*

- *The strategies of all DPAs should be as co-ordinated, consistent and complementary as possible.*

- *Each DPA should adopt a risk-based approach to all its activities, basing priorities on activities that create the most harm to individuals or to democratic and social values.*

- *An approach of constructive engagement with the emphasis on leadership, information, advice, dialogue and support will be more effective than excessive reliance upon deterrence and punishment.*

- *Emphasis on information and advice is especially important in the field of data protection due to its broad impact on so many organisations and the nature of the requirements that are either not precise or are context driven and require judgement in specific situations.*

- *Open and honest relationships with organisations handling personal information, based on constructive dialogue and mutual co-operation, but without blurred responsibilities, will improve overall compliance outcomes.*

- *Regulated organisations should be assessed in particular by reference to demonstrable good faith and due diligence in their efforts to comply.*

- *Organisations trying to behave responsibly and to "get it right" should be encouraged to identify themselves, for example by transparently demonstrating their accountability, their privacy and risk management programmes, the influence of their DPOs and their use of seal / certification programmes, BCRs, CBPR and other accountability frameworks.*

- *Punitive sanctions should be mainly targeted on non-compliant activity that is deliberate, wilful, seriously negligent, repeated or particularly serious.*

- *DPAs should treat regulated organisations in a consistent manner—adopting similar approaches across and within sectors, irrespective of the type or geographical reach of the organisation.*

- *Though the need to deal with individual complaints can be an important component of protecting individuals, handling high volumes is very resource intensive and can impede wider strategic goals. Complaints are a valuable source of intelligence, but should be tightly managed with clear criteria to determine the extent of investigation.*

A Protocol?

Any set of Principles is bound to be high level and aspirational. It may be premature to consider how to put more concrete flesh on to them and bring a Results-based Approach to life as the modern regulatory norm for DPAs. Also, the risk is real that any attempt to articulate specific standards will be seen as some sort of external imposition.

It is absolutely not the vision of this paper to propose any sort of mandatory requirement. CIPL is quite clear that moves towards a Results-based Approach for Data Protection must be taken forward by DPAs themselves. This is not just a matter of their independence. Such an approach will only ever succeed if its central reasoning is embraced by the DPA community. It can never be imposed.

To help this process, and to bring together the main ideas set out in this paper and stimulate further discussion, CIPL has produced a first draft of a Protocol for a Results-based Approach for Regulating Data Protection. The draft Protocol forms Annex D of this paper.

Like the Principles, any Protocol for DPAs can only be agreed and adopted on a collective and voluntary basis with consensus about the basic framework and language. As a possible way forward—not least in the context of developing the Consistency Mechanism—the EDPB could develop its own Protocol to bring the Principles to life and then encourage its adoption by all EU DPAs.

Worldwide (particularly through the APPA network and/or operationally through GPEN and the CPEA) the same Protocol might be adopted by DPAs or the Annex D draft could be taken as their starting point for developing something more tailor-made.

QUESTIONS FOR DISCUSSION

1. Will the bodies bringing DPAs together globally, regionally and operationally consider adopting Principles for a Results-based Approach?

2. How can the suggested Principles be improved?

8. Possible Problems

All strategies involve tough choices. It needs to be openly recognised that a Results-based Approach may bring some challenges and risks. Any ranking of priorities must mean “losers” as well as “winners”. Engagement with regulated organisations may be counter-intuitive and raise genuine worries—both that DPAs may become “captured” and that some regulatees will not welcome excessive DPA involvement in their past, present and future activities.

a. Reluctance to Relegate Functions

DPAs themselves will be nervous about downgrading any function which is cast in terms of a statutory duty. As noted above, in the EU, many of the GDPR functions are written as “tasks” which the DPA “shall” perform. Because the GDPR does not provide any overarching strategic goals for DPAs or any explicit authority to rank some functions above others, DPAs may be reluctant to do so on their own.

