



CASTLEBRIDGE

Changing how people think about information

**Submission on Public Consultation for
Data Protection Commission
Regulatory Strategy 2020-2025**

Contents

Introduction	3
Our approach to this response	3
Assessment of Outcomes	4
Completeness	4
Consistency	5
Relevance	5
Data Ethics and the Supervisory Authority	7
Navigating the Conceptual Landscape	7
The Needs of the Many and the Needs of the Few, or One	10
Responses to Consultation Questions	12

Introduction

Castlebridge is pleased to participate in this valuable consultation process to help inform and shape the Regulatory Strategy for the Irish Data Protection Commission. We believe this is a significantly important period in the global evolution of data protection practices and enforcement.

It is imperative that the Irish Supervisory Authority has appropriate clarity on their mission, objectives, and priorities in the context of this global evolution, while at the same time not losing sight of their critical role in relation to the impact of data processing activities on the fundamental rights and freedoms of people living in, and engaging with organisations, based in Ireland and, by extension, the EU.

The striking of this balance must be addressed in the context of a rapidly evolving pace of change in information management, societal awareness, competing agendas, and the broader socio-economic and socio-political questions pertaining in the evolving information age.

Our approach to this response

In framing our response to this consultation, we have endeavoured, insofar as was possible, to adhere to the Data Protection Commission's format for submissions addressing the Outcomes and the defined Consultation Questions.

We would note, however, that the format and layout of the consultation document and the absence of internal numbering or cross referencing of the defined activities under each Outcome made it difficult to perform an appropriately detailed analysis and cross reference of the strategic goals and activities defined in this iteration of the process.

In addition, we provide appropriate (and we hope relevant) references and examples from our consulting and research activities, including content drawn from *Ethical Data and Information Management* by Dr Katherine O'Keefe and Daragh O'Brien, published in 2018 by Kogan Page and other relevant research on data protection frameworks and information ethics which has been undertaken by Castlebridge over the past number of years.

This submission is structured as follows:

1. Assessment of proposed Outcomes
2. Issues raised from analysis of described activities
3. Response to Consultation Questions

Assessment of Outcomes

The proposed Outcomes were reviewed by members of the Castlebridge team to assess them for:

- Completeness
- Consistency
- Relevance

As a general comment, it is a concern that the high-level strategy statement at this point could be interpreted as being pre-emptively managing expectations of under-delivery (see paragraph 4, page 12). While we recognise that any initial statements of strategy must sometimes be couched with caveats, the constraint on ambition that seems to be expressed here must be addressed through clearly defined goals which are specific, measurable, actionable, realistic, and timebound as part of the implementation of any strategy. These goals should address the development of specific organisation capabilities and competences in the DPC required to give effect to the identified outcomes.

Completeness

In reviewing the actions listed and documented under each of the outcomes identified by the Data Protection Commission, we were surprised to see a comparatively limited emphasis placed on issues of enforcement when assessed against the non-enforcement type actions identified, with only 23 out of the 70 activities identified having an explicit or clearly implicit enforcement component, compared to 47 out of 70 describing activities centred on informing people and/or organisations about issues, or conducting research to inform the Data Protection Commission's own actions and guidance.

Within that, there was an emphasis in the discussion of enforcement on the conclusion of "as many complaints as possible by amicable means", which would seem to be internally inconsistent with the other themes in the activities of improving standardisation of processes and ensuring legal certainty.

While there is an important place and role for amicable resolution in an enforcement strategy, it is a concern that the strategy, at this point, seems to be conflicted on whether the Commission is an ombudsman seeking to promote mediated settlements between parties or a statutory regulator with a specific mandate to uphold fundamental rights enshrined in EU law in a consistent manner.

This represents a key gap in the overall strategic vision at this time which needs to be addressed in the formulation of and codification of the strategy and its associated goals, metrics, and priorities. A critical question needs to be asked as it will define the prioritisation of what core and non-core tasks for the organisation over the next five years are.

Is the Data Protection Commission an ombudsman or a Regulatory/Supervisory Authority with an enforcement function?

It is through this lens that the formulation of any Regulatory strategy should be viewed, particularly with regards to the prioritisation of core and non-core activities or the prioritisation of statutory and non-statutory roles which the Supervisory Authority is called on to perform or contribute to.

