An Coimisiún um Chosaint Sonraí
Data Protection Commission

Regulatory Strategy

Consultation Feedback Report

Contents

Introduction

The application of the GDPR in 2018 was a watershed moment in European regulatory history and the fortified rights it afforded individuals – along with the enhanced powers for Supervisory Authorities and enhanced obligations for organisations who process personal data – have fundamentally altered the way that many of us operate in our daily lives. The GDPR is still in the very early days of its implementation, however, and the next five years will be crucial in delivering on the principles that underpin the legislation. It is with this knowledge that the DPC has given thoughtful consideration to the responses it has received from stakeholders, both to the draft strategy itself and to the various rounds of consultation that have preceded it.

In order to prepare its Regulatory Strategy for the next five years, the Data Protection Commission (DPC) has engaged in a period of iterative consultation with a broad range of stakeholders, both internal and external, gathering insights and experiences of how the application of the General Data Protection Regulation (GDPR) has impacted the lives of individuals and organisations operating across a wide range of sectors. In June 2021, the DPC closed its final open call for submissions to its regulatory consultation on the draft strategy itself. The breadth of the DPC's stakeholder body was reflected in the submissions received.

It is clear from the depth of thought given to these submissions – which may be found in the appendices at the back of this report – that the GDPR is a matter of vital interest for many people. As is the case with any far-reaching legislation, the various interpretations from stakeholders of how best to apply the GDPR are not always in sympathy with each other. Nonetheless, the DPC is tasked with extracting the commonalities from these disparate points of view, and identifying an agenda of regulatory priorities that will drive compliance and promote better data protection outcomes for EU individuals. In setting these priorities, the DPC has been motivated by one overarching aim: to do more, for more.

Helen Dixon,
Commissioner for Data Protection

1. Who are the DPC's Stakeholders?

Given the ubiquity of personal data, and its increasing centrality to modern life, the DPC's regulatory activities impact on vast range of stakeholders. These stakeholders can be broadly categorised as, but are not limited to:

- The people of Ireland
- EU Individuals whose personal data is processed by businesses headquartered in Ireland
- Irish Civil Service and Public Sector Bodies
- Government
- Domestic (Irish) business and industry
- NGOs and advocacy groups
- Representative bodies
- Multinational business organisations and platforms whose EU headquarters are in Ireland
- Education providers (including centres of research and innovation)
- The Health Sector (both the provision of care and research)
- Data Protection Officers
- Other EU Data Protection Authorities
- Other International Data Protection Regulators
- Legal professionals
- Financial institutions
- Media (both national and international)

*This presentation of this list should not be interpreted as indicating an order of priority.

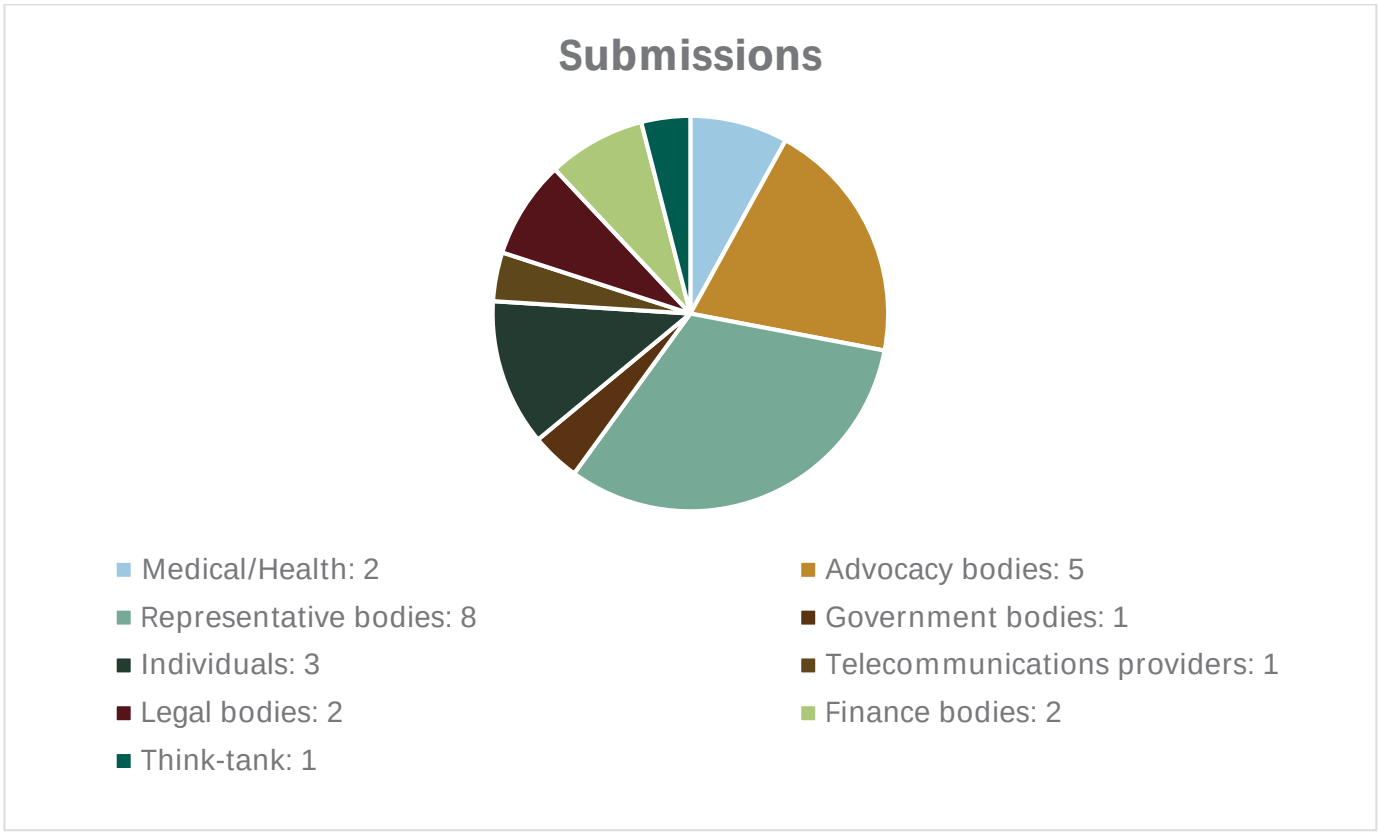
2. Consultation Overview

In early Q2 of 2021, the DPC presented its Draft Regulatory Strategy for public consultation. The Draft Strategy was developed on foot of iterative rounds of prior consultation and expert feedback. Stakeholders were invited to submit written comments on the draft, and the length and structure of these responses were left to the discretion of respondents.

The Strategy was arranged according to fundamental goals, underpinned by the DPC's mission, vision and values, which will collectively contribute to the delivery of its strategic priorities.

In all **32** written responses were received. Of these submissions, **4** were out of scope (did not relate to the Regulatory Strategy) and **28** were deemed valid. Of the 28 valid submissions, **3** (individuals) requested that their submissions not be made public. The remaining **25** submissions are consequently available in the appendices of this report.

Sectoral breakdown of submissions received



The DPC recognises that it cannot achieve its ambitions alone – new partnerships and new ways of engaging will be necessary as it looks towards a future of closer convergence in the data protection space. The DPC has consequently been very heartened to see such variety in its consultation respondents; such depth of thought given in the various submissions, and the degree of willingness toward future mutual engagement on the fundamental importance of data protection to so many sectors of society.

3. Stakeholder Views

General Comments

For the most part, the aims and objectives of the DPC's Draft Regulatory Strategy were broadly welcomed by all respondents. The risk-based approach to regulation and need for prioritisation resonated with the majority of commentators. There were some who queried how a particular goal might manifest, but no contrasting methodologies were presented to illustrate how the DPC might achieve more for its stakeholders by alternative means. The format of the consultation responses was left to the discretion of the respondents themselves. In several instances, the areas of importance identified by respondents overlapped. In other instances, respondents had a unique perspective on a particular area of relevance to themselves. Where areas of common importance were identified, respondents sometimes differed on how best to strategically progress these areas. What was very clear from all responses, and what was most encouraging for the DPC to see, is that Data Protection is of fundamental concern to all who made submissions, and the desire to improve data protection outcomes is universal.

The reconciliation of so many different points of view is challenging. Given the high-level function of the Strategy, some of the commentary provided by respondents was more granular in nature and could not be said to constitute priority items in-and-of themselves. However, this granular commentary will be invaluable in setting work plans and identifying the output targets that will underpin the strategy, ensuring that the DPC's strategic goals are realised over the course of the next five years.

Emerging Themes and Issues

1. Guidance and Education

Calls for increased guidance – as well as more nuanced, accessible guidance – were almost universal across all responses. Almost all of the respondents indicated that increased compliance would be predicated on a greater understanding of data protection obligations, and that DPC guidance would be fundamental to that. Particular areas of concern for organisations involved in the processing of personal data are:

- Data Processing Agreements;
- Data Protection Impact Assessments;
- Standard Contractual Clauses;
- Records of Processing Activities; and
- The safe sharing of personal data.

The DCP will continue to provide guidance to both organisations and individuals going forward. As outlined in the Draft Strategy, the next five years will be characterised by

the building of beneficial partnerships with a broad range of stakeholders, so that their expert input can help the DPC to develop more tailored and accessible guidance.

2. Case Studies

Building on the need for more and nuanced guidance, respondents also broadly welcomed the DPC's proposal to increase its publication of case studies beyond those that already appear in its annual report each year. Increased case studies, including sector-specific case studies were felt to be aids to compliance, as were DPC-identified examples of good practice or themed findings. The DPC will create a public schedule of Case Studies, with quarterly updates so that stakeholders have access to more up-to-date learnings throughout the course of a given year.

