Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CIPL Submission to the Information Commissioner's Office on the Consultation on its Draft Regulatory Action Policy, Statutory Guidance on Regulatory Action and Statutory Guidance on PECR powers

I. INTRODUCTION

The Centre for Information Policy Leadership (CIPL[1]) welcomes the opportunity to comment on the Information Commissioner's Office (ICO's) Consultation on its Draft Regulatory Action Policy, Draft Statutory Guidance on its Regulatory Action and Draft Statutory Guidance on its Privacy and Electronic Communications Regulations (PECR) Powers pursuant to its obligations under s160 of the Data Protection Act 2018 (DPA) and s55C of the Data Protection Act 1998 accordingly.

We have a number of substantive comments that cannot adequately be conveyed using only the short-form survey that the ICO has created for this consultation. Accordingly, we have produced this short paper to supplement and explain our survey response. CIPL welcomes the opportunity to comment on the Draft Regulatory Action Policy and Draft Statutory Guidance on Regulatory Action and PECR Powers. We note that the ICO has a dual role as a regulator, to both promote information/privacy rights, and also to ensure that data and technology can be used in a way that is beneficial and promotes economic and societal goals.

This dual role should be emphasized in the Draft Regulatory Action Policy to reflect the ICO's position as a modern digital regulator, regulating both the industrial and digital economies, that takes into account multiple rights and interests as it performs its role, exercises its supervisory powers, sets out its guidance and engages in enforcement activity.

II. BACKGROUND

By way of context, we note that the ICO is obliged to produce statutory guidance on some of the Information Commissioner's powers - under PECR and the DPA. However the ICO is a

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 89 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

regulator for many other areas as well. These new draft documents update the Regulatory Action Policy (RAP) of 2018. The ICO has now decided to separate the statutory guidance from the RAP and create two documents: the RAP 2021 and the Statutory Guidance on the Regulatory Action. The Statutory Guidance on the PECR Powers replaces the retained statutory guidance "Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the DPA 1998. The suite now looks as follows:

- A Regulatory Action Policy which covers all the ICO enforcement functions
- Statutory Guidance on PECR enforcement
- Statutory Guidance on the DPA 2018 powers

The suite of documents is intended to set out a coherent approach to the use of all the ICO powers. CIPL welcomes the introduction of a coherent set of documents covering both regulatory policy and statutory powers. CIPL recognizes that, throughout the suite of material, the Information Commissioner has aimed to provide sufficient detail to properly explain his policy without burdening the text with legal detail which may make it less accessible to some readers. Overall CIPL commends the clarity and readability of the text[2]. CIPL also appreciates that links to the legislation and other guidance are included. However, we recommend that the introductory section, headed **About this guidance,** include a statement that the guidance does not set out all the detail of the Commissioner's enforcement powers or how the law applies them in all circumstances. The section should make clear that these are set out in legislation and further explained in the Commissioner's other guidance.

This may seem like a statement of the obvious to anyone familiar with the field. However it addresses the risk that less well-informed readers who refer to the guidance will assume that, because it is statutory guidance, it is a comprehensive statement of the Commissioner's powers and any limitations on those powers.

CIPL also recommends that the guidance include a statement that there is no legal hierarchy governing the use of the various powers, except in relation to monetary penalty notices ("MPNs"), for which the ICO is required to serve a Notice of Intent ("NOI") before issuing a fine. For example the Commissioner does not have to serve an information notice before taking enforcement action or before serving an assessment notice.
In particular, CIPL welcomes the following features:

[2] A minor comment is made on drafting in the Appendix

- the ICO has taken on board some of the responses to the previous consultation[3] e.g. over coherent structure of material and some of the comments on content.
- the commitment of the ICO to transparency in publishing policy approaches. Although, we consider that in some areas improvement is still needed.
- the overview of its ICO legal responsibilities and the section on how the ICO meets its obligations to support economic growth.
- the inclusion of the further reading and references, the material on international work and on working with other regulators.
- the explanation of the ICO's engagement as part of the Digital Regulation Co-operation Forum (DRCF) – CIPL very much welcomes this initiative.
- the overview of the participation of the ICO as an active participant in a range of global data protection and information rights fora
- the risk-based approach **(see previous submission[4])**, although CIPL notes that there are still points to be addressed.

Given the significance of the issues addressed in the Draft Statutory Guidance for the RAP and PECR, which go to the core of the ICO's enforcement strategy, controllers and processors are key stakeholders and should be specifically targeted as part of the consultation. In preparing the Draft Statutory Guidance for the RAP and PECR, the ICO is conducting 'a formal consultation with the public'. Section 160(9) of the DPA obliges the ICO to consult 'such other persons as the Commissioner considers appropriate', which should include those who will be most affected by the two Draft Statutory Guidances. As the ICO has done for other significant guidance, it should consult widely in preparing these two Draft Statutory Guidance, including industry bodies, groups representing controllers and processors, rights organisations and civil society as key stakeholders. Recent enforcement action by the ICO indicates that (unsurprisingly) organisations will closely evaluate and may in all likelihood challenge the ICO's enforcement strategy and guidance. Given this, the ICO may wish to consider engaging proactively to ensure that the full breadth of organisations have had an opportunity to respond, beyond those who respond to the public consultation.