Consistency

A high-level review of the stated activities within each Outcome domain was undertaken. This review identified:

- Duplication of some activities across multiple Outcomes
- Internal inconsistency in the allocation of activities under Outcome headings.

For example, we identified 11 activities across Outcome 1,2,3, and 5 which would more logically be described as activities contributing to Outcome 4 as an objective.

In formulating the outcomes, and in describing the activities that are identified as contributing to each outcome, it would be strategically helpful for the dependencies between Outcomes to be identified explicitly so that appropriate decisions on prioritisation and resource allocation can be made in a transparent and consistent manner.

For example, Outcome 4 tasks relating to communication and awareness building contribute to Outcome 2 clarity and certainty objectives, but the scope and focus of Outcome 2 would be on research, litigation, analysis of precedent, and legislative review (for example). The communication and awareness building tasks could be identified as an output of Outcome 4 that supports the overall Outcome 2 objective.

Relevance

Overall, our assessment is that the outcomes selected by the DPC within this strategic planning framework are broadly relevant. However, we would raise a

significant caveat in respect of the focus on Ethics that is explicitly referenced in Outcome 3. The appropriate scope of the role of a Supervisory Authority in the *day to day* implementation of and evaluation of ethical decisions by organisations is open to some debate. A focus on “[Insert Technology] Ethics” is increasingly arising in areas of innovation where the perceived wisdom is that “the law is lagging so we need to focus on ethics instead”, leading to a risk of “Ethics Washing”.

We note that Outcome 3 explicitly references a objective of ensuring that organisations “operate and innovate in an accountable, compliant, ethical, and fair way”. We submit, however, that the primary function of a Supervisory Authority is to ensure accountability, compliance, and fairness as these are enshrined in law. While ethical outcomes are to be encouraged and pursued, it is essential, particularly in the context of constrained resources and hard choices, that a Supervisory Authority is clear about the scope of their function with respect to Ethics.

We will set out a detailed view on this later in this document, based on material from *Ethical Data and Information Management*.

Our review identified two areas where the formulation of the Outcomes could benefit from improved clarity.

- 1) International co-operation and activities related to the development or promotion of global data protection standards or interoperability should be considered a stand-alone outcome given the broad societal value and strategic impact of such initiatives. The inclusion of the international dimension as a component of multiple other outcomes does a disservice to the importance of this element of the DPC’s function but also makes it harder to identify dependencies and clearly articulate priorities in this area, particularly when those priorities compete for resources with “doing the basics” of day to day enforcement.
- 2) The focus on the rights of children is to be commended, but it risks being prioritised at the expense of consideration of the rights of other classes of vulnerable person such as the elderly, or the disabled. Given the historic (and present) use of restrictions on access to services for vulnerable groups by government, or the prevalence of imbalances of power and agency in the relationship between vulnerable persons and service providers, it is important that sight is not lost of these issues as part of a defined Outcome.

Data Ethics and the Supervisory Authority

The role of ethics in data management, and its affinity to the objectives of data protection law and practice of reducing or avoiding the risk of harm to individuals or their fundamental rights or freedoms through the processing of data is trend which has become firmly established in the mainstream of discussion and debate about innovation and implementation of information management systems. However, when it comes to formulating a strategic statement of how a Supervisory Authority can *meaningfully* affect and influence the ethical conduct of organisations with regard to their data management practices, it is important that we avoid simplistic or knee-jerk approaches that may result in over-inflated expectations, under-resource implementations, or ineffective interventions.

Above all else, in the context of a resource constrained Supervisory Authority, priority should be given to actions and activities that are likely to have a meaningful effect and influence tangible changes in behaviours with respect to data and the people it defines, describes, and impacts.

Navigating the Conceptual Landscape

In *Ethical Data and Information Management: Concepts, Tools, and Methods*, Katherine O’Keefe and Daragh O Brien set out a framework for Ethical Information Management that draws on concepts from data management and research in ethics and business ethics.