3. Hard Enforcement (sanctions)

The need for consistent, proportionate and effective enforcement are identified as key priorities for the DPC over the next five years and beyond. Approaches to – and interpretations of – "hard enforcement" differed between the various respondents, from those who favoured increased engagement as a means to drive compliance, to those who are of the view that swift and severe penalties are the best way to promote compliance among DPC's regulated entities. For the most part, there was a recognition of the legal challenges inherent in pursuing precedential, pan-European inquiries which are the means by which the mechanisms of the GDPR will be codified.

The DPC will continue to impose sanctions where it is fair and appropriate to do so, but the DPC has also made increasing the turn-around times for inquiries a strategic priority. As more and more cases now move though the Article 60 and Article 65 processes, the mechanisms of the GDPR are being tested and greater clarity is being derived.

4. Complaint Handling

In its draft Regulatory Strategy, the DPC proposed that it would "*rebalance the way it approaches individual complaints, to ensure that its resources are being used in the most efficient way possible to bring improved results to the maximum amount of people*". In order to do this, the DPC would "*prioritise cases that are likely to have the greatest systemic impact for the widest number of people over the longer-term*".

The majority of respondents recognised the difficult position in which the DPC finds itself with respect to resources and caseload. There were some respondents who suggested that the DPC should make it mandatory for individuals to demonstrate that they had exhausted all other forms of redress before approaching the regulator, and others who opposed any form of collective treatment for individuals. This was a strategic approach that divided some respondents. On balance, more respondents supported this approach than opposed it.

There were reasonable requests for clarity as to how systemic risk would be identified and how individuals would be kept informed of the status of their own cases. The high-level nature of the strategy is not the correct format to drill into this in detail but, acknowledging this reasonable feedback, the DPC will publish separate and more expansive guidance on its complaint handling processes – including how systemic risk is identified - in 2022.

5. Personal data and academic research (including medical research)

Stakeholders specifically expressed a desire for greater clarity and more guidance around the proper processing of personal data for research purposes, in order to ensure that innovation remains possible whilst also adhering to the principals of the GDPR. While not a strategic objective for the DPC for the next five years, this type of guidance and support will drive the work items that give functional effect to the priorities set out in the Strategy.

6. The specific protections afforded to children and other vulnerable groups

The inclusion of this strategic objective as a key priority for the DPC was met with widespread support from stakeholders. Nuanced and valuable commentary was made in respect of this priority by some of the advocacy groups who responded to the consultation, such that it will be made clearer in the strategy that there is no intention to represent children's needs as the same as those who are considered vulnerable owing to age or physical or intellectual disability. The action points under this priority will also be expanded to make it clear that the engagement efforts that are envisaged for the protection of children will also be mobilised in respect of the other groups served by this strategic objective.

7. Engagement with other legislative frameworks

Stakeholders in general were anxious that the next five years would see greater clarity on the interplay between data protection legislation, in particular the organisational obligations that exist in respect of financial legislation, but also the pending Digital Services Act and Digital Markets Act, as well as the Assisted Decision Making Act, 2015, given its relevance to the DPC's third Strategic Priority. The DPC does – and will – engage with all relevant legislation. The Strategy will be updated to ensure that this is called out in a way that reassures stakeholders.

8. Collaboration with sectoral expertise and partner groups

There was broad welcome to the DPC's assertion that it will, over the course of the next five years, increase its collaborative engagements with experts from disparate sectors in order to develop more useful guidance and push meaningful compliance in its multi-stakeholder base. Most welcome, from the DPC's perspective, were the many

expressions of interest from consultation respondents, willing to engage further with the DPC to increase clarity and improve data protection outcomes for the sectors they represent.

9. Increasing Legal Clarity

Respondents expressed support for the DPC's goal of increasing legal clarity in the application of Data Protection law. This included clearly drawn parameters as to the scope of the DPC's remit. The DPC is committed to driving this clarity over the next five years, so that the regulatory landscape becomes more stable.

10. Cross Border Data Transfers and Brexit

The vital importance of clarity around third-country data transfers was an area of concern for many respondents. While acknowledging that it is for the European Commission to lead in these areas, the DPC is committed to playing an active supporting role where appropriate, to ensure that clarity in this regard is achieved as soon as possible. This will continue to be a key activity for the DPC going forward.

11. Codes of conduct and certifications

Respondents to the consultation called on the DPC to promote the development of Codes of Conduct and the use of Certification as tools to drive compliance. While the DPC recognises that the development of Codes of Conduct is the remit of each respective sector, the promotion of their development and use will be a key task for the DPC over the five years of its Regulatory Strategy.

12. Resourcing and restructuring the DPC

Resource constraints for the DPC were an area of concern for a number of respondents, with references made to both expansion and retention of the staff cohort. This is a concern that is shared by the DPC and was called out as a priority in its Draft Regulatory Strategy. The DPC will continue to work with the relevant government bodies to secure the funding and structural changes necessary for the DPC to meet its enhanced remit under the GDPR. While acknowledging the support of government over the last five years in particular, more support will be needed as the ubiquity of data protection legislation increases in the future. In order to maximise its funding allocation, the DPC will publish the findings of an independent review carried out by KOSI Corporation, into the structure and future state of the DPC.

13. Transparency

The DPC's goal of increasing transparency around its processes and procedures over the next five years was broadly welcomed and will remain a stated objective for the DPC. The DPC believes the values of good governance and accountability, including those in respect of the Public Sector Equality and Human Rights Duty, live in the

priorities and objectives of this Strategy, showing the DPC's clear commitment to standards of good governance.

14. Support for SMEs and Data Protection Officers

DPOs and DPO networks who responded to the survey recognised that the DPC has commenced targeting supports to their specific needs, but called for this to be expanded going forward. The DPC, in its Draft Strategy, has made supporting DPOs a priority but, in recognition of the submissions received, will expand the language around this priority to ensure that non-designated data protection operatives are brought within the ambit of the DPC's DPO Network. This means that those who hold compliance positions in organisations (which are not obliged by the terms of the legislation to appoint a DPO) will be able to access the necessary supports to help them perform effectively in their roles. Similarly, SMEs have been – and will continue to be – the focus of specific support, to help them meet their compliance obligations.

15. Technological capacity building

The DPC has made technological capacity building a priority for the next five years, and this has been broadly welcomed by respondents to the consultation. From the point of view of the DPC, technological capacity in this instance refers to both the people and systems who drive its operations. With this in mind, and in recognition of the suggestions made in the responses to its consultation, the DPC will make the development and publication of its Technological Policy a target objective under the new Regulatory Strategy.

16. Outreach and Awareness

Outreach and collaboration with its stakeholders are stated objectives of the DPC's Draft Strategy and it looks forward to operationalising those goals with even greater energy post-pandemic. However, one respondent to the consultation did identify a gap in the DPC's outreach plans; specifically direct engagement with individuals through media awareness campaigns. The published Strategy will be updated to reflect the DPC's intentions to utilise mainstream media channels to make individuals more aware of data protection and their rights under the GDPR.

4. Comments on the DPC's Mission, Vision and Values

In general, the DPC's Mission, Vision and Values attracted very little commentary from respondents to the consultation. There were two commentators who shared their views on these specific aspects of the Draft Strategy, including:

- The expansion of the DPC's values to include proportionate; evidence-based and results-driven; and
- The modification of the DPC's Mission to place greater primary emphasis on its enforcement role.

The DPC is happy to include results-driven as an additional value, but believes that proportionality and evidence-based regulation are encapsulated by the values already enumerated. With reference to the suggested changes to its mission statement, and taken in conjunction with the tone of the majority of responses to the open consultation, the Mission will remain as is, reflecting – as it does – the equal priority given to each of the named methodologies under Article 57 of the GDPR, as well as the strong call for more guidance and engagement that has been evident in the consultation process as a whole.

5. Conclusions and Next Steps

The DPC has been very encouraged by the number and variety of responses that the Draft Strategy attracted. The careful consideration given and fulsome expression of views – including opposing schools of thought – have been a significant contribution to the finalisation of the Strategy.

As has been said before, the breadth of the DPC's remit is so extensive that there will naturally be sections and sub-sections of that remit that are of more direct concern to one sector over another. The DPC's challenge has been to reconcile those concerns and find the way forward that is equitable for all, progressive and – ultimately – achievable.

The DPC would like to thank those participants who took the time to share their views on the future regulatory approach of the DPC. The Draft Strategy will be updated in to reflect the nuances called out in Chapter 4 of this report, at which point the Strategy will be adopted by the DPC for publication, along with this report on the consultation feedback.

The DPC looks forward to implementing the aims of its strategy and delivering more, for more, over the next five years.

Appendices

6. Appendices: Submissions Received

Contents (submissions are presented in order of date received)

**The contents of the submissions have not been altered and are presented verbatim.*

Tallaght University Hospital

Tallaght University Hospital (TUH) has reviewed the information presented in the Data Protection Commission's (DPC) document *Regulation Strategy – Consultation*. It sets out its responses under the five sections identified in that document.

1. Regulate consistently and effectively

Desired outcome

The DPC's application and enforcement of data protection legislation, including the GDPR, LED, the E-Privacy Directive and the Data Protection Act 2018 provides consistent understanding and legal clarity for all stakeholders.[1]

TUH response

Tallaght University Hospital (TUH) is one of Ireland's leading academic and teaching hospitals. Consequently, research is one of its core functions. In evaluating projects, TUH complies with data protection legislation requiring Data Protection Impact Assessments (DPIAs) to be carried out where personal data and special category personal data (i.e. data concerning health) are to be processed in the research.