[3] Summary of responses from the statutory guidance public consultation (October 2020) https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-rap-statutory-guidance-on-our-regulatory-action-and-statutory-guidance-on-our-pecr-powers/

[4] See CIPL Paper on Regulating for Results - Strategies and Priorities for Leadership and Engagement (October 2017) https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf

III. GENERAL COMMENTS ON THE REGULATORY ACTION POLICY (RAP)

The RAP should clearly demonstrate the ICO's commitment to ensuring an effective and proportionate regulatory response, evidencing the ICO's risk-based approach, and emphasizing the role of accountability.

The RAP should reflect more deeply the **ICO's risk-based approach to supervision and enforcement**: The ICO has championed its risk-based approach to regulatory oversight and enforcement in numerous public statements, parliamentary hearings and other regulatory guidance (e.g. the RAP and its regulatory approach issued during the coronavirus pandemic6). The same approach should be reflected more explicitly in the Draft Statutory Guidance for the RAP and more explicitly in every enforcement action taken. We support that the Draft Statutory Guidance notes at the outset that the ICO takes a risk-based approach to taking regulatory action. Adopting a risk-based approach is beneficial to all parties, including the ICO, which will incur very high costs if it pursues punitive regulatory action against every organisation, without regard to the impact of the particular infringement and applicable circumstances.

Accountability should be an explicit and strong mitigating factor when considering regulatory enforcement. In exercising its statutory powers, the ICO should emphasize the role of accountability and organisational commitment to compliance, as well as behaviours that go beyond just legal compliance, as mitigating factors that will be considered following infringement. An assessment of accountability (from data protection management programs to formal certifications and adherence to codes of conduct) and best efforts to comply should be addressed explicitly as part of the ICO's risk-based approach. The ICO should actively encourage accountable behaviour from organisations by explaining how it will factor accountability into any assessment of infringement, and in determining an appropriate regulatory response, including the quantum of sanctions. There should be specific consideration of whether an organisation takes into account the ICO Accountability Toolkit in building and implementing its data protection management program. The adoption of the Toolkit should be explicitly mentioned as one of the factors that may be taken into account in any enforcement action. Acts of non-compliance do not take place in a vacuum, and should be considered within the context of an organisation's wider data protection management program and any external certifications or adherence to a code of conduct. The same act of non-compliance should be evaluated differently by the ICO where an organisation has made best effort to implement and maintain an extensive data protection management program, compared with an organisation that has committed wilful acts of non-compliance. Further, the intent or good faith effort of an organisation should be a consideration when establishing the action that will be taken against it.

For example, if an organisation has carried out a data protection impact assessment, considered the risks and attempted (in good faith but albeit unsuccessfully) to mitigate them, this should stand it in better stead than an organisation that has wilfully or negligently disregarded the existence of risk. Similarly, the level of oversight and supervision that senior management provides with respect to data management should be considered, as well as other elements of accountability, as advocated by the CIPL Accountability wheel and the ICO Accountability Toolkit.

An outcome or results based approach to data protection regulation. An outcome or results-based approach to data protection regulation is one in which DPAs seek to maximise effectiveness by adopting modern, risk-based and strategic approaches to regulatory functions that achieve the best outcomes for individuals, society and organisations. It involves responsibly engaging with, and supporting those organisations that are trying to "get it right" while also dealing firmly with those not trying.

An outcome/results-based approach provides many benefits to different stakeholders. It benefits individuals by making sure that they are protected in practice, not just on paper. It benefits organisations through providing consistency, predictability and constructive engagement with the ICO. It also benefits the ICO itself by ensuring that it makes the best possible use of available resources to achieve the best outcomes.

Studies of regulatory effectiveness in other sectors provide insights applicable to data protection[5]. Many regulatory spheres now focus on an outcome-based approach focusing on engagement through information, advice, support and incentivising good practices rather than only deterrence and punishment. These approaches also rely on the nudge theory of behavioural economics, whereby a regulator should deploy carrots and not just sticks. This means that the regulator should encourage and reward those organisations that are demonstrating good faith and a commitment to data privacy compliance. Regulators should also understand and leverage the self-interest and motivation of organisations and their leaders to "get it right." Such a positive and proactive approach is one way that the ICO can achieve maximum effectiveness. Enforcement should be reserved for those engaged in deliberate, repeated or wilful wrongdoing.