There are, however, several answers to these concerns. Despite the lack of explicit authority, some DPAs already adopt their own high-level values or goals. A transparent and strategic approach is far preferable to ad hoc and unpredictable shifts, driven by events, from one activity to another. Low ranking, or tight management of demand, does not mean abandoning any function in its entirety—and this is not suggested here. Even where there is no explicit discretion, there is still room for judgement and proportionality. It is increasingly the norm, for example, for other regulatory bodies to give priority to Leadership functions as being more effective in changing behaviours than their Police Officer role. Indeed, it may be inappropriate for any regulator to take enforcement action, seeking to impose severe penalties, for behaviours which it had not previously identified as unacceptable.

Likewise, a general policy of tightly managing complaints in general, but treating a few as worthy of significant attention, is entirely possible. For example, complaints are commonly received and recorded as prima facie evidence of a problem and yet the vast majority may not be subjected to detailed investigation or resolution. The depth of investigation into each complaint is thus proportionate to the potential severity of the matters involved. This requires robust triage arrangements so that the key features of each complaint can be rapidly assessed and (in most cases) complainants can be told why scarce resources and disproportionate efforts cannot be specifically dedicated for them.

b. Regulatory Capture

There may be anxieties about giving greater priority to engagement with regulatees. There may be some concerns of “Regulatory Capture” if DPAs get too close to organisations which they regulate. Regulatory Capture is described as the process through which the regulated sector can influence and manipulate the agencies that

are supposed to control them. This can be seen as a threat to both the independence and integrity of regulators.

Without a doubt, regulators must always properly manage their relationships with those they regulate, and limit the risk of “Regulatory Capture”. They must be alive to pressures, for example, which could result in improper influence on the selection of “targets” for regulation, excessive sympathy with the needs of those they regulate or more lenient penalties.

With maximum transparency and other safeguards, fears of Regulatory Capture should remain largely theoretical. As happens in every field, independent regulators must be able to have a “grown-up” relationship with those they regulate. This necessitates contact with the regulated sector. A conscious and open “culture of integrity” will help DPAs to resist any pressures from the regulated sector. DPAs are rightly proud of their independence and are mature enough to know that independence also means impartiality—looking carefully at both sides of every issue and weighing up all the facts. A corporate culture promoting integrity and high levels of probity, perhaps with some internal separation of functions, will enable DPAs to make the right decisions about appropriate levels of engagement with the regulated sector, both formal and informal.

c. Regulatee Resistance

There may be corresponding concerns from the regulated community that excessive engagement with regulators could be problematic. Some regulated organisations may prefer to keep their distance from a DPA, perhaps because of fear of a penalty for past misconduct, having documents or practices disclosed to the DPA during consultations and then used against them in an enforcement matter, or fear of veto for a planned innovation. This would, however, be very misguided. Secretive organisations may ironically draw more attention to themselves and it is better to be warned about non-compliance in advance rather than discovering it, expensively, at some later stage. Also, a DPA would risk damage to its own reputation and strategy if it pursued heavy-handed enforcement in response to information disclosed in the course of a supposedly constructive relationship.

More generally, as already stated, engagement is closely connected with organisational accountability and must be a two-way process based on mutual trust. Regulatees cannot expect DPAs to engage in a Results-based Approach unless they also play their part.

Annex A – DPA Functions Under GDPR

In the following table, the main tasks and powers assigned to DPAs have been grouped into one of these four categories. Section 5 of this paper uses this breakdown in the context of setting priorities.

TASK / POWER	ARTICLE
LEADER	
Promote public awareness of risks, rules, safeguards and rights	57(1)(b)
Promote controller / processor awareness of obligations	57(1)(d)
Advise national parliament, government etc.	57(1)(c)
Provide information on request to data subjects	57(1)(e)
Monitor application of Regulation	57(1)(a)
Monitor relevant technologies and commercial practices etc.	57(1)(i)
Give advice on processing operations requiring a DPIA	57(1)(l)
Encourage and facilitate codes of practice, certification mechanisms and seals & marks	57(1)(m)-(q)
AUTHORISER	
Authorise high-risk processing on public interest grounds	58(3)(c)
Authorise contractual clauses for international transfers	58(3)(h)
Authorise administrative arrangements for international transfers	58(3)(i)
Authorise Binding Corporate Rules	58(3)(j)
Approving / accrediting codes, certification mechanisms and seals & marks	42, 43, 57, 58 & 64 *passim*
POLICE OFFICER	
Enforce application of Regulation	57(1)(a)
Conduct investigations on application of Regulation	57(1)(h)
Order controller / processor to provide information	58(1)(a) & (e)
Obtain access to premises, equipment and means of controller / processor	58(1)(f)
Issue warnings and reprimands	58(2)(a)-(b)
Order compliance	58(2)(c)-(e)
Impose limitations and bans on processing	58(2)(f)
Order rectification, erasure etc.	58(2)(g)
Impose administrative fines	58(2)(i)
Suspend international data flows	58(2)(j)
COMPLAINT-HANDLER	
Handle and investigate complaints	57(1)(f)