We would welcome more consistent regulation in this area.[2] The compilation and review of DPIAs is proving to be a timely and resource dependent activity which can, in certain instances, delay research. It would be of great benefit therefore if the DPC considered provision of the following:

- a DPIA form created by the DPC for application across all organisations so that the approach taken and information gathered is consistent (as is available from supervisory authorities in other Member States)
- guidance on how many DPIAs are required where more than one organisation is involved in the research (i.e. does each participating organisation have to provide a DPIA or is one per project sufficient?)
- specific guidance on, and specialised training in, the GDPR and 'Scientific research, historical and statistical purposes'

[1] 1 DPC (2021), p.8.

[2] TUH confirms it has consulted and applied DPC guidance: https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#should-the-data-protection-commissioner-be-consulted-on-completion-of-the-dpia

2. Safeguard individuals and promote data protection awareness

Desired outcome

Individuals have a better understanding of their data protection rights, know how to exercise those rights on their own behalf and how to escalate their issues to the DPC when necessary.[3]

TUH response

TUH would welcome the proposals as presented

3. Prioritise the protection of children and other vulnerable groups

Desired outcome

Children and vulnerable groups are specifically protected, and those who act on their behalf have a better understanding of data protection rights and the legal bases on which personal data can be shared. Guidance for children and other vulnerable groups is made available through accessible means, so that obtaining information is not impeded by language, capacity, financial or other barriers.[4]

TUH response

TUH would welcome the proposals as presented

4. Bringing clarity to stakeholders

Desired outcome

The DPC follows fair, impartial and transparent complaint-handling processes in a prioritised way, to ensure that its resources are deployed proportionally in order to maximise their impact and corresponding benefit to stakeholders.[5]

TUH response

TUH would welcome the proposals as presented.

5. Support organisations and drive compliance

Desired outcome

Business and organisations of all sizes are informed and accountable for their data processing activities and there is clarity and consistency regarding sanction and enforcement actions.[6]

TUH response

TUH would welcome the proposals as presented.

[3] DPC (2021), p.10.
[4] DPC (2021), p.13.
[5] DPC (2021), p.16.
[6] DPC (2021), p.19.

1. Data Protection Professional (Individual)

To support companies / organisations and to drive data protection compliance, the DPC should write to and advertise publicly via media TV, radio etc. to inform all types of companies / organisations, outlining the following:

- Data Protection Agreements (DPAs) & Standard Contractual Clauses (SCCs) : - outlining the mandatory obligations to have these in place.

The facts are that most small, medium enterprises (SMEs) companies do not understand and/or refuse to enter 'Data Protection Agreements - DPAs'.

As aligned and outlined in DPC publications includes the following extract

"...One obligation under the GDPR is the requirement of Controllers and Processors to enter into a legally binding contract when a Controller engages a Processor to process personal data on its behalf.."

See DPC link below:

https://www.dataprotection.ie/sites/default/files/uploads/2019-04/Guidance-for-Data-Processing-Contracts-GDPR.pdf

Please note: the above also applies to SMEs and larger companies with regards to Standard Contractual Clauses whereas such providers/suppliers (including SaaS or other types) are located in jurisdictions without EC Adequacy Decision Approvals (i.e. Third Countries) and refuse to enter into such legally binding agreements, whereas they outline to the data controllers (i.e. users) that they (the provider) rely on their 'Terms and Conditions (T&Cs)' for users using their platforms. And particularly they don't seem to understand and/or blindly ignore that if they process any EU Citizen data regardless of where their entities are located outside Ireland that they have both legislative and regulatory obligations.

For the DPC to drive data protection compliance, then, a simplified message (continually delivered) from the DPC involving the following 3 legislative and regulatory requirements needs to be communicated multiple times and via multiple communication ways, to all sized companies in Ireland, outlining why and how to put in place the following:

1) DPAs and SCCs
2) Register of Processing Activities (RoPA) and processing legal bases (Art 6 & 9).
3) Data Protection Impact Assessments linked with their Risk-based assessments.

3. Safeguarding Ireland

Safeguarding Ireland is registered with both the Companies Registration Office and the Charities Regulatory Authority. Its main functions include the promotion of adult safeguarding and their protection from all forms of abuse by persons, organisations and institutions, and the development of a national plan for promoting their welfare. This is achieved through the promotion of inter-sectoral collaboration, developing public and professional awareness and education, and undertaking research to inform policy, practice and legislation in the Republic of Ireland.

Many of Safeguarding Ireland activities and resources, as well as other information, can be found on its website https://www.safeguardingireland.org/

BACKGROUND.

Safeguarding Ireland welcomes the opportunity to make this submission to the Office of the Data Protection Commissioner on its Regulatory Strategy 2021-2026. It does so against a backdrop of an awareness by Safeguarding Ireland of increasing numbers of adult abuse being reported to the HSE safeguarding services and an acknowledgement that these referrals to the HSE are likely to be a very significant under-reporting of the adult abuse cases in Ireland. It also does so in the knowledge that the sharing of data between agencies where there are concerns of abuse, exploitation or neglect is an important element in combatting abuse. However, it would appear that there is limited understanding or awareness on the part of many agencies and individuals on their obligations and responsibilities in relation to data sharing vis-a-vie protection of adults.

Prior to specifically addressing the DPC's Regulatory Strategy, it is important to outline the type and extent of adult abuse. There are a number of different types of abuse and it is not uncommon for more than one type of abuse to be afflicted upon an individual.

- Physical Abuse can include pushing, shaking, slapping, punching, kicking;
- Financial Abuse includes stealing, accessing bank accounts without consent, abuse of joint accounts, abuse of agency arrangements, pressure in relation to wills;
- Psychological Abuse - threats of harm or abandonment, deprivation of contact, humiliation, blaming, controlling, intimidation, coercion;
- Sexual Abuse – unwanted touching, sexual harassment, rape;
- Neglect – ignoring physical or emotional needs, withholding treatment or medication, withholding food;

- Institutional Abuse – overuse of power or control, inappropriate or excessive restraint, lack of choice, lack of consultation;
- Self-neglect includes lack of attention to one's own physical needs, a refusal or inability to cater for one's own basic hygiene needs, hoarding.

Unfortunately, there is no collection of data at national level, therefore, the true extent of adult abuse in Ireland is unknown. The HSE National Safeguarding Office Annual Report 2019, stated that there were 42,022 safeguarding concerns reported to the safeguarding service in that year. However, the HSE acknowledges that these figures do not reflect the true extent of adult abuse. "The current data as collected by the HSE is limited and lacks the depth of information necessary to provide a comprehensive assessment of abuse of adults at risk of abuse in Ireland".

The Report goes on to state that "there are also important sectors outside of healthcare that do not gather data and as such safeguarding concerns are underreported especially in areas such as financial abuse".[7]

International research has indicated that adult abuse is common. Some studies have shown that "at least one in 10 community-dwelling older adults experienced some form of abuse in the prior year" and "global prevalence rates of the abuse of older women found that one in six experienced abuse in the prior year".[8]

In Ireland, a study by the National Centre for the Protection of Older People[9], which examined the prevalence of elder abuse, (i.e., abuse of people over 65) and only that occurring in the community, found that the overall prevalence of mistreatment in the previous 12 months was 2.2%. Applying these statistics to the general population of people aged 65 years or older at the time of the study (2010) using the most recently available CSO figures at that time (CSO 2007), the number of older people who had experienced mistreatment was estimated at 10,201. If these figures were to be applied to current population estimates[10], the number of older people who have experienced mistreatment rises to 15,842. In the 2010 study, financial abuse was the most frequent type of abuse reported, followed by psychological abuse (1.2%), physical abuse (0.5%), and neglect (0.3%).

---

[7] National Safeguarding Office Annual Report 2019. HSE.

[8] https://ncea.acl.gov/What-We-Do/Research/Statistics-and-Data.aspx

[9] Abuse and Neglect of Older People in Ireland. Report on the National Study of Elder Abuse and Neglect. NCPOP (2010).

[10] https://www.cso.ie/en/releasesandpublications/er/pme/populationandmigrationestimatesapril2020/

The above research relates to elder abuse only (i.e., abuse of people 65 years of age and older). There appears to be less research on the extent of abuse of younger adults. However, in the HSE's 2019 Annual Report referred to above, the rate of referrals for those under 65 was 2.53 per 1,000 compared to the rate for over 65s at 5.23 per 1,000.

In a RedC Survey commissioned by Safeguarding Ireland, the Irish public believes abuse of vulnerable adults is widespread while in another poll,12% of respondents said they had experienced adult abuse during the first six months of COVID-19[11].

The above illustrates the hidden nature of, and indicates the very sizeable extent of, the problem of adult abuse. However, in outlining the figures above, it is important to recognize that, behind each of these figures, is an adult who is experiencing abuse that has a negative impact on their quality of life, sometimes to very significant levels.

Data sharing can be a vital element in safeguarding, both in preventing abuse and promoting the welfare of adults. The amount, type and with whom data is shared can have a very significant impact on an abused person's life. In addition, it can ensure that an individual receives the right services at the right time, it can prevent identified needs from becoming more acute and difficult to meet and, where there are concerns about an adult's safety, the sharing of information in a timely and effective manner between organisations can reduce the risk of harm. In extreme cases, it can be the difference between life and death.

Safeguarding Ireland believes that both agencies, i.e., the Office of the Data Protection Commissioner and Safeguarding Ireland, are committed to safeguarding the rights of vulnerable people. In that context, we believe it to be very important that, in safeguarding those rights, one agency's focus in safeguarding those rights do not negatively impact on another's to the detriment of vulnerable people. One of the challenges for Safeguarding Ireland and for agencies dealing with abuses of vulnerable people is that there is no specific safeguarding legislation in Ireland. It is important, then, that vulnerable people do not suffer erosion of their rights in an area that is not enshrined in specific legislation while satisfying other legislative requirements. It would potentially be of considerable benefit to vulnerable adults who lack capacity and who may be experiencing abuse, neglect and/or exploitation if a specific defence against liability, where there is an informed reasonable belief that there is a safeguarding issue, was included in data protection legislation.