[5] Ethical Business Regulation; Growing Empirical Evidence, Christopher Hodges, Wolfson College, University of Oxford, 2016 available at https://www.fljs.org/sites/default/files/migrated/publications/Ethical%20Business%20Regulation.pdf

The essence of the results based approach is that it challenges businesses and regulators to cooperate to achieve common purposes and outcomes. It aims to incentivise people and organisations to engage more so as to agree their common purposes and objectives and to achieve their agreed common goals. It aims to combine multiple goals of business (commercial success and profit), governments, regulators and societies (economic growth and protection from harm) with acceptable risk. It achieves this by enabling organisations to opt for basing their activities around demonstration that they can be trusted[6].

The current linear model to regulation is focused on creating rules, identifying breaches of those rules and imposing sanctions for those breaches. It assumes that sanctions will deter bad behaviour and achieve better current and future compliance, but the empirical evidence suggests otherwise, both within the privacy sector (where some very significant fines have been imposed with little or no reaction in terms of customer engagement/uptake with the fined entity, and little or no impact on the share price of the entity, supporting the conclusion that fines are factored in as a "cost of doing business" rather than acting as the deterrent they were intended to achieve), and in other sectors such as financial services.

Leveraging the learnings of behavioural science, there is an opportunity in build on the reality that humans achieve more when they cooperate. This cooperation takes the following form:

- Agree common purposes, objective and outcomes
- Build relationship based on trust, and evidence of trustworthiness
- Evaluate evidence based on common ethical values
- Everyone to play their part
- Measure the achievement of the purposes, objectives and outcomes

This approach ensures a virtuous circle, or continuous improvement model, which can flex as maturity evolves, external pressures change and trust increases.

When parties are actively engaged, with clarity on the purposes, object and outcomes desired, there will be less need for regulators to need to resort to enforcement (except for those organisations which deliberately or negligently choose to breach their obligations). The aim of regulation should be to engage all parties on the same journey toward an overall public good.
These approaches generate the culture change necessary within organisations to ensure consistent and lasting approaches to compliance. It also means that fining becomes an action of

[6] O O'Neil, A Question of Trust (Cambridge University Press, 2002). Many other sources include N Luhmann, Trust and Power (John Wiley & Sons, 2018); BA Misztal, Trust in Modern Societies (Polity Press, 1996); AB Seligman, The Problem of Trust (Princeton University Press, 1997); P Sztompka, Trust. A Sociological Theory (Cambridge University Press, 1999).

last resort, rather than a primary or first tool of regulation, which adversely impacts confidence and trust between both businesses with the regulator, and for the individuals ultimately impacted. CIPL supports and would encourage even **further constructive engagement between the ICO and regulated organisations.** Constructive engagement in the data protection sphere consists of many activities:

- Maximum Transparency: The ICO should be transparent in setting out its priorities, expectations and working methods, which will help the ICO 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 ICO, without fear or the threat of self-incrimination.
- Practical Guidance: This involves guidance 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: This includes open and closed meetings between the ICO and regulated organisations, technologists, industry associations, experts and academics to communicate concerns and expectations. These meetings can also be important to find out about legal uncertainties, trends, commercial and technology developments, etc.
- "Regulated Self-Assurance" and co-regulation: 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 the ICO.
- Maximum Consultation: There should be a "no surprises" approach to regulatory strategy, rulemaking and regulatory guidance, which means getting feedback on proposed strategic plans, draft rules or guidance from stakeholders before final adoption. Such dialogue is especially beneficial where there are new requirements or no common views on what is the "right thing" to do to comply, or even what harms should be prevented.
- Frank Exchanges: A willingness to participate in confidential discussions, often with a market leader, about the implications and acceptability of a technological innovation.

Encouraging a "race to the top"

Increasingly, regulators are recognizing that organisations look to each other to benchmark appropriate practices and that they tend to follow the leaders among them. 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 the ICO to leverage this tendency

by 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. In this way, DPAs leverage market forces to promote a race to the top, with companies competing on privacy, security and trust.

- Incentives: Corporate leadership will take data protection and privacy more seriously if the ICO can create and communicate incentives for good faith privacy and compliance programs. Such incentives can include the ability to share data across borders, engage more broadly in big data and machine learning activities, provide services to the public sector and, crucially, for accountable practices to be recognized as mitigation factors in enforcement.
- Creating Space for Responsible Innovation: There is considerable scope for building compliance solutions cooperatively. The regulatory sandbox offers one such possibility. "Policy prototyping" is another approach where possible policy positions and legal rules are tested on a cohort of willing entities, including SMEs or start-ups, to provide concrete, experience based input from those implementing the rules. This ultimately helps create more viable and effective rules. "Design Thinking" is another method whereby data privacy requirements and compliance challenges can be addressed, made scalable and developed bottom-up, by multifunctional teams. The concept of "design thinking" may also provide opportunities for regulatory participation and engagement with regulated organisations and experts from other areas (e.g., behavioural economists, user-centric designers, technology engineers, marketing and customer relationship experts).
- Reiterative and Dynamic Compliance: Just like with technology and software development, it would be helpful if both the ICO and regulated organisations approached compliance as a reiterative, dynamic and ongoing 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. Just like technology deployment, compliance should be agile and subject continual feedback. This approach 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 ICO success in directly influencing the spread of good practice, preferably with common and/or comparable metrics.