Annex B – DPA Resources

The most recent comparative survey of DPA budgets was carried out by the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in 2017.[54] The survey responses include resource data for 87 data protection authorities from 58 countries. Of the countries which provided financial resource information, the total global DPA budget for 2016 was €887,320,351.[55]

Financial resource information is available for every European Member State except Austria, Croatia and some of the German Länder. CIPL has taken the financial data from that survey for the 26 EU countries[56] which are included and set the figures against the relevant population numbers. These figures show a total budget in 2016 of €205,703,574 for a total population for that year of 507,471,970.[57] This would suggest, across these 26 countries as a whole, that the budget per citizen was less than €0.41. The actual figure would probably have been slightly higher if the budgets for Austria, Croatia and all the German Länder had been available. The figures for 2017 will doubtless be higher—every Member States' 2016 DPA budget increased from its 2015 figure except for Portugal, Cyprus, Latvia and one German Länd—but it is doubtful that the budget per citizen is significantly more.

It is even more indicative of the demands upon each DPA to establish the number of regulated organisations. Unlike most regulatory bodies, the responsibilities of DPAs are not sectoral and cover all sectors of the economy. In addition, most public bodies fall within the jurisdiction of DPAs and indeed the GDPR imposes some more stringent requirements with corresponding DPA responsibilities.

Eurostat estimates that "in 2014, the EU28's business economy was made up of around 26 million active enterprises".[58] This presumably excludes most public bodies. Very few enterprises now fall outside the scope of data protection requirements. Even the smallest one-person SME is likely to be processing the personal data of customers and other contacts on a mobile phone or laptop. This suggests that, across the EU, DPAs have an average budget of around €8 per business.

[54] The census data is available upon request from the International Conference of Data Protection and Privacy Commissioners Secretariat https://icdppc.org/the-conference-and-executive-committee/icdppc-census/.
[55] Many countries reported their budget totals in local currency. These were converted to euros using currency exchange rates on 27 July 2017.
[56] The figure for Germany is lower than the actual value as only 7 out of 16 Länder provided data.
[57] Population figures were sourced from the World Bank on 27 July 2017 http://data.worldbank.org/indicator/SP.POP.TOTL.
[58] http://ec.europa.eu/eurostat/statistics-explained/index.php/Business_demography_statistics.

Annex C – Basic Conclusions From "Law and Corporate Behaviour"

1) **A regulatory system is most effective where it is consistent and supports behaviours which are widely seen as fair, proportionate and ethical.**

   Regulators should adopt the right incentives and actions that support, and do not hinder, efforts by individuals and businesses to behave correctly. For example, regulators should adopt published enforcement strategies that recognise business attempts to do the right thing.

   Regulators should be cautious about concentrating too much on detailed or prescriptive rules ("tick-box approach") which reduce the ability of those on the front line to think for themselves and diminish both the power and the scope to act in responsible ways. Regulators should influence the propensity for successful businesses to adopt cultures based upon values in which everyone is aligned to focus on the achievement of desired outcomes. Such a culture will, for example, learn from mistakes, avoid blame, put things right when they have gone wrong, welcome complaints and generate ideas for improvement and innovation.

2) **Organisations should be accountable for demonstrating, with evidence, their commitment to behaviour that will attract the trust of regulators—as well as their own management and staff, customers, suppliers, investors and other stakeholders.**

   A business should be encouraged—and sometimes required—to adopt accountable and responsible business practices in everything that is done throughout the organisation. Codes on individual aspects are not enough—the approach has to be holistic. It has to be led from the top, but to exist at every level of the social groups within an organisation.