SUBMISSION.

[11] https://www.safeguardingireland.org/public-awareness/

MISSION.

The Mission outlined in the DPC's Regulatory Strategy Consultation document is to uphold 'the consistent application of data protection law through engagement, supervision and enforcement, and driving compliance with data protection legislation'. The Mission further states that the 'Data Protection Commission provides clarity for the organisations it regulates by.....educating stakeholders on their rights and responsibilities' and 'communicating extensively and transparently with stakeholders.' These are very welcome elements of the Mission as there seems to be a lack of clarity in relation to data protection law in the context of information sharing where there are abuse concerns relating to a vulnerable adult. There is a real need for many agencies to gain clarity on their obligations and restrictions in relation to data sharing versus their obligations to share data in an appropriate manner where safeguarding issues arise. Safeguarding Ireland considers this to be one of the most important elements in terms of safeguarding vulnerable adults related to the work of the DPC.

STRATEGIC GOALS.

1. REGULATE CONSISTENTLY AND EFFECTIVELY. Safeguarding Ireland considers this an important Goal in the context of adult safeguarding and data sharing. Some of the proposals outlined are necessary to ensure data protection and vulnerable adult protection. Safeguarding Ireland particularly welcomes the commitment to increase 'transparency and provision of information on the DPC's outreach activities and engagement with stakeholders'. We consider that, at the present time, there is a lack of clarity among many stakeholders in relation to data sharing where there are concerns of abuse. This is borne out in engagements we have had with many different agencies and individuals. Indeed, this lack of clarity and understanding seems to exist both across different agencies and within agencies. The proposed publication of case studies should include those cases that encompass both data protection and safeguarding concerns.

2. SAFEGUARD INDIVIDUALS AND PROMOTE DATA PROTECTION AWARENESS. Safeguarding Ireland welcomes the commitment to work on 'Codes of Conduct and Certifications, so that best-practices can be developed within sectors, in turn facilitating demonstrable compliance with processing standards and providing assurance for consumers and organisations'. There is a pressing need to initiate, develop through consultation with relevant agencies, and actively promote codes of conduct on the processing and sharing of the personal data of vulnerable adults. These codes of conduct should address issues of consent in relation to vulnerable adults and the circumstances where consent is not required. They should also define the specific protections required to safeguard the rights of vulnerable adults both in the protection of their personal data and in safeguarding them from abuse, and provide guidance for

people and organisations. In drawing up the codes of conduct, there is a need to collaborate with, and seek advice from, advocates and experts in the field of protection and promotion of the rights of vulnerable adults, including other regulators and statutory bodies. It may be of benefit to conduct detailed research on how data protection law applies to vulnerable adults, both internally and through research partnerships with relevant organisations. In addition, in making data sharing decisions and in assessing data protection concerns, there will be a need to be aware of decision-making capacity and the Assisted Decision Making Capacity Act, 2015. In the context of the above, the commitment to take 'account of how data protection impacts vulnerable groups and engaging with advocacy groups to communicate this appropriately' is very welcome. In addition, Safeguarding Ireland welcomes the intentions to 'engaging fairly with organisations to promote openness, trust and compliance culture' and 'actively promoting the development of codes of conduct and certifications to enable sectoral best-practice and demonstrable compliance in processing activities'.

3. PRIORITISE THE PROTECTION OF CHILDREN AND OTHER VULNERABLE GROUPS. While Safeguarding Ireland fully supports this overall strategic goal, we are disappointed that, of the nine proposed actions outlined to achieve the goal, only one refers specifically to vulnerable persons. Moreover, that action – 'Engaging and partnering with representative bodies and advocacy groups who act on behalf of vulnerable persons, to get their insight into how best to tailor guidance for their clients' – only proposes providing guidance to vulnerable clients. It does not refer to the need to provide guidance to agencies who actively engage in the protection and safeguarding of vulnerable clients or to all organisations to understand their obligations to vulnerable persons generally. This is in marked contrast to the commitments to children under the same strategic goal. Safeguarding Ireland is fully supportive of the need to specifically protect children but would suggest that there is an equal need to protect vulnerable adults. Therefore, Safeguarding Ireland proposes that there be a separate section specifically relating to vulnerable adults. Putting children and vulnerable adults together may infer that issues relating to both groups are similar, which is not the case. In a separate section on vulnerable adults, Safeguarding Ireland proposes the following activities that the DPC should undertake in this regard –

- Initiating, developing through consultation with relevant agencies, and actively promoting codes of conduct on the processing of personal data of vulnerable adults. These codes of conduct should address issues of consent in relation to vulnerable adults.
- Defining the specific protections required to safeguard the rights of vulnerable adults in the protection of their personal data and providing guidance for people and organisations.

- Collaborating with and drawing from the advice and experiences of advocates and experts in the field of protection and promotion of the rights of vulnerable adults, including other regulators and statutory bodies.
- Conducting detailed research on how data protection law applies to vulnerable adults, both internally and through research partnerships.
- In making data sharing decisions and in assessing data protection concerns, cross-referencing decision-making capacity and the Assisted Decision Making Capacity Act, 2015.

Safeguarding Ireland's view is that the inclusion of these activities specifically related to vulnerable adults would play a significant part in safeguarding them from abuse and, in addition, provide clarity to agencies dealing with vulnerable adults on data collection and sharing in circumstances where people may be suffering abuse, neglect and/or exploitation. In addition, inclusion of the above would support the other four strategic goals and ensure a consistency and dovetailing of the goals to make the Strategy more inclusive and complete.

4. BRING CLARITY TO STAKEHOLDERS. This overall Goal is vitally important because, as outlined above, there certainly appears to be a lack of clarity at present. It is interesting that, following the DPC's focus group consultations, there was a feeling 'that businesses and organisations were essentially divesting themselves of data protection accountability and passing it on to customers. Stakeholders felt that organisations were more intent on indemnifying themselves against future action, as opposed to processing information in accordance with transparent and legitimate standards'. Safeguarding Ireland would concur with this and believes that much of this approach stems from a lack of clarity in relation to the processing and sharing of data. Engagement by the DPC with various organisations is critical. In that sense, while supporting this Goal, Safeguarding Ireland believes the other recommendations it has made in relation to the other Goals, if adopted, would enhance the desired outcome related to this Goal.

5. SUPPORT ORGANISATIONS AND DRIVE COMPLIANCE. Safeguarding Ireland is fully supportive of this Goal, believing it complements the other Goals, particularly if the recommendations made above are included in the final Strategy. We note the reference to 'guidance and engagement with organisations will be crucial to drive accountability and promote the culture of data protection compliance more generally'. We entirely agree that these are 'regulatory tools' in their own right and there is more to gain in employing these tools in appropriate circumstances, particularly where there is genuine

confusion and lack of understanding of the data protection legislation. This is why engagement with stakeholders, consultation, education, research and the development of codes of conduct are so important.

4. National MedLIS Project Training and Data Protection Lead

Here are some of the suggestions I have

Interchanging between acronyms and expansion of same (e.g. DPC and GDPR) is confusing.

Data Protection in relation to healthcare data is not called out and given that the focus of the DPC is a shift from individual issues to broader issues that affect higher volumes then this should be a main focus.

Training for children and adults should not only cover their rights as individuals but should focus more on the rights of their peers who may be children or other vulnerable groups. For example if the training included that one child does not have the right to publish sensitive data about another on social media you are teaching the child not only about their rights but that everyone has the same rights . Equally important is training in the area of what one adult can or not publish or disclose in relation to their dependents or other adults. Approaching training in an alternative manner to the standard approach may reach a wider audience.

5. IAB Ireland

1. Introduction

1.1. IAB Ireland welcomes the opportunity to respond to this consultation.

1.2. Digital advertising is a crucial component of a healthy digital media economy. It generates important revenue to support content production and diversity of the media ecosystem.

1.3. The digital advertising ecosystem is undergoing profound change - including changing media consumption patterns, accelerated digitisation due to the pandemic and deprecation of third party cookies in browsers - and the interpretation and enforcement of regulation is having an ever greater impact on the shape and sustainability of media.

1.4. Data protection regulation is one element of an increasingly complex framework of intersecting rules which govern the digital media landscape. Significant further regulation is under development such as the ePrivacy Regulation and the proposed DSA and DMA.

1.5. The successful transition and evolution of this complex ecosystem depends to a large extent on nuanced and thoughtful interpretations of existing rules and careful design of new ones. This consultation is therefore timely and we welcome the opportunity to provide these initial comments. We and IAB Europe look forward to further engagement on the points we raise here.

2. About IAB Ireland

2.1. IAB Ireland is the trade organisation for digital advertising in Ireland and a member of the global IAB network. IAB members include advertisers, agencies, ad intermediaries, technology providers, media owners and publishers all working together to help deliver a sustainable industry. With 1over 70 member companies, IAB Ireland represents the key stakeholders in digital advertising who collaborate in IAB councils/working groups to grow knowledge and share best practice in the Irish digital advertising industry.

2.2. IAB's remit is to prove, promote and protect the Irish digital advertising industry through events, research and standards, as well as engagement in policy development and regulatory affairs.

2.3. IAB Ireland and its members have invested significantly in the development and implementation of self-regulatory schemes which help govern digital advertising supply

chains and aid compliance with regulations, including data protection laws. Full membership list: https://iabireland.ie/members-list-by-type/

2.4. For example, IAB Ireland introduced the Gold Standard in February 2021, a certification programme for IAB Ireland members which incorporates a global set of standards across 4 key pillars: uphold brand safety, tackle ad fraud, improve the digital advertising experience and help compliance with the GDPR and ePrivacy law.