Organisations need to know that their best efforts will be recognized and given due consideration.

Building trust and transparency is dependent on openness and regular engagement. Regulatory sandboxes are a key bridge to enable businesses to share their innovations with the regulator and to work together to a compliant approach. Sandboxes also provide an excellent opportunity for regulators to keep abreast of developments, to help them develop their policy thinking, and to work with business to navigate through new and evolving scenarios, challenges and opportunities to ensure privacy compliant approaches and a flexible and forward looking regulatory approach. An approach which supports innovation rather than putting unnecessary hurdles and obstructions to UK economic growth and development. Leveraging the breadth of these tools will help organisations to develop practical approaches to compliance which, when widely adopted, will encourage other organisations, particularly SME's who struggle with the complexity of data protection obligations, to adopt proactive compliance. Compliance will only become a norm when it is part of the culture; when it becomes an accepted way of organisational behaviour which generates tangible benefits, rather than a hurdle and penalty-based approach which results in a tick-box compliance. Clarity on how best efforts as demonstrated through accountability practices should be explicitly included in the Draft Statutory Guidance.

Codes of conduct, certifications and other industry tools can help ensure and demonstrate compliance.

If codes of conduct, certifications, BCR's and other industry tools were more accessible, flexible, cheaper, scalable and faster to obtain, particularly if administered by third parties rather than resource limited regulators, these would be helpful in developing a culture of data protection compliance. These tools would also enable regulators to focus their efforts and resources on deliberate wrong-doings and organisations that do not engage in accountable data protection practices. An explicit reference to the role of these sorts of tools would be helpful in bringing further clarity to the Draft Statutory Guidance.

Promoting best practice and ensuring compliance is a key element of the RAC and Draft Statutory Guidance.

CIPL welcomes that this is stated in both the RAC and Draft Statutory Guidance, but would suggest that this could be further developed to reflect the approach to proactive compliance. Regulatory action, depending on how it is executed, can help drive improvement in standards in a balanced, fair and proportionate approach. For example, we support the approach taken in

the Age Appropriate Design Code where the ICO led a process of consultation, thought leadership and iterative drafts which enabled industry and others to participate. The ICO further accepted a period of adjustment for controllers to bring their operations into line with the clarified requirements. This approach facilitated improved open dialogue and understanding of both the legal and practical issues of the challenges at hand, and enabled all parties to better assess the impact of changes for firms and for individuals, thereby avoiding a response from the ICO which is more likely to be challenged.

The reality is that businesses are operating in an increasingly complex environment where businesses are subject to multiple, often conflicting, regulatory pressures.

Having the ability to work with the ICO to navigate these different requirements to achieve an outcome which is acceptable across the board, together with achieving an improved understanding of the various issues and requirements in play, is very helpful. The level of interest expressed in participation in the Sandboxes which the ICO has run, and the ICO's own positive feedback on these initiatives, is evidence that these approaches generate positive outcomes for both business and individuals, together with enhancing the ICOs toolbox.

By contrast, there is an increasing body of evidence which demonstrates that the crude use of immediate penalties or orders on existing business practices where business is given no opportunities to work with regulators to agree societal solutions does not generate positive outcomes in the same way. As the work of the DRCF has recognized, data powers both the traditional and digital economy, and its impacts are felt across all sectors. Organisations are therefore increasingly subject to multiple legal and regulatory requirements which may overlap, be inconsistent, or event conflict. In the digitally connected world, and given that breadth of data processing across all sectors, with the potential to have a huge impact on a wide range of systems and processes, it is critical to achieve regulatory coherence.

However, with the ICO less well funded and resourced than some of the other regulators in the DRCF, it will be essential for the ICO to ensure that there is an appropriate balance attributed to the data protection elements of the combined data issues in the cooperative framework moving forward. The ICO has a broader reach than any of the other regulators across multiple sectors, and so is uniquely placed to see and influence the impact of a cooperative regulatory approach to data.

Additional clarity would be helpful as to how the Draft Statutory Guidance will interact with other ICO policy and guidance documents.