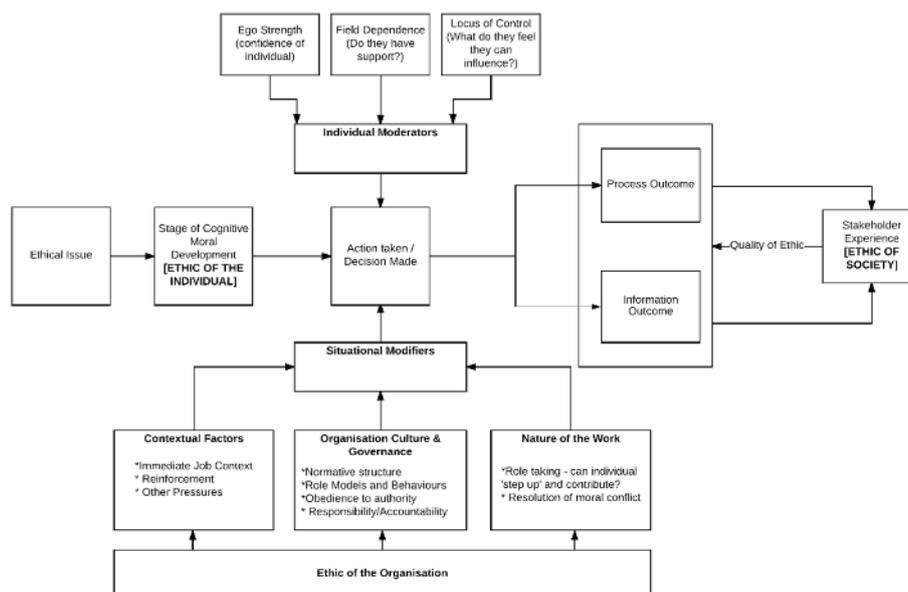


Figure 1: Adapted from Trevino's Interactionist Ethics Model, (c)2017 Daragh O Brien, Katherine O'Keefe

In the context of this model, a Supervisory Authority can influence the Individual Moderators of behaviour, which reflect the factors that enable or prevent individuals in an organisation in their ethical decision making, as well as the Situational modifiers, which reflect the organisational structures and constructs within which decisions are taken in an organisation. They can provide an educational and advisory input into discussions about the “Ethic of Society” and the expectations people may have of process and information outcomes arising from the processing of their data.

However, without effective and meaningful enforcement action which will provide both a clear Situation Modifier for organisations, addressing the contextual factors and organisation governance and culture around data, as well as a clear Individuals Moderator, establishing a locus of control for individuals grounded on “if I raise a concern the Regulator will take action”, any other action by a Supervisory Authority will have little influence on changing how ethical perspectives are addressed in decision making in organisations. Furthermore, unless education and information provision is matched by timely enforcement, the Expectation of Society risks becoming one where apathy about data rights and the impacts on individuals limits the development or expression of an Ethic of Society that properly considers these impacts.

If the experience of individuals in society is that they cannot consistently get the expected information and process outcomes, and they cannot consistently get appropriate and timely support from the Supervisory Authority, the question “Why bother complaining, nobody will do anything?” increasingly is answered by an acceptance of processing activities and ethical data decisions that result in negative outcomes for individuals and society.

The creation of Codes of Practice also provide a key Situational Modifier that can influence the “Ethic of the Organisation”, however these codes are also expressions of the Ethic of the Organisation as they are, by necessity, an expression of how a particular industry sector or collection of industry actors choose to define the minimum standards for data protection for them and their peers. In this context, the role of the Regulator from an ethics perspective should be to represent the Ethic of Society and the expectations of society *as set out in the legislation and case law for data protection.*