2.5. In addition, IAB Europe pioneered the development of the Transparency and Consent Framework (TCF) which seeks to achieve uniform implementations of very complex law - that is interpreted and applied differently by different data authorities - within the complex open demand and publisher supply chains. Without industry-wide collaboration, it would be far more difficult to comply. TCF is now in v2.0 following feedback from DPAs and introduces more granularity transparency and controls for consumers, supports signalling to allow users to object to legitimate interest based processing, and gives publishers more control over who can do what kind of processing on their properties.

2.6. The IAB Ireland PwC Online Adspend Study 2020 reported digital advertising 2 in Ireland grew 8% to €726m outperforming all other media. Industry predictions for digital advertising in 2021 anticipate a growth of 10-20%.

3. General comments

3.1. The Covid-19 pandemic has resulted in the rapid adoption of digital technology across the economy. Data use is core to the economy and decisions made in one sector have implications for future uses of data that will drive the recovery and Ireland's economic goals. Economic sectors which were previously referred to as 'digital' are now core to all economies such that they should no longer be referred to as "*non-traditional*". Digital *is* the economy and this should be reflected in the DPC's thinking.

3.2. The consultation recognises that the DPC cannot achieve its ambitions alone and that new partnerships and new ways of engaging will be necessary. This is very welcome. The DPC is right to observe that the 2021-2026 lifecycle of this strategy will be five crucial years in the evolution of data protection regulation and culture. Decisions made during this period, in combination with wider digital policy and market developments, will shape the future media landscape and this must be done in close consultation with the full range of stakeholders, including industry.

4. Detailed comments.

Strategic Goal 1: Regulate consistently and effectively

4.1. We welcome the commitment to increase certainty and stability in how data protection is applied and the acknowledgement that data protection law aims to accommodate future developments in the use of personal data. This is crucial in fast moving markets like digital advertising.

4.2. Transparency about how the DPC carries out its regulatory functions, improved guidance, and clarity and consistency on procedures are essential See https://iabireland.ie/wp-content/uploads/2021/04/IAB-PwC-Adspend-study-2020-infographic.pdffoundations for a vibrant domestic and European digital advertising market. It is important that the DPC's priorities are in sync with market developments so that procedures are efficient and decisions are timely, and that guidance is issued at the moment the market needs it. The DPC's processes and resourcing will need to be sufficiently agile to respond to changes in the wider landscape.

4.3. A greater use of case studies illustrating how data protection law is applied would be very useful in terms of educating all stakeholders. Such publications should include international examples which would assist companies operating internationally and would also benefit peer DPAs. This would place Ireland's data protection law as a benchmark and core part of a global framework, and would also serve as a counter to the increasingly divergent views around the world on the best approach to privacy and data protection regulation.

4.4. We are concerned about the risk of a "splinternet", where some countries or regions of the world adopt approaches to privacy and data protection that are mutually exclusive to other regimes and do not allow for digital services to be provided globally or across different jurisdictions. In this regard, a responsible and balanced approach regarding the international transfers is urgent which requires to take into account, as required by the GDPR and Charter, of the economic and social impact of data protection decisions that isolate the EEA by imposing a de facto data localisation or other unworkable or unviable solutions.

4.5. In this vein, we are supportive of the DPC's objective of engaging with data protection authorities both within and outside the EEA to understand the differences in data protection laws and their implications, and collaborating with peers on international cooperation endeavours.

4.6. The OSS is highly valued by industry and cooperation and alignment with other European DPAs is crucial for companies operating internationally. We support the commitment to partnerships with EEA DPAs to ensure that GDPR delivers on its promise to provide a uniform set of rules in all member states and for companies operating in the single market.

4.7. The strategy could go further by setting out how the DPC will make progress towards this goal and address instances where there are conflicts or where other DPAs encroach on the DPC's jurisdiction so that Irish companies can make good faith efforts to comply under the certainty that the GDPR OSS rules are going to be respected by all DPAs. The DPC should consult with concerned DPAs in advance of new inquiries and set out indicative timelines for the progress of cases.

4.8. A more frequent and detailed engagement with individual stakeholder groups would aid the DPC's understanding of the market and prioritisation. Creating a genuinely safe and open space for confidential and trusted discussion about the sustainability of the media ecosystem is important for our members. IAB Ireland, in partnership with IAB Europe, stands ready to facilitate such a dialogue.

4.9. Particular concerns for our industry include:

4.9.1.Shifting interpretations of consent which require repeated refreshing of consent, leading to fatigue and confusion among consumers.

4.9.2.Repeated examination of digital advertising models which creates uncertainty and unpredictability, particularly among competing ad firms and publishers who only contest a small market segment.

4.9.3. Knock on effects for the evolution of industry initiatives, such as TCF's efforts to deliver predictable and consistent approaches to consent in complex supply chains like open-demand.

4.9.4.Risk of different approaches to data protection emerging around the world that do not allow for digital services that rely on scale to be provided across different jurisdictions.

4.9.5.Ongoing instability in the legal framework around international transfers, and data protection decisions that isolate the EEA by inferring data localisation or other unviable solutions.

4.10. As noted above, we highlight the importance of clarity and consistency between data protection law and other horizontal or sectoral regulatory developments. While acknowledging that this is primarily a matter for Government to consider as it develops new domestic policy and engages in EU policy-making, it is important the DPC recognises that the design and implementation of data protection regulation intersects with other policy objectives and this can lead to competing expectations of companies.

4.11. Other governments and regulators are increasingly acknowledging the interdependencies between data protection and other regulation and the long-term health of digital markets. The DPC should therefore build engagement with Government

and other regulators, including the CCPC which is examining the operation of digital markets. This should include joint programmes of work and coordination to deliver coherence and clarity across intersecting areas of policy. The DPC should also routinely assess the economic impact of different interpretations and enforcement options, for example where they would have differing effects on competing business models or are in tension with strategic public policy goals, such as the sustainability of news media.

4.12. It is important for digital advertising firms that the DPC has the resources to operate in a timely and responsive way. The DPC should also explore changes that could make smart use of existing resources. For example, the cross-border complaints unit could introduce more timely referrals to companies, swift closure of uncontentious cases and improved communication with end users, as well as enabling direct engagement between data controllers and their customers to speed up resolution. The efficient operation of the OSS is important to maintaining the principle of country of origin control as well as the reputations of both the DPC and the companies receiving complaints via the OSS.

4.13.It is important that the DPC remains competitive in attracting and retaining top quality talent. The impact of staff churn is evident in companies' day-to-day engagement with the DPC. We therefore support the DPC seeking Government sanction to conduct specialist recruitment in key areas in order to increase the pool of skilled candidates and support retention.

5. Strategic Goal 2: Safeguard individuals and promote data protection awareness

5.1. We support the DPC to carefully prioritise its resources on the issues that pose the greatest impact for the widest number of people over the longer-term. It is not in the interests of any party for the DPC to be operationally and statutorily bound by a complaint-heavy system.

5.2. To support this goal, the DPC should adopt the practice from other markets which requires a data subject to exhaust existing complaints mechanisms made available to them by the data controller before submitting a complaint to the DPA, e.g. UK and Spain. This approach should apply to both domestic and cross-border complaints and would meet the DPC's objective to find more efficient ways to manage complaint volumes, allow the DPC to redeploy resources to priority areas and be consistent with GDPR's principle of accountability (of data controllers).

5.3. We also welcome the proposal to engage with civil society on areas of concern for individuals. This provides an opportunity to explore approaches consistent with Strategic Goal 5 by aiding compliance to avoid repeated investigations which are highly disruptive to the competitive operation of complex markets, and to weigh interventions

against long term direct and indirect impacts on consumers, including on the sustainability of digital services and consumer choice.

5.4. The DPC should also prioritise amicable resolution of user complaints wherever possible, as set out in the DPC's earlier consultation. Guidance on how settlements can be used to drive more effective and faster data protection compliance would also be welcome. The DPC should consider formalising procedures for this, including appropriate transparency measures.

5.5. Finally, there are complaints made to the DPC which are outside the scope of or only tangentially related to GDPR (e.g.: quality of service, authentication issues, safety matters etc.). We recommend the DPC set up clear parameters as to what it considers to be categories of complaints which fall within the scope of GDPR so that these are clear to users and that complaints handling resources are not expended on such matters. Where users erroneously submit out-of-scope reports to the DPC or through the OSS, the DPC should have effective triage processes so that these reports can be extracted and passed to service providers so that they can respond to their customers in a timely way. The DPC should drive a uniform approach at the EDPB level.

6. Strategic Goal 3: Prioritise the protection of children and other vulnerable groups

6.1. We support the DPC in prioritising the protection of children and the fact that the best interests of the child must always be a primary consideration in the processing of children's data. The DPC acknowledges that there is a risk of over-caution on the part of data controllers. The DPC's attention on this is welcome as certain interpretations of data protection law can generate consequences for children and young people, for example by discouraging the provision of ad-funded services for children or impacting children's fundamental rights such as access to information including online news. In this regard, the DPC should consider including some guidance in the Fundamentals specifically for digital news providers.

6.2. We note the DPC's intention to promote the development of codes of conduct on the processing of children's data and IAB Ireland looks forward to further engagement once guidance is finalised. 6.3. We would welcome further DPC consultation regarding 'other vulnerable groups', since the Fundamentals are limited to children and young people.

7. Strategic Goal 4: Bring clarity to stakeholders

7.1. We welcome the commitment to ensure that the resources of the DPC are not disproportionately occupied by complaints that are easily resolved and "*of less systemic importance*". As noted above, small procedural and operational changes and greater use

of amicable resolution would ensure more efficient resolutions for consumers and free up DPC's resources to focus on priority areas and avoid a build-up of cases.