The relationship between the two Draft Statutory Guidances and the RAP should be clarified. The RAP sets out the ICO's approach to taking enforcement action across all of the areas that the ICO regulates, including data protection. The Draft Statutory Guidance on the RAP explains how the ICO will exercise its functions in connection with information notices, assessment notices, enforcement notices and penalty notices, and the Draft Statutory Guidance on PECR explains how the ICO deals with its powers to impose monetary penalty notices. There is a fair amount of repetition of relevant portions of the current RAP. Clearly the Draft Statutory Guidances are intrinsically linked to the RAP and they should be read together and refer to each other. This would assist organisations in understanding precisely the ICO's policy and intention, the behaviour that the ICO expects of them, and the nature of the enforcement action to which they may be subject. The RAP and two Draft Statutory Guidances should identify the documents they are designed to update/replace and make clear the time period from which it will apply. It would also be helpful to clarify whether earlier guidance or statements in other ICO materials, such as the general guide to the GDPR, will be taken into account in considering regulatory activity covered by the RAP and Draft Statutory Guidances. If this is the case, there should be a clear statement that this is replacement guidance, and clarification of whether this document replaces all prior material produced by the ICO on the subject of these powers or only the prior version of this particular document. Apparent overlap with other regulators and regulatory supervision should also be clarified. Overlap and cooperation with other regulators and regulatory supervision will be an important interface for many businesses, such as in the financial services sector, in relation to competition law and consumer protection law, or in respect of forthcoming online harms regulation. This overlap and convergence of different regulators is helpfully recognized in the engagement by the ICO in the relatively new DRCF, recognizing the increase in growth of the digital economy and data use in all sectors. See our additional comments above on the engagement of the ICO with the DRCF.

IV. DRAFT STATUTORY GUIDANCE ON THE RAP

Sections of the Draft Guidance lack detail and clarity that would assist organisations and aid transparency.

The structure and language of the Draft Statutory Guidance should be consistent and clear. There is inconsistency between different sections of the Draft Statutory Guidance, which may disadvantage an uninformed reader. To ensure clarity and transparency, the same material should be reproduced with respect to each type of notice, preferably with the same set of headings. For example, rights of appeal, or the formalities with respect to each type of notice should be clearly set out. Currently, the section on enforcement notices lists what the notice will contain, and includes a reference to the appeal process. In contrast, the sections dealing

with information notices and assessment notices do not mention rights of appeal at all, despite the availability of such rights in respect of both types of notice. Each section should also fully explain the rights of organisations, and the exemptions or limitations that may apply. In addition, some statements appear contradictory. For example, with regard to assessment notices, the Draft Statutory Guidance states: "We will access the minimum amount of information we need to assess whether the organisation is handling personal data appropriately"(page 13). A few sentences later (page 14), it states: "Organisations can contact us to request that, if an assessment notice requires access to such information, this access is limited to the minimum required to adequately assess their compliance with the legislation." This suggests an organisation must actively request that access is limited, and it is not clear whether an organisation will be told of the ability to request a limitation on access to certain types of material.

The extent of the ICO's discretion, and how it will be exercised, should be made clear. The Draft Statutory Guidance makes reference to the issuance of notices when the ICO is "*exercising our discretion*"[7]. While the ICO has a degree of discretion, there are specific statutory obligations with which organisations are required to comply, and it is non-compliance or suspected non-compliance with these obligations that should trigger action by the ICO, not the ICO's judgment alone. At the same time we recommend some more clarity on when particular actions are likely to be triggered as between the use of information notices, assessment notices and possibly warrants as methods to carry forward investigations. CIPL notes that in the section on assessment notices there is a useful statement on the circumstances in which an assessment notice would be potentially triggered (under the heading **When would we issue an assessment notice**.) This includes cases where there is existing evidence of non-compliance. However the equivalent section on information notices does not state what the triggers for an information notice might be. Presumably these are when a complaint has been received or information received which indicates a real likelihood of non-compliance and an investigation is considered appropriate. The section covers the factors the ICO would consider relevant to serving an information notice rather than proceeding by correspondence or less formal enquiry, but not what would be likely to trigger one.

It is also noted that the public interest is listed as a discretionary consideration in relation to service of an information notice, but not in relation to assessment notices or enforcement notices. CIPL recognizes that some considerations, such as damage or distress to individuals or public interest in compliance, will be relevant to the exercise of all regulatory powers, but also, as these are different regulatory tools, different considerations will weigh in relation to particular powers and it cannot be an exact science to list all possible considerations.

[7] Page 8 Statutory Guidance

Nevertheless it seems anomalous to refer to public interest only in relation to information notices and we would suggest it be included as a generally applicable consideration to the exercise of any regulatory power.

Information notices

What may trigger the issuance of an information notice is not made clear in the Draft Statutory Guidance. For example, is an information notice likely to be issued following a breach? Following a consumer complaint or a tip-off from a third party? Following an inquiry from the organisation itself on a data protection matter? This latter question is important, as some organisations may avoid seeking information or advice on data protection issues from the ICO if they believe that a query might spark a regulatory inquiry. It is also not clear whether an information notice will only be issued in the event that the ICO suspects there has been an infringement of data protection law, or in other circumstances. Section 142(1) of the DPA provides that an information notice may be issued to require an organisation to provide the ICO with the information it "reasonably requires" for the purposes of carrying out its functions under data protection legislation, but organisations would be assisted if the ICO could provide some concrete examples or criteria for when such a need would be likely to arise. The ICO must also set out in the notice the basis on which it is given and why the ICO requires the information.