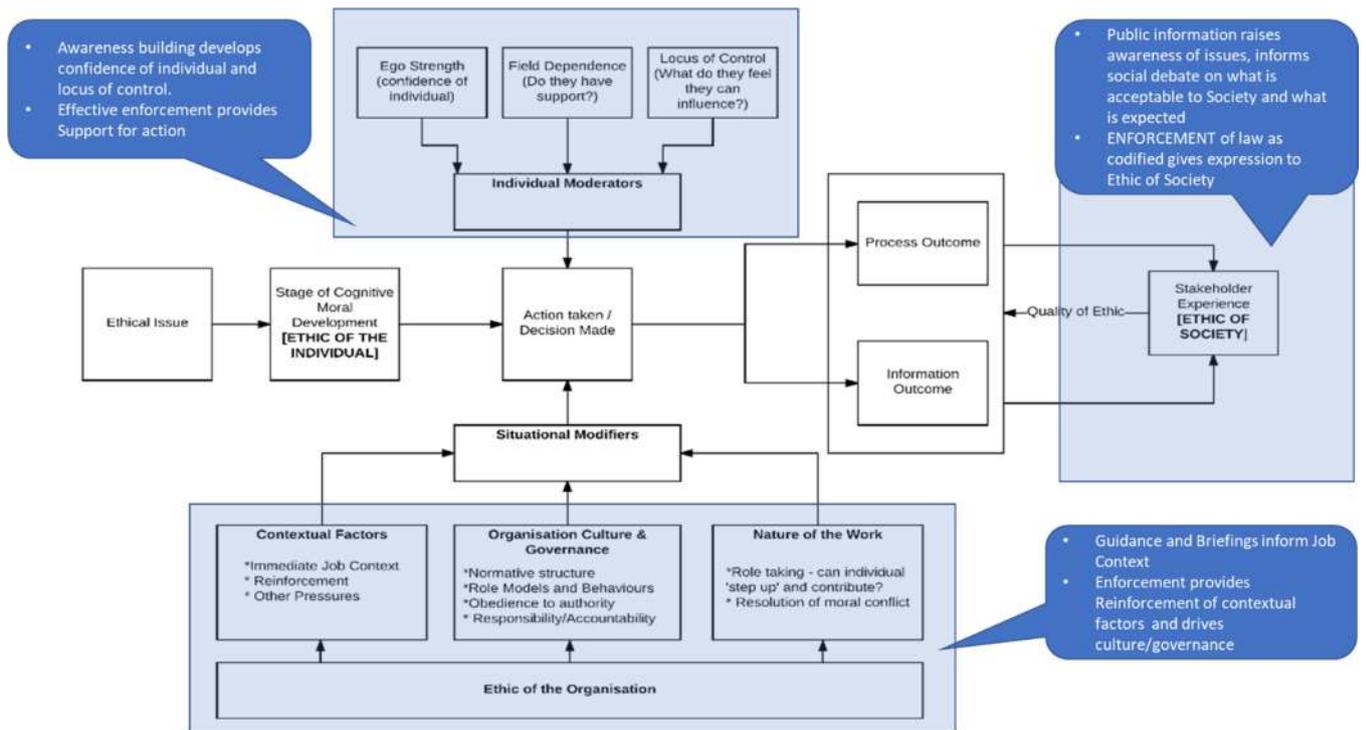


Figure 2: Mapping Possible Regulator Actions to key influence points in Ethical Decision Making

Ultimately, the rule of law that is effect at any given time represents a codification of the Ethic of Society, influenced by the Ethic of the Organisation through lobbying and other activities. Therefore, to give effect to ethics in the context of data management, the starting point for any Supervisory Authority should be the fundamentals of the legislation that is in operation, and the effective and timely enforcement of that legislation through efficient processes that are seen to be effective.