7.2. We also welcome support for data controllers in their compliance effort and the commitment to fair engagement with organisations to promote openness and trust. In developing this approach, care must be taken to avoid tension with data controller accountability and the risk-based approach at the heart of GDPR.

7.3. This approach should also recognise industry self-regulation as a compliance tool. The DPC should not be constrained by the fact that schemes are not formally recognised by the EDPB as codes of practice. Codes of Conduct developed collaboratively by industry and regulators can provide important clarifying guidance for particular and esoteric types of data and/or practices. Approval of codes is a nascent process and takes considerable time, and it is important in the meantime to incentivise continued investment by market participants in evolving schemes which aim to develop and improve consistency and uniformity for consumers, such as the TCF.

7.4. The consultation notes that the DPC's focus group consultations revealed that consumers felt an undue burden on them as a result of the implementation of GDPR. It is important to recognise that this is to a large extent a consequence of legislators' decision to narrow the available legal bases for the processing of data for the personalisation of advertising and content. While steps can be taken to explain and present these choices in more engaging ways, legislators *intended* consumers to bear the burden of choosing and subsequent DPA guidance has encouraged controllers to unbundle choices and make them more granular. These facts should be integrated in to the DPC's work to promote awareness under Strategic Goal 2.

7.5. IAB Ireland would welcome more detail regarding the DPC's vision for a "*collective approach to investigating systemic issues*" and clarification of what it would entail in practice. This should include published criteria on when a "collective approach" will be adopted and guidance on the procedures to be followed, enshrining fairness and respect for confidentiality. Likewise, we would welcome clarity on what is envisaged by introducing "*consolidated*" enforcement in partnership with peer DPAs.

8. Strategic Goal 5: Support organisations and drive compliance

8.1. In recognition of the DPC's finite resources and to enable both the DPC and its stakeholders to prioritise sufficient resource to engagement, we would recommend that the DPC takes a risk-based approach across all aspects of its Regulatory Strategy, including its approach to communicating with stakeholders in an effective manner on the issues that impact most on individuals. This approach will ensure that Ireland's data protection law is consistent and interoperable with the international data protection regulatory landscape in which Ireland is situated.

8.2. IAB Ireland welcomes the commitment to greater transparency and communication around the scope of DPC inquiries and investment in engagement to drive compliance. We agree that where the DPC acts as a lead regulatory authority in cross-border inquiries, results must be deliverable within the stipulations of the law and as such consistent with a risk-based approach and the accountability principle.

8.3. We welcome the commitment to maintaining and enhancing technological foresight. It is important that the DPC makes decisions with a fulsome understanding of how the architecture of the internet is evolving and what this means for the sustainability and future evolution of new uses of data of great benefit to society, and business models that rely on it, including for how this shapes compliance with GDPR.

8.4. IAB Ireland welcomes the proposal to engage with representative bodies to build trust. As noted above, IAB Ireland, in partnership with IAB Europe, stands ready to facilitate such a dialogue.

8.5. IAB Ireland would welcome more detail regarding the DPC's vision for producing "*indicative guidance on scope-setting for large-scale and multi-national inquiries*" and what this might entail in practice.

6. Unidentified individual

I ASK NOT TO BE PUBLICLY IDENTIFIED.

BUT AM AVAILEABLE TO EXPLAINN ANY OF MY OBSERVATIONS IN LIFE.

Community Policing .

Review of there powers , not allowed to act in surveillance capacity of Ordinary individuals going about there daily lifes.

They should be made visible to the public and identifiable and accountable .

What safe guards are in place if a member of an Garda was to divulge sensitive information to members of community policing and this information leaked out to wider community.

Are there minutes of meeting kept and are they available to the community on request.

How safe are the citizens mobile phone numbers who sign up to the community text alert system ?????

Policing

Before some one is added to the Pulse system all parties should be informed of the incident report and its content, to make sure there are no mis representations.

Covert Surveliance of our public beaches ,parks scenic areas, graveyards public and private roadways This should have signage explaining to the public of any activity or intended activity which would infringe on there human rights.. The majority of people who use these public area are decent law abiding citizens and it would be unfair to have there privacy infringed.

Phone watch home security cameras

Need for workers to be informed cameras are they being monitored. Should be made Compulsory to have appropriate signage in place. Notify the parties and give them the option do they want there work monitored at the outset.

What safe guards are in place so as the phone watch contract on a premises dosent extend into the surrounding adjacent areas.

Any proposed use of drones needs to go throug public debate to inform citizens of the possible infringement of there privacy.

Area of HR

Any personal data gathered by employers and there HR department should be shared with the data subject from the outset , to make sure they are happy with the process and the data collected.

Other points of view

There needs to be more accountability and consequences for any failings or wrong doing by organizations and individuals. HSE .DATA BREACH.

There needs to be Independent review of any organization found to have being involved in data breaches or violations of a persons or organizations privacy.

NO MORE INTERNAL REVIEWS WHICH HAVE BEEN KNOWN TO SWEEP THE WRONG DOING UNDER THE CARPET.

Greater urgency in implementing the full new GDPR REGULATIONS INTO SOCIETY ITS 3 YEARS ON SO NO EXCUSES FOR NEGLEGENCE OR IGNORANCE ON THE SUBLECT

The new Digital travel card should have been voted on by the Irish citizens ,not some group of European MPS a (REFERENDUM) Is it democratic or constitutional to have this imposed on citizens.

Any state bodies or Goverment organisations including the HSE , TUSLA GARDA

Should show all paaries any data they have built up on there filies ,WHEN REQUESTED so that everyone is in agreement with the information gathered from the outset before it is uploaded on to computer files.

We are all equal citizens have rights'

Any person or organization who have been wrongly identified accused of any wrong doing by the above organizations should be notified immediately and appropriate apologies and compensation put in place. (Observed by social workers for example)

Why cant the survivors of institutional abuse be given there data ?. Whats the hold up?

7. Irish Council for Civil Liberties

Response to the DPC regulatory draft strategy

Dear Colleagues,

We commend your exercise in consulting on the Data Protection Commission's strategy for the next half decade, and endorse many of the aspirations contained within the consultation document.

In this response to your invitation we make two recommendations of highest priority, and further recommendations on matters of lower priority.

HIGHEST PRIORITY

Highest priority: take on Big Tech

ICCL notes the realistic and practical reference to the finite resources of the DPC, and the need to put these resources to where they can do the most good. We also note with approval the intention to take an approach based on risk, prioritising matters that create higher risks for larger numbers of people over others.

The DPC has shown itself willing to enforce against the public sector, for example in the matter of the Public Services Card. But there is a severe underenforcement against dominant players in the private sector that create high risks for large numbers of people. Those entities set the model for the behaviour of smaller firms, too.

We are therefore deeply concerned by the consultation document's suggestion that guidance from the DPC will suffice.

It is now over five years since the GDPR was applied, and over three years since it came into effect. The 2018-2020 grace period is over. Indeed, since an infringement of the GDPR is highly likely to be an infringement under the ePrivacy Directive, this grace period may have been unnecessary. We strongly urge that the DPC to move to hard enforcement. Urgently. Otherwise, not only will the fundamental rights of individuals remain imperilled, but the DPC will face a more emboldened and entrenched group of systematic infringers.

We also caution against relying on guidance as a means of prompting enforcement. Those with experience in industry will recognise that the surest way to give clarity to data controllers about the law is to show that several years of systematic infringement will be sanctioned. Sanctions must be severe enough to be dissuasive, and should use orders banning processing where possible.

Therefore, while recognising the DPC's efforts to enforce in the public sector, ICCL strongly suggests that the DPC's highest strategic priority must be robust, adversarial enforcement against unlawful data processing by Big Tech.

Highest priority: reform and strengthen the Commission

An important step over the next five years should be to acknowledge and the many issues raised at the 27 April hearing of the Oireachtas Justice Committee. We recommend that the DPC urgently request that the Minister appoint two additional commissioners, and that it request that the State establish an independent review of how best to reform and strengthen the DPC. In addition, we commend the consultation document's references to expertise and training. Further detail in this area would be useful.

LOWER PRIORITY

1. Competition

We recommend that the DPC investigate collaboration between data protection supervisory authorities and their sister agencies supervising competition matters. Underenforcement in competition has made the task of data protection authorities harder, by allowing big tech firms to gain positions of significant power.

Underenforcement in data protection has now also made the task of competition authorities harder, entangling them in matters previous beyond their purview. Big Tech market and rights problems metastasized in the gap between data protection and competition authorities. These gaps must close.

Though competition & data protection communities have caused problems for each other, they offer remedies for each other, too. For example, the supervisory authorities of Hamburg and Bonn's cooperation with the Bundeskartelamt in Germany, the cooperation between the CNIL and the Autorité de la concurrence in France, and the recent memorandum of understanding between the ICO and the Competition & Markets Authority in the UK.

As lead authority for Google, Facebook, Microsoft, Apple, and other Big Tech firms, it is important that the DPC attempt to stimulate cooperation with its competition counterparts.

2. Transparency

We commend the DPC for aspiring to more transparency. However, we note that the DPC has so far refused to provide ICCL with a statistics on the use of its powers – while ICCL has received information from other supervisory authorities. We urge the

Commission to regularly publish statistics on the use of its powers of investigation and sanction under Section 127 and 130 - 140 of the Data Protection Act 2018. We also urge the Commission to waive its broadly interpreted exceptions to the Freedom of Information Act.

3. We note that the DPC has a responsibly to investigate every complaint

The DPC is required to investigate every complaint, and inform the complaint of the outcome, per Article 57(1)f of the GDPR. The only exception is if a complaint is withdrawn by the person who made it. There may have been confusion about this responsibility in the Commissioner's testimony. We elaborate on this in a note to the Oireachtas Justice Committee, following the 27 April hearing at which I and the Commissioner gave testimony.