   Regulators should be looking for evidence that an organisation operates with integrity and has a positive approach to compliance. Mere claims by a company that it can be trusted will clearly not suffice. Evidence may take such forms as governance structures which place emphasis on compliance, consistent adherence to behavioural standards, a high proportion of satisfied customers, consistent application of compliance and audit systems and a transparent approach to external scrutiny.

3) **Learning is fundamental and is encouraged by open and constructive engagement between regulators and regulated organisations, but is deterred by emphasis on "blame" and/or punishment.**

Regulatory systems where learning and maintenance of performance are critically important—such as civil aviation, pharmacovigilance and workplace health and safety—approach "regulation" as a behavioural framework for supporting people to make the right decisions through constant learning.

A critical issue is to identify why a risk or problem occurred, what factors were actual or potential causal factors and how the risk of a similar event can be reduced. The focus is on constant monitoring and learning from events, to improve performance and reduce risk.

However, people will not readily volunteer information if they fear attracting criticism or blame. So, with suitable safeguards, it is essential to encourage an "open culture" of sharing and questioning, rather than a "blame culture" or an adversarial relationship with regulators. This should be the norm except in cases of obvious or serious wrongdoing.

4) Regulatory systems need to be based on dialogue and mutual co-operation which is explicitly directed at maximising compliance, prosperity and innovation.

Ongoing dialogue and mutual co-operation which is transparent to outsiders, rather than an adversarial and distanced relationship, are consistent with systems for management, compliance and risk. These all involve mechanisms based on the circulation of information which monitors performance, identifies risks and makes improvements.

If the primary objective is to bring about the right behaviours through maximum compliance, this is best done by combining regulatory systems with structured and supervised co-regulatory arrangements. Such co-regulatory structures can be developed to include commitments to compliant and ethical behaviour and mechanisms that generate the evidence to support a relationship of trust.

5) Where organisations do break the rules, a proportionate response is needed, with the toughest penalties reserved for deliberate, repeated or wilful wrongdoing.

Although there are obviously many "shades of grey", a modern regulatory regime distinguishes between people who are basically trying to do the right thing and those who are not—largely an issue of motivation. Having fair and proportionate enforcement responses is important.[59] If people engage in non-

[59] See also GDPR, Article 83(2).

compliant activity that is deliberate, wilful or seriously negligent, the law should be upheld with a proportionate response. But where people have been trying to do the right thing or have been generally, but not wilfully, ignorant about their responsibilities, adopting a punitive response would be seen as unfair and not helpful in promoting willingness to comply.

The modern approach to enforcement rests on the proposition that “most organisations are trying to do the right thing most of the time”. That approach can be contrasted with a dominant approach that is repressive, deterrent-based or heavy-handed. Behavioural psychology, especially in the corporate context, does not support the idea that future compliance—or deterrence of non-compliance—is increased by the threat or imposition of strong penalties. The idea that people in the corporate world will obey the law because of fear that a breach will be punished—so it is better to conform than suffer—has been shown to be effective only where there is perceived to be a high risk of identification followed by loss of corporate or personal reputation. The prospect of a financial penalty on the business is not a strong driver for compliance. Ruling by fear in a modern democracy is, in any event, an unattractive policy.

Annex D – First Draft of a Possible Protocol

Draft Protocol for a Results-based Approach for Regulating Data Protection

1. **The effectiveness of Data Protection Authorities is assessed primarily by the extent to which individuals are protected in practice.**

2. **Data Protection Authorities should ensure clear information, guidance and advice are available to help those they regulate meet their obligations to comply.**

- DPAs should provide advice and guidance that is focused on assisting those they regulate to understand and meet their obligations. When providing advice and guidance, the impact of the advice or guidance should be considered so that it does not impose unnecessary burdens in itself.

- DPAs should write information, guidance and advice in plain language and use clear, accessible and concise formats and media appropriate for each target audience. They should consult (as early as possible) on the guidance they plan to produce.

- DPAs should seek to create an environment in which those they regulate have confidence in the advice they receive and feel able to seek advice without fear of triggering enforcement action.