We note that under the section headed, **When would we issue an enforcement notice** there is reference to the possibility a party had not responded to an information notice. We can envisage this being used by those subject to assessment notices to argue that the Commissioner should first have served an information notice. We suggest the guidance makes explicit there is no hierarchy; the ICO must make a judgment on all the facts and circumstances on what is the appropriate and proportionate action in each case.

In addition, it would be helpful for controllers and processors to be reassured that information notices cannot be used for "fishing expeditions" and also to have some guidance on the likelihood of the specific regulatory tool they may face in different circumstances.

Assessment notices

In relation to assessment notices CIPL notes at Page 16 that it is explained that a draft report will be provided to the party assessed *"for the purpose of identifying factual errors".* The examples given are correcting names. It would be useful to include some brief explanation of how the matter will be handled if there are substantive differences of view of the facts. Clearly

the ICO must be able to call a halt to matters and parties cannot expect to re-write the ICO's assessment reports in their own favour, but it is assumed there will be cases where there is a genuine dispute over relevant facts, and it would be useful to have some guidance on how these are handled.

CIPL would also reiterate a further point made in its submission on the previous document that s.160(4)(c) requires that the Draft Statutory Guidance include provisions specifying the documents or information that are not to be examined/inspected, or those which can be examined/inspected only by certain people. While the Draft Statutory Guidance explains a number of these cases, it does not cover all of those specified in s.147, for example a controller or processor processing for the special purposes. CIPL is sympathetic to the view that these are unlikely to be relevant to the majority of readers. Nevertheless they appear to be required by the legislation and should be included.

Statement of law

CIPL notes that the inaccurate statement of the law from the previous draft which suggests that enforcement notices can be served for future breaches has still been included (see page 18 "processing or transfer of information to a third country fails **(or risks failing)** to meet the requirements of the data protection legislation")**.** In our view this does not reflect the law, under which the ICO must be satisfied that 'a person has failed, or is failing' to comply. It is not sufficient that a failure may occur in the future.

Penalty notices

CIPL notes that the material on the use of panels has been extended, on page 25. This explains that in some cases a panel may be convened to advise on penalty amounts or other corrective measures. It is helpful that this is included in the Draft Statutory Guidance. However the placement of the material is confusing. It appears that a panel is only convened where a penalty is being considered but it can also consider the application of other corrective action such as an enforcement notice. It is not clear when such a panel would be convened, whether before a Notice of Intent has been served or after, and how the panel would interact with any representations received. It would be helpful if the panel section was separated out under its own heading and a clearer description of when it would be involved and its role included. It would also be useful to understand in broad terms the composition of the panel and how it is selected and if the organisations have the ability to make representations to the panel.

Steps for determining whether a penalty notice is appropriate and setting the fine

CIPL welcomes the expansion of the explanation of the aggravating and mitigating factors considered relevant to the service of a penalty notice and the list of other factors which may be relevant. CIPL also welcomes the fact that more detail has been provided on the factors to be considered in determining whether the overall penalty sum is effective, proportionate and dissuasive. However, CIPL is disappointed that the complex nine step process for assessing a penalty has been retained. We still stress that the starting point of any penalty assessment should not always be the turnover of an organisation. Specifically, CIPL recognizes that, in order to ensure fairness and consistency in setting the level of fines, the ICO needs to establish a standard methodology which can be used to assess the appropriate level of the penalty sum. We also recognize that penalties must be of a level to act as an effective deterrent. However, it is often the case that reputational damage caused by enforcement action by a regulator, or a requirement to implement an accountability based privacy management program, has more impact on organisational behaviour that a financial penalty. The calculation of penalties should take this into account.

1. **Step 1 – Seriousness of the breach**

CIPL notes that the previous calculation model, which included consideration of both the level of breach and the level of culpability of the party has been changed. The guidance now classifies breaches as being of low, medium, high and very high seriousness. Two new factors have been added. These are:

a) previous history of compliance and
b) reporting

Previous history of compliance

Previous history of compliance is an important element of supporting the approach to accountability and the ICO's accountability framework. Accountability, coupled with a recognition of the risk based approach, are important elements for consideration. Organisations which are able to demonstrate an accountability driven approach to data protection compliance and the existence of a privacy management program, should be able to have their efforts recognized in the context of an assessment of previous history of compliance when determining the seriousness of a breach. In terms of the risk based approach, it may be tempting to approach this from hindsight, which is neither fair nor reasonable. When assessing the risk based approach, care must be taken to ensure that the assessment considers the

factors relevant at the time which informed the risk based approach, and not those factors which may benefit from hindsight.