We note that some of the plans in the consultation document may envisage an approach at odds with this responsibility.

Yours faithfully,

Dr Johnny Ryan FRHistS

ICCL Senior Fellow

8. The Association of Compliance Officers in Ireland (ACOI)

The Association of Compliance Officers in Ireland (ACOI) is the professional body for compliance professionals. With over 3,000 members, it is the premier provider of education and professional development in compliance, providing an authoritative voice on matters relating to regulatory compliance and business ethics in industry in Ireland.

The ACOI welcomes the publication of the Regulatory Strategy Consultation by the Data Protection Commission (DPC) and the opportunity to input to the Strategy for 2021-2026. The ACOI is well placed to provide informed commentary given its diverse membership that includes Data Protection Officers (DPOs) and compliance professionals from a broad range of sectors subject to different levels of regulation and supervision. ACOI members are engaged at the front line in safeguarding the data protection rights of data subjects, be they customers, employees or other stakeholders.

The membership also includes compliance professionals with experience working for regulators or for industry participants with deep knowledge of developed, risk-based regulatory models, such as the EU Single Supervisory Mechanism (SSM). The ACOI also engages with other regulators such as the Central Bank of Ireland on learning events on issues of importance to members. The ACOI welcomes such mutually beneficial engagement that enables open and clear communication between the compliance community and regulatory actors with the shared purpose of enhancing and supporting robust compliance risk management across firms for the benefit of society.

The timing of the consultation is also welcome at a key juncture in the development of the DPC's regulatory model- three years after the coming into force of the EU General Data Protection Regulation (GDPR) and the issuance of a growing volume of decisions and key judgements on the application of the GDPR including DPC v. Facebook Ireland Limited & Schrems – July 2020.

This response is structured according to the five strategic goals set out in the Strategy document, preceded by general feedback. The views expressed in this consultation reflect those of the ACOI as a professional body.

General Feedback

The ACOI notes and welcomes the publication and engagement on the Regulatory Strategy of the DPC. The ACOI also acknowledges the expansive mandate of the DPC ranging from advisory activities of educating and raising public awareness of data protection rights to enforcing those rights through supervision and enforcement. Therefore, applying a risk-based regulatory approach as noted in the Regulatory

Strategy consultation makes sense in terms of maximising the effectiveness of available resources.

The ACOI proposes that additional detail is published on how this risk-based regulatory approach will work in practice, particularly in terms of the risk criteria that will determine the level of supervision and scrutiny that data controllers and processors will be subject to. Further detail would also be welcome on what supervisory methods and the frequency of their application can be expected by firms and organisations for the different risk tiers. This context will enable our members who are DPOs and data protection compliance professionals to clearly and credibly communicate with boards and senior management on the DPC's expectations for an effective data protection compliance framework for their firm's peer group.

1. Regulate Consistently and Effectively

The ACOI welcomes the DPC's acknowledgement of the need to increase the certainty and stability in how data protection law is applied to underpin consistent and effective regulatory performance.

The ACOI notes that most of its members' employer firms and organisations conduct business across borders or have service providers based in other jurisdictions. Key to such firms seeking to apply the same data protection framework in different jurisdictions is regulatory consistency among and between EU Data Protection Authorities (DPAs). For instance, the current divergent approach across EU Member States towards website cookies creates an undue regulatory burden for firms and impedes harmonisation. While acknowledging that this particular divergence emanates from the stalled negotiations over the proposed ePrivacy Regulation, there is evidently room for further coordination and greater consistency between EU DPAs in which the DPC can play a lead role in promoting.

There is further scope for EU-level coordination on identifying key data protection risks such as systemic cyber security vulnerabilities. A supranational data protection risk assessment, similar to the exercise published by the European Commission under the EU Fourth Money Laundering Directive, should enable a greater harmonisation of supervisory priorities and regulatory outcomes across EU Member States.

We also note that the DPC must work within the procedures of the European Data Protection Board including consulting with other EU Data Protection Authorities which can lead to delay and moderation of regulatory outcomes such as enforcement Decisions, impinging on regulatory effectiveness. Therefore, the ACOI supports the proposal of the DPC to seek clarification and consistency under the One-Stop-Shop mechanism and international cooperation.

The ACOI also notes and supports the DPC in seeking adequate resources from Government to ensure its operational effectiveness and capacity to discharge its broad mandate and prevent, detect and deter breaches of data protection law.

2. Safeguard individuals and promote data protection awareness

The ACOI supports the objective and proposal to proactively raise public awareness so that individuals can understand their rights and entitlements under data protection law, with a view to addressing concerns of data subjects without those individuals having to contact the DPC. The ACOI also welcomes the proposal to engage with civil society bodies and is ready and willing to partner with the DPC on awareness-raising events and fora. ACOI members, particularly those that are DPOs are eager to engage with the DPC to understand regulatory priorities, common data protection issues and observed good practice. Post-pandemic, the ACOI plans to launch a DPO Forum to facilitate this engagement and cross-learning between DPO members and, it is hoped, direct engagement with the DPC. The ACOI is also available to engage with the DPC and coordinate with ACOI members who are also members of DPC's DPO Network.

The ACOI is a leading provider of education in the area of data protection, through the delivery of the Professional Certificate in Data Protection in conjunction with the Institute of Banking. The Professional Certificate is accredited by University College Dublin at postgraduate level 9 on the National Framework for Qualifications. The ACOI offers the Certified Data Protection Officer designation to successful graduates subject to Continuous Professional Development requirements. The Professional Certificate was developed and designed to strengthen data protection risk management skills before the introduction of the GDPR and has evolved continuously in tandem with data protection requirements and expectations.

In addition, the ACOI is keen to support strong levels of data protection awareness on an ongoing basis across its broader membership. Representatives of the DPC have presented at ACOI events in the past and it is hoped to increase this engagement and provide the DPC with direct access to a community of over 3,000 compliance professionals. ACOI members are also keen to engage with the DPC on the development of sectoral codes of conduct and certifications to facilitate the implementation of good data protection compliance practices across sectors and the demonstration of same.

As noted above we also echo the proposal for the DPC to take a lead role in engaging with other DPAs to drive harmonisation and cohesiveness of enforcement and consistency of regulatory outcomes.

3. Prioritise the protection of children and other vulnerable groups

The ACOI recognises the social imperative in providing special protections to children and vulnerable groups given the potential risks and impacts in this evolving area. The proposals to conduct research on how data protection controls are applied, and also to provide educational materials in a variety of formats, are also welcome. As articulated above, ACOI members are keen to engage on the development of codes of conduct that can underpin consistent standards of data protection and bring clarity to all stakeholders.

4. Bring clarity to stakeholders

The ACOI welcomes the proposal to move away from investigations based on individual complaints to "a collective approach". Further detail would also be welcome on how this will work in practice and within the risk-based supervisory approach. The proportionate application of corrective powers is also welcome, particularly in cases of complaints where there are no systemic or significant impacts to fundamental rights and freedoms. The ACOI also supports the proposal to maintain and enhance the DPC's technological foresight to ensure that risks with emerging and rapidly evolving technologies do not go unidentified.

It falls to the DPC to set the regulatory priorities that data controllers and processors should be focussed on, as the DPC has the holistic view of data protection risks and threats. The ACOI advocates that the DPC engages and communicates on these priorities, even if they are varied across sectors and types of data controllers and processors. As noted above, the ACOI advocates enhanced regulatory coordination and cohesion at an EU and international level.

5. Support organisations and drive compliance

The ACOI supports the DPC's proportionate application of its enforcement tools in an evolving data protection environment. Such proportionality provides scope to take into account the influence dynamics between small-scale data controllers and large-scale data processors, and data protection arrangements therein. The prioritisation of infractions that result from wilful, negligent or criminal intent facilitates risk-based supervision while addressing the most acute data protection risks.

The ACOI very much supports the proposal to promote a cultural shift towards compliance by extensive engagement with stakeholders, and stands ready to facilitate such engagement with the compliance community. The ACOI can provide established means of communication to enable this engagement through membership webinars, podcasts, events and conferences, as well as a quarterly membership publication and monthly email bulletin. The ACOI is also ready to engage informally as needed on DPC proposals and initiatives through its Data Protection and Information Security Working Group and DPO members.

The ACOI also advocates engagement on proposed guidance with impacted stakeholders through consultation on proposed, draft guidance. The proposal for guidance for micro, small and medium sized enterprises is likely to be of particular interest but ACOI members are eager to engage in developing guidance more broadly, be it for particular sectors or risk areas.

The ACOI supports the publication of detailed case studies of decisions which provide a useful if specific frame of reference. Another mechanism, which has been historically effective in regulators communicating expectations to stakeholders, has been the publication of themed findings and identified good practices from inspections of particular sectors, or specific areas of risk and/or control. Such publications allow members to meaningfully benchmark their employers' against regulatory expectations for their peer group.

Conclusion

This regulatory strategy consultation is welcome and timely given the ongoing evolution of data protection legislation and guidance, and the implementation of same. The regulatory strategy consultation is also transparent and open regarding the challenges faced by data controllers and processors and the DPC that have led to ambiguities in the interpretation and application of data protection law. These ambiguities present difficulties for our members in data protection roles, their boards and senior management in effectively managing their data protection frameworks. Enhanced engagement and guidance from the DPC coupled with further EU legislation on specific risk areas, such as the Artificial Intelligence Regulation, will help members and their firms and organisations by removing such ambiguities.

The ACOI supports the desired outcomes and proposals of the proposed regulatory strategy and its five strategic goals. We also look forward to engaging with the DPC and further information on how the strategy will be applied in practice in order to achieve the continuous enhancement and strengthening of data protection standards in Ireland

9. Office of the Government Chief Information Officer Department of Public Expenditure and Reform: Data Governance Unit

General Comments:

- Good to see consistency in all areas as a key element of the strategy.
- It would be good to see the DPC be clearer about what technological methods they will use to deliver on this strategy.
- The term 'governance' is not referenced (data or otherwise) in the strategy document.
- It's not clear what the DPC's approach is when new data protection law is introduced, something we may expect over a duration of 5 years.
- Clear concise regulation is key and the DPC is underlining this in the strategy which is important – this is a positive.