3. **Data Protection Authorities should provide simple and straightforward ways to engage with those they regulate and hear their views.**

- DPAs should have mechanisms in place to engage with those they regulate, enabling citizens and others to offer views and contribute to the development of their policies and service standards.

- In responding to non-compliance, DPAs should clearly explain what the non-compliant item or activity is, the advice being given, actions required or decisions taken and the reasons for these. DPAs should provide an opportunity for dialogue in relation to the advice, requirements or decisions, with a view to ensuring that they are acting in a way that is proportionate and consistent.

- This paragraph does not apply where the DPA can demonstrate that immediate enforcement action is required to prevent or respond to a serious breach or where providing such an opportunity would be likely to defeat the purpose of the proposed enforcement action.

- DPAs should ensure that there is an impartial and clearly explained route to appeal against their regulatory decisions.

- DPAs should regularly invite, receive and take on board feedback, including, for example, through satisfaction surveys of those they regulate.

4. **Data Protection Authorities should carry out their activities in a way that supports those seeking to comply.**

- DPAs should choose proportionate approaches to those they regulate, based on relevant factors including, for example, business size and capacity and the volumes and nature of personal data processed.

- When designing and reviewing policies, operational procedures and practices, DPAs should consider how they might support or enable innovation and economic growth for compliant businesses, for example, by considering how they can best:

  - encourage and promote compliance;

  - improve confidence in compliance for those they regulate, by providing maximum certainty;

  - understand and minimise negative economic impacts of their regulatory activities; and

  - minimise the costs of compliance for those they regulate.

5. **Data Protection Authorities should base their activities on risk.**

- DPAs should take an evidence-based approach to determining the priority risks in their area of responsibility, and should allocate resources where they would be most effective in addressing those priority risks.

- DPAs should consider risk at every stage of their decision-making processes, including choosing the most appropriate type of intervention or way of working with those regulated. Risk assessment should also target checks on compliance and choice of enforcement action.

- DPAs, in making their assessment of risk, should recognise the accountability and compliance record of those they regulate (for example through use of earned recognition approaches) and should consider all available and relevant data on compliance, including evidence of relevant external verification.

- DPAs should review the effectiveness of their chosen regulatory activities in delivering the desired outcomes and make any necessary adjustments accordingly.

6. Data Protection Authorities should ensure that their approach to their regulatory activities is transparent and consistent and is well co-ordinated with the approaches of other authorities.

- DPAs should publish their strategies, annual work plans, standards and targets etc. so that those they regulate know what they can expect from them. This should include, for example, clear information on:

  - how they communicate with those they regulate and how they can be contacted;

  - their approach to providing information, guidance and advice;

  - their approach to checks on compliance, including details of the risk assessment framework used to target those checks; and

  - their enforcement policy, explaining how they respond to non-compliance.

- In a digital society where data does not recognise national boundaries, DPAs should maximise effectiveness, consistency and efficiency thorough close co-ordination and co-operation with their counterparts in other jurisdictions.

Bibliography

This discussion paper has drawn upon various sources. The following publications are particularly helpful.

Responsive Regulation – Ian Ayres and John Braithwaite, OUP, 1995.

A Reader on Regulation – Baldwin, Scott & Hood, OUP, 1998.

The Regulatory Craft – Malcolm K. Sparrow, The Brookings Institution, 2000.

The Governance of Privacy – Colin Bennett and Charles Raab, MIT Press, 2006.

Implementing Hampton: From Enforcement to Compliance – UK Better Regulation Executive, 2006.

Really Responsive Regulation – Baldwin & Black – LSE Working Paper, 2007.

Risk and Regulatory Policy - Improving the Governance of Risk – OECD, 2010.

The Governance of Regulators - Best Practice Principles for Regulatory Policy – OECD, 2014.

Law and Corporate Behaviour - Integrating theories of regulation, enforcement, compliance and ethics – Christopher Hodges, Hart Publishing, 2015.

The European Union as Guardian of Internet Privacy – Hielke Hijmans, Springer, 2016.

Regulatory Theory - Foundations and Applications – Peter Drahos, Australian National University, 2017.