Reporting requirements

It is not made clear that notification to the ICO is only mandated in specific cases. Reporting requirements under the legislation are applicable only to notice of breaches of security under Article 33. There are no other legal obligations to report breaches to the ICO. (If all breaches had to be reported the ICO would disappear under the weight of reports.). Accordingly the issue of reporting will only be relevant in a limited number of cases. Where there is no legal duty to notify the ICO and there is no specific reason to do so by the nature of the breach, this is not a relevant consideration. It certainly does not go to whether or not a breach has occurred.

It cannot be taken into account in other cases e.g. failure to carry out a proper DPIA, or failure to deal with SARs effectively. The factors to be used in making the assessment of whether a breach is low, medium, high or very high seriousness, should be equally applicable to all breaches.

Further, a failure to report a security breach where the party is under an obligation to report is itself a breach which carries a potential penalty and is as such a separate issue, and not part of the substantive breach in question. In effect therefore the ICO needs to ensure that it is not "double counting" such a breach. If there has been a failure to report a security breach then it should be treated as an actual breach the seriousness of which needs to be determined, but not as an aggravating factor in determining some other breach.

2. **Step 2 – Culpability for a breach**

CIPL agrees that the level of culpability must be relevant to the assessment of a penalty. We would suggest that the wording around negligent failures could be re-considered. While the examples provided are helpful, the wording reads that the ICO considers "*negligent failures to be those which are unintentional".* Negligence is perhaps difficult to capture but it is not only an absence of intention to breach. It requires some level of carelessness or failure to pay due attention to a duty or task.

3. Step 3 - Determination of turnover or equivalent

CIPL recognizes that it will be relevant for the ICO to be aware of the size and economic strength of a controller or processor when assessing a penalty so will need to factor it into its considerations, but reiterates its view that turnover should not be a starting point for considering fines on undertakings, and welcomes the statement that turnover is not determinative in assessing fines.

4. Step 4 Calculation of a starting range

In this step the ICO has set out its proposed percentage approach to setting a starting point sum of fine. This is to be determined by reference to:

a) whether a breach is regarded as low, medium, serious or very serious, issues on which we have already comments, and
b) which level of fine applies.

Once the breach has been placed within the appropriate range e.g. 0 – 1% for a low level of seriousness within the higher range, then the level of culpability of the party will be used to determine what the percentage. Accordingly, our understanding is that a negligent breach would attract a lower percentage than an intentional breach.

5. Step 5 Aggravating and mitigating factors

CIPL would recommend a less cumbersome process as noted earlier. However, if this is to be adopted, it is at this stage that previous behaviours should be considered.

We would also recommend that the potential gain of a breach or avoidance of loss should be considered either as an element of the seriousness of the breach, or in conjunction with the determination of intent. While clearly the ICO is not dealing with financial regulation, and in many cases there will be limited gain or loss avoidance, in certain cases it will be a significant amount and be intimately connected to the decision of the party to carry out the breach at issue. As such it may be difficult to separate from the assessment of intent.

The Draft Statutory Guidance should clarify how this overlap or joint activity with "expert financial or accountancy advice" (page 31) and with other regulators will be approached, or refer to other materials such as memoranda of understanding or the work that the ICO has commenced with respect to other regulators and the Regulatory Sandbox. The current statement is not an appropriately clear or transparent statement of policy in this area. It does not identify which other bodies the ICO will work with, how they will work together, whether

the ICO will take the lead or defer to other regulators, or where and how those arrangements will be set out so controllers and processors can see them.

However, the ICO does have discretion on these matters, and any language that suggests otherwise and confuses this issue should be clarified or removed from the Draft Statutory Guidance. The relative weight of each factor the ICO will take into account when considering penalties should be made clear. More clarity should also be provided as to the weight to be attached to each of the factors listed by the ICO that may result in a penalty being imposed, and whether they are considered in isolation or conjunction with one another.
The relative weight of each may depend on the unique nature of each breach, but to the extent that certain factors are likely to be determinative of whether or not a penalty is imposed or is likely to increase, these should be highlighted. The ICO's process for enforcement should be made clear. The Draft Statutory Guidance refers to options the ICO will have in certain circumstances, such as the further action that may be taken where an enforcement notice is not complied with.

Transparency requires that all of the options that are available to the ICO should be set out, so that organisations may understand the full range of possibilities. With regard to enforcement notices specifically, Section 160(6)(c) requires that the ICO provide information as to how it will proceed if a notice is not complied with. The DPA also requires that certain content be provided in information notices, including the specific ground on which it is served. It should be made clear to organisations that certain decisions will be taken only in certain circumstances or if certain thresholds are met, and certain criteria fulfilled. These thresholds and criteria should be clearly detailed in the Draft Statutory Guidance, so that organisations are aware of the type of behaviour that is likely to trigger enforcement action from the ICO. Finally, the Draft Statutory Guidance should make clear that the burden of proof with respect to any relevant breach of data protection law lies with the ICO, and that the ICO will also bear the burden of justifying any action it takes.