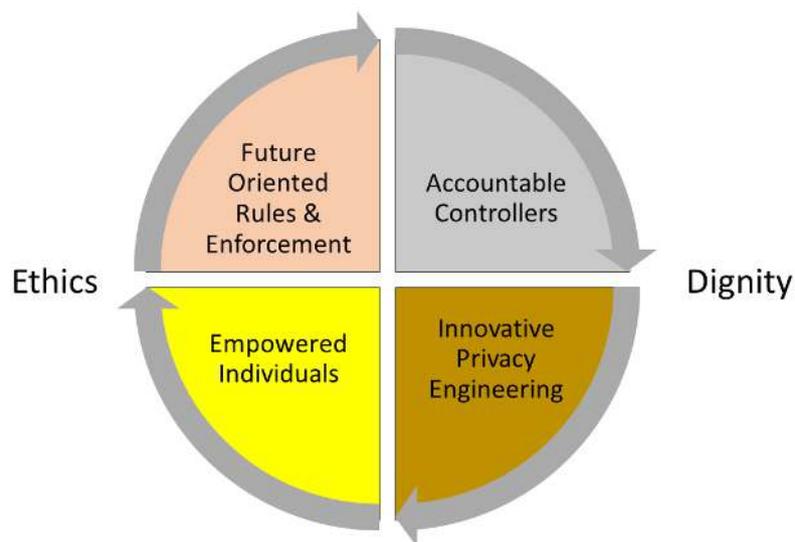


Figure 3 Adapted from EDPS 2015

The Ethical Framework proposed by the EDPS in 2015 recognises this implicitly when they discuss the importance of Accountable Controllers (which requires enforcement to hold controllers to account), Empowered Individuals (which requires data subjects to feel that action will be taken on foot of their concerns), and Innovative Privacy Engineering (which requires clear incentives for organisations to invest in the design and implementation of technologies in a manner that is respectful to and supportive of data protection and privacy).

The Needs of the Many and the Needs of the Few, or One

The question of Ethics in the management and processing of data also arises with regard to the conduct of enforcement actions by the Supervisory Authority and must be recognised in the formulation of the Regulatory Strategy of the organisation.

Simply put, how the Supervisory Authority addresses the challenges of meeting the tangible and immediate needs of the few (i.e. individual complainants) versus the more abstract and intangible risks to the many (i.e. investigation of “Big Tech” will be an ethical statement as to whether the data subject is a means to an end or an end in and of themselves (to paraphrase Kant’s Second Formulation of the Categorical Imperative).

In this context, it is important to bear in mind that the issues and implications for individuals who may have submitted complaints in respect of, for example, a refusal to process a Subject Access Request by a professional body citing sections from Part 5 of the Data Protection Act 2018 as a justification could have significant personal, professional, and even health or welfare implications for the data subject. In such cases, it is of cold comfort to hear that the Regulator is under resourced when a time sensitive complaint has gone without any update or answer for several months.

If a Kantian/deontological framing of the choice facing the Supervisory Authority seems harsh, we can consider this choice through a Social Justice lens. Velasquez et al define this at its most basic as:

“The common good, then, consists primarily of having the social systems, institutions, and environment on which we all depend work in a manner which benefits all people”¹

Therefore, if a Supervisory Authority is to take a meaningful lead in promoting Ethics in information management, it may well be that an appropriate focal point

¹ Velasquez, M, Andre, C, Shanks, T, and Meyer, MJ, (1992) *The Common Good*, <https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/the-common-good/>

for strategic action would be the systems, processes, and culture within their operating environment which impede the timely and effective resolution of issues for data subjects in a manner which has a meaningful and sustainable impact on the behaviours and decisions of Data Controllers with the goal of improving those outcomes and creating the required individual and situational modifiers needed to drive meaningful change in organisations.

This will necessitate a rigorous assessment and appraisal of tasks and activities which do not contribute to these outcomes, particularly in the context of constrained resources. This may result in the Commission having to consider alternative approaches to activities that are non-core to their regulatory enforcement function.

Responses to Consultation Questions

In this section we provide responses to the specific consultation questions raised by the DPC as part of this process. We have broken compound questions out into their constituent parts so that appropriate answers can be given that are sufficiently granular in their addressing of the core issues raised.

Question	Question Text	Response to Question
1a	Is there any other distinct outcome that the DPC should include and why?	<p>International co-operation (outside EU/EEA), including international standards development or regulatory interoperability should be defined as a distinct category of outcome as it raises a broader set of strategic issues than the core regulatory function of the DPC as would be perceived by data subjects. It would allow for the international co-operation and engagement to be clearly recognised as a distinct function and for its relationship to other core outcomes to be clearly identified and measured.</p> <p>In addition, we would suggest that the focus on the rights of children in Outcome 5 should be framed in a broader context of the rights and freedoms of vulnerable persons, including children.</p> <p>Finally, activities and functions that are relevant to Outcome 4 should be moved from Outcomes 1,2,3, and 5 to Outcome 4 for internal consistency.</p>
1b	How would that additional outcome fit with the existing five target outcomes?	

Question	Question Text	Response to Question
2	Which of the DPC's activities have the greatest effect on achieving the target outcome on consistent regulation?	The focus on and reliance on amicable resolution as an enforcement mechanism invites inconsistency in regulation arising from "bespoke" responses to situations and avoidable bottlenecks and delays in processing complaints which are factually clear. A standardisation of process that reduces the reliance on this mechanism, introduces a structured "graduated response" model, and provides a structured approach for decision making on non-complex cases (e.g. SARs denied under incorrect section of Act or where excessive information has been sought) would be preferable and would have a significant effect on the target outcome of consistent regulation.
3	What are the most critical gaps in legal clarity and certainty that may be hindering organisations in being compliant or that may be negatively impacting the rights of individuals?	The most critical gap in legal certainty and clarity is the lack of meaningful enforcement and the delays experienced by Data Subjects in getting timely investigation and action on complaints is a critical gap in legal clarity and certainty. Organisations are uncertain when or if they will receive sanctions, and will therefore be more inclined to take risks or ignore their legal obligations. This combined with unfounded confusion as to the applicability of Part 5 of the Data Protection Act outside of the law enforcement context of a Competent Authority, particularly with regard to the application of limitations on Data Subject rights, is an area of challenge.

Question	Question Text	Response to Question
		<p>Enforcement will drive an awareness of the need for organisations to educate themselves properly and will contribute to quashing the various half-truths and myths that pervade. Often the route to legal certainty is through a decision and a challenge resulting in a body of precedent.</p> <p>Finally, the importance of the “risk based approach” rather than a tick-box approach to compliance needs to be emphasised as organisations are often over-investing in “Data Protection Theatre” while failing to properly address fundamental cultural and awareness gaps. Again – enforcement provides clarity through case studies and precedent.</p>
4	Which of the DPC’s activities have the greatest effect on achieving the target outcome on legal clarity and certainty?	<p>Timely investigation of and resolution of data subject complaints is the activity which will have greatest impact on legal certainty, with clear and consistent processes for moving a case through to resolution.</p> <p>Focussing on amicable resolution as a primary objective in dispute resolution is the antithesis to legal certainty, notwithstanding it may be an acceptable outcome for data subjects in many cases. Education and awareness building activities are contributory to legal certainty, however the old adage that "ignorance of the law is no defence" exists for a reason.</p>

Question	Question Text	Response to Question
5a	How can the DPC set the right balance within the constraints of our legal obligations and our finite resources, so that we have the greatest impact on organisations' accountability and compliance?	<p>The right balance for achieving impact on accountability and compliance requires a reconsideration of enforcement approach. Amicable resolution emphasis should be reconsidered. While it has a valuable function in contentious matters, in many instances it may not be appropriate and in others the delays introduced by an excessive focus on trying to avoid a meaningful sanction impact the data subject, the complained of controller, and the Regulator and contribute to a perception that accountability and compliance can be de-prioritised in organisation.</p> <p>Consideration should be given to how complaints on simpler issues (e.g. delays in SAR responses, failure to implement cookies notices/fair processing notices etc.) are addressed at the individual claimant level. Alternative models based on other areas of administrative enforcement should be considered (e.g. parking fines/penalty points).</p> <p>The comments in this strategy consultation document to the effect that the DPC will abandon investigations when they are more trouble than they are worth was disturbing and this is a key area for reassessment of priorities.</p>

Question	Question Text	Response to Question
5b	How can the DPC influence organisations beyond basic accountability and compliance and towards ethical and fair processing of personal data?	<p>We have discussed this previously in this document. Fair processing is something that falls within the scope of the DPC's regulatory function as it is a principle set out in the law as it is today. The question of Ethics has become a somewhat hollow buzzword and care should be taken to avoid conflating "ethics" with regulation and enforcement, as often the former is used by organisations and lobbyists as a crutch to avoid having to deal with the latter.</p> <p>We have provided a detailed overview of how the DPC can influence and what the nature of that influence should be.</p>
6	Which of the DPC's corrective powers have the greatest impact in terms of their deterrent effect?	<p>The most effective power is the power to order people to STOP doing things (suspension of processing and suspension of transfers (f and j)). Fines are dissuasive but ultimately become a business case calculation for organisations.</p>
7a	How should the DPC's power to impose administrative fines be used to achieve the maximum and most sustainable benefit for people?	<p>We would suggest that imposing smaller fines on a more frequent basis would be an approach to delivering a more sustainable benefit. Also, increasing the speed of progression of complaints, particularly on simple matters, to a decision on an administrative fine would deliver a sustainable benefit.</p> <p>Back in 2011/2012 our founder, Daragh O'Brien, discussed a penalty points/parking fine model for smaller scale offences which would lead to cumulative sanctions for</p>