V. COMMENTS ON THE DRAFT STATUTORY GUIDANCE ON PECR POWERS

As a general matter, CIPL reiterates its comments above in relation to the RAP. In particular, the Statutory Guidance on PECR enforcement (PECR Guidance) should clearly demonstrate the ICO's commitment to ensuring an effective, risk-based and proportionate regulatory response and emphasizing the role of accountability. While the legal provisions that underpin the DPA and PECR enforcement are different, CIPL nevertheless believes that the risk based approach to enforcement should be prioritized. In relation to accountability, the PECR Guidance in various places emphasizes that the implementation of appropriate accountability measures will mean

the ICO is less likely to issue a monetary penalty (for example in the **What do we mean by 'reasonable steps'?** section), we believe the role of accountability should be emphasized in the PECR Guidance from the outset. As noted in our comments in relation to the RAP above, CIPL believes that the ICO should actively encourage accountable behaviour from organisations by explaining how it will factor accountability into any assessment of infringement, and in determining an appropriate regulatory response, including the quantum of any sanctions.

Meaning of serious contravention. CIPL welcomes clarification from the ICO in relation to breaches that are likely to constitute a 'serious contravention', in particular the various examples of matters that the ICO considers to be 'serious contraventions' that are provided. We note, however, that the ICO does not provide a specific statement of what it considers to constitute a 'serious contravention', nor does it explain why the examples of 'serious contraventions' that are provided constitute serious contraventions. Clarification of what the ICO considers to constitute a 'serious contravention', or clarification of why the provided examples are considered to be 'serious contraventions' would be welcomed.

Further to our general comment regarding the role of accountability above, it would be helpful if the PECR Guidance also provided examples of breaches that the ICO considers are not 'serious contraventions' (for example, where the organisation has implemented appropriate policies, procedures and other accountability measures, but a small number of marketing messages were sent in breach of the law due to a software configuration error that was not identified until after the messages were sent).

CIPL welcomes the recognition that "evidence of multiple breaches and systemic non-compliance is more likely to amount to a serious contravention of PECR", but cautions that prior instances of non-compliance should not, in line with our comments on the RAP above, go to the seriousness of a particular breach. Instead, evidence of previous behaviour should be considered as an aggravating or mitigating factor in setting a penalty.

Lastly, we note that the section includes two lists of examples (the first and second sets of bullet points in the section). The second list of examples simply describes activities that would be a breach of the law, but does not provide any additional colour as to why those activities are serious contraventions. We recommend combining the two lists, in line with our comments above.

What do we mean by knew or ought to have known?

CIPL welcomes the ICO's guidance in this section. We note, however, that the majority of the examples provided in the first set of bullet points do not appear to specifically relate to the question of whether the organisation "knew or ought to have known". Instead, the majority of those bullets appear to be more relevant to the question of whether the organisation took reasonable steps to prevent a contravention (for example, the third bullet point, that refers to a failure to carry out a risk assessment). CIPL recommends providing further examples of factors that are likely to indicate that an organisation knew or ought to have known of a contravention.

How do we calculate the level of penalties?

CIPL welcomes the detailed list of factors that the ICO will consider when determining the level of any penalty to be applied. That being said, as a starting point, the guidance simply refers to the "aims of why we issue MPNs, and the general factors detailed above". It would be helpful if the guidance set out explicitly in this section the ICO's overarching goal in issuing MPNs (e.g., to eliminate any financial gains resulting from non-compliance, and the deterrent effect of fines).
We also reiterate our comments above that prior instances of non-compliance should not, in line with our comments on the RAP above, go to the seriousness of a particular breach. Instead, evidence of previous behaviour should be considered as an aggravating or mitigating factor in setting a penalty.

We also note that the list of factors does not explicitly include any accountability measures implemented by the organisation (e.g. internal policies, procedures and controls). In line with our comments above and the risk based approach, we believe that the role of accountability should be reflected in the calculation of any MPN issued by the ICO.

Lastly, while the PECR Guidance is clear that one of the aims of the ICO in setting the level of MPNs is to eliminate any financial gain or benefit resulting from non-compliance, the PECR Guidance does not indicate how any such effect is quantified. It would be helpful if the PECR Guidance set out, at a high level, the methodology that the ICO will follow to determine the extent to which an organisation has benefited financially from non-compliance.

Additional Comments:

More generally, and in addition to our specific comments above, CIPL has set out below the **Principles for a Results-based Approach** which it published in October 2017, which it believes provides some useful principles to be considered in the context of this current consultation.

Regulating for Results – Strategies and Priorities for Leadership and Engagement
10 October 2017[8]

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.
- 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 programs, the influence of their DPOs and their use of seal / certification programs, BCRs, CBPR and other

[8] Regulating for Results: Strategies and Priorities for Leadership and Engagement (English)

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.

Appendix I: Minor clarifications/updates to the Statutory Guidance on Regulatory Action

Draft Regulatory Action Policy 2021 page 22	In the title, reference to Digital Regulation Co-operation Forum, change (DCRF) to (DRCF)