Question	Question Text	Response to Question
		repeat offenders. While this may require legislative change, for simple cases where the facts are well established it may be an appropriate model to consider.
7b	Should fines be imposed in combination with other corrective powers?	Yes. Fines are often built into the "cost of doing business". Suspension/ordering changes etc. have systemic benefits; Publishing details of sanctions (similar to food safety inspections) will provide information on precedent and create a situation where the risk of sanction for non-compliance will be more tangible for the leadership in organisations.
8	How can we set the right balance between our work on individual complaints and our work on issues that can affect millions of people, so that we have the greatest impact for as many people as possible?	<p>Legally we don't believe you discount individual complaints in favour of large scale action. An individual complaint can have significant impact on the rights/freedoms of individuals, and can lead to precedential value affecting others. Equally individual complaint can bring to light larger systemic issues.</p> <p>It is simply not a good quality management principle to ignore cumulative defects in a system in favour of the high profile, media friendly exploding petrol tank syndromes.</p> <p>Furthermore, as discussed earlier, we believe that any approach that ignores the impact of individual complaints on those individuals who are complaining raises significant ethical issues for a Regulator, who is in effect determining</p>

Question	Question Text	Response to Question
		<p>that the fundamental rights and freedoms of one individual are less important than those of others.</p> <p>The appropriate balance needs to be struck through a reappraisal of enforcement strategy and a shift away from the emphasis on amicable resolution in cases. While an amicable resolution can solve the problem for an individual at a point in time, it does not address systemic failures and does not provide any legal certainty, while consuming potentially greater resources in handling the case.</p>
9a	Which of these activities are likely to have the greatest effect on achieving the target outcome of ensuring that children are specifically protected?	Enforcement will have the greatest effect. Everything else is marketing as no amount of well-reasoned guidance or awareness building will change behaviours in the absence of clear, meaningful, and timely sanctions.
9b	Is there an order in which these activities should be prioritised?	<p>Timely investigation and enforcement should be the priority actions. Development of guidance and awareness building material and EU/EEA level co-operation on standardisation and consistency should be next. The critical aspect of the prioritisation should be driven by a Goal Cascade tied to a very clear strategic focus on the role of the DPC. Hence, if the role is defined as an ombudsman, enforcement actions will be less important than guidance.</p> <p>However, it is unlikely that that positioning of the role would be welcomed internationally as the enforcement posture of other supervisory authorities hardens.</p>

Question	Question Text	Response to Question
10	Are there any other actions that the DPC should be undertaking that will help us to achieve our target outcome of ensuring that children are specifically protected?	<p>Engagement with relevant civic society organisations to develop appropriate codes of practice, and identify and promote "role model" behaviours in the sector.</p> <p>We would note however that the focus on children's rights, while welcome, cannot be at the expense of attention to the rights of other vulnerable persons.</p>
11	What other non-statutory activities of the DPC would positively affect our target outcomes?	<p>In the context of constrained resources, we would question whether increasing the scope of non-statutory activities is congruent with the delivery of the identified outcomes.</p> <p>There is a strong argument that could be made in favour of scaling back on these activities and/or adopting an approach that requires more engagement by organisations with their stakeholders and appropriate advisory supports.</p>
12	What evidence could the DPC use to identify which of its statutory and non-statutory tasks and activities have the greatest effect on achieving the target outcomes?	<p>Definition of KPIs and metrics needs to flow from a clear definition of the strategic mission and priorities.</p> <p>Measuring the trend of enforcement actions as a percentage of complaints could be one potential metric; Behaviour change in organisations, Sectoral awareness surveys and other metrics could be considered. Ultimately, SMART goals need to be defined before KPI formulation is considered</p>