Section: Regulate Consistently & Effectively (Pg10)

- *"Improving guidance to individuals, including vulnerable groups, in an appropriate format, promoting deeper understanding of data protection law and increased control over personal information "*

It's not clear by what methods, how? Will this impact data sharing capabilities?

- *Increasing transparency and provision of information on the DPC's outreach activities and engagement with stakeholders;*

Will there be specific provision of information for Data Protection Officers?

- The use of case studies is a very useful tool in improving understand of the data protection law, we support this in particular when new data protection legislation is introduced.
- *"Working closely with the European Data Protection Board to develop legal certainty for international transfers of personal data"*

Is this just for EIDAS or what else is in scope?

Section: Safeguard Individuals & Promote Data Protection Awareness (Pg11)

- Most of this section seems to be suggesting targeted case resolution. Handling bigger / wider ranging complaints. It's not clear what they will do with the smaller complaints. Will they be addressed?
- Will they use analytics to correlate the data & address higher volume queries as one "super complaint"
- Interested to see how machine learning / analytics can address this and if so are there GDPR processing issues processing / analysing complaints?

Section: Prioritise the protection of children and other vulnerable groups (Pg14)

- *"Actively promotion the development of codes of conduct of processing of children's personal data."*
- This seems reasonable however they are suggesting increased standards? Maybe higher business case / DPIAs for data which holds children info / vulnerable persons. How does this work with the SP data set where it would be a mix?
- There are 4 references to data sharing – all in Strategic Goal 3 which is to Prioritise the protection of children and other vulnerable groups but the scope of data sharing is pan public service.

Section: Bring clarity to stakeholders (Pg17)

- *For complaints that disclose no significant impact to fundamental rights and freedoms and are not systemic in nature, the DPC will take a proportionate response*
- This seems like a good concept – focusing on those issues that are most impactful – how they differentiate will be interesting? "Higher systemic impact" – the metrics for this perhaps should be detailed?

Section: Support organisations and drive compliance (Pg20)

- *"The introduction of harmonised data protection law without a harmonised enforcement framework has produced some inconsistencies of understanding as to what impactful regulation measures"*

- Agree with the above statement – it can be very tough to understand and bodies tend to be risk adverse so it seems like it dissuades data sharing completely.
- Driving compliance will be more effective than fines – ultimately. So believe this is a good position to start with.

10. Technology Ireland

Technology Ireland is an Association within Ibec, which represents the ICT, Digital and Software Technology Sector. The Association is a pro-active membership organisation with over 200-member companies located throughout Ireland. We advocate on behalf of Ireland's indigenous and foreign direct investment (FDI) technology companies to Government and policy makers.

Summary of Technology Ireland Position:

Technology Ireland is very grateful to the Data Protection Commission for the opportunity to comment on the draft Strategy for 2021-2026. As the Strategy itself notes, these will be five crucial years in the evolution of data protection law, regulation, and culture.

We share our member's wish for the clear, risk-based and evidence-based regulation of personal data, consistent and interoperable with the international data protection regulatory landscape in which Ireland is situated. In particular we believe that this entails ensuring that Ireland's data protection law protects all stakeholders and takes special account of the protection of children.

Technology Ireland is strongly supportive of the five goals outlined by the DPC. We also agree that the most successful outcomes for the DPC, individuals, companies, and society is contingent on a pro-active and engaged approach to regulation. The DPC should ensure that the strategy centres on three guiding principles:

I. The DPC should continue to reinforce a risk-based and evidence-based position on all activities and decisions.

II. The DPC should strategically prioritise its complaint handling resources to provide timely compliance support and guidance when and where it is needed and support the evolution of digital business and new technologies.

III. The DPC should continue a policy of close engagement and consultation with companies to understand their business, the functioning and evolution of markets and the impact of ever evolving technology as well as the social and economic impact of personal data protection decisions.

Using the framework of the draft Strategy's proposed five strategic goals please find more detailed comments below:

1 - Regulate consistently and effectively

Consistency with other legislative and regulatory developments: Technology Ireland fully supports the desired outcome that "the DPC's application and enforcement of data protection legislation ..... provides consistent understanding and legal clarity for all stakeholders". Consistency and certainty are key requirements for our members. We would like to emphasise the importance of clarity and consistency between Ireland's data protection law, the primacy of the role of the DPC in enforcing data protection rights and obligations, and other legislative and regulatory developments. We accept that this is mainly for policymakers to address. However, we wish to note that data protection regulation in Ireland is considered in the context of other related policy objectives (around growth of the digital economy and facilitating innovation in the data-driven industry; safety and security; and data portability) to make sure any changes are holistic, and companies do not find themselves being instructed to take diametrically opposed actions due to differing legislative requirements.

Appropriate resources: Technology Ireland has consistently highlighted the need for the DPC to be adequately resourced to carry out its expanding workload. Given Ireland's position as a digital hub and as the repository of 30% of Europe's data[12], this is particularly important, and any shortfall risks reputational damage for Ireland. We note the resolution by the European Parliament on 20 May, calling on the European Commission to open an infringement procedure against Ireland for failing to enforce the General Data Protection Regulation. This resolution underscores the seriousness of ensuring that the DPC has the resources to meet Ireland's objectives under GDPR.[13]

It is also important that the DPC remains competitive in attracting and retaining top quality talent and where necessary should receive sanction from government for specialist recruitment campaigns. Consideration should also be given to providing additional education and training to facilitate the transfer of civil servants from other government departments. Page 3 of 6

Case studies as a mechanism to educate and inform: Technology Ireland members and other stakeholders have expressed how useful the DPC's case studies are in terms of demonstrating the application of data protection law. It would be increasingly valuable for the DPC to extend these case studies to include examples of how an international company should approach compliance with various data protection frameworks.

Threat of regulatory fragmentation: As more countries and regions adopt privacy legislation and develop their regulatory approaches, there is a risk that this could result in divergent approaches being adopted. In light of this, we support the DPC's objective

[12] National Cyber Security Strategy 2019-2024
[13] European Parliament Resolution of 20 May 2021 on the Ruling of the CJEU of 16 July 2020

to engage with data protection authorities from outside the EEA to understand the differences in data protection laws and their implications and collaborating with these authorities where possible.

International data transfers: There is an urgent need for a responsible and balanced approach regarding international transfers that takes into account, as required by the GDPR and Charter, the economic and social impact of data protection decisions that could isolate the EEA by imposing a de facto data localisation or other unworkable or unviable solutions.

Guide to Settlements: Technology Ireland would welcome DPC guidance on how settlements can be used in view of the obvious potential for driving effective and faster data protection compliance and huge resource savings at the DPC national and, where applicable, also at the EDPB level. Where possible settlements can provide a faster solution for resolution of complaints and bolster data protection and compliance, resulting in a better outcome for both parties, and less of a drain on DPC resources. Guidance on how settlements could be used would be very valuable. Case studies, as mentioned above, may be of use here.

One Stop Shop: The OSS (One Stop Shop) model is viewed by Technology Ireland members as an integral part of the efficient and fair monitoring and compliance of data protection regulations across Europe. Cooperation and alignment with the EDPB and other European DPAs is crucial in this regard particularly for companies operating internationally and striving to comply with various authorities. We support the statement in the Strategy that the DPC will work with peer DPAs to introduce consolidated and consistent enforcement across Europe, which would harmonise enforcement approaches and agree the criteria for regulatory success. We would support the strategy going further and setting out how the DPC will work towards this goal and address instances where there are conflicts or differences in interpretation.

While the DPC's support for the OSS is implicit in its draft Strategy, Technology Ireland members would be reassured by an explicit declaration of support, given efforts by some parties in Europe to undermine it. Such efforts represent a minority view and Technology Ireland notes that our colleagues in Digital Europe are firmly supportive of the OSS.

2 - Safeguard individuals and promote data protection awareness

Technology Ireland welcomes the DPC's intention to prioritise cases that are likely to have the greatest systemic impact for the widest number of people over the longer-term. The smooth and efficient operation of the DPC is in the interest of all stakeholders.

It is not specified how the DPC would carry out the assessment on prioritised cases. Could industry share their information about the major misunderstandings their customers face and proactively help resolve such issues partnering with the DPC on a voluntary basis?

Technology Ireland recommends a funnelling system similar to that employed by some DPAs, where appellants are encouraged to demonstrate that they have already contacted the organisation concerned through the data protection dedicated channels with their complaint and have not received a response or the response is not compliant with relevant law. In such cases the regulator contacts the DPO of a data controller on behalf of the data subject and provides a timeline for which the DPO should make contact with the data subject - without regulatory involvement - in an attempt to resolve the matter. This approach ensures that the regulator has an initial involvement, providing the data subject with confirmation of the escalation of their complaint. It also provides the DPO with an opportunity to successfully resolve the complaint outside of the data controller. This process ensures efficiency in resolving these matters and avoids the DPC acting as a conduit for such communications between a data controller and / or its DPO and the complainant. In instances where the DPO is unable to successfully resolve the matter, this could then instigate the full involvement of the DPC.

3 - Prioritise the protection of children and other vulnerable groups

Technology Ireland shares the view of the DPC that children require specific protection and that the best interests of the child must always be the primary consideration in all decisions relating to the processing of their personal data.

Technology Ireland looks forward to the DPC defining the specific protections which will guide companies in safeguarding the rights of children and would be happy to assist in this process as per our earlier submission in March 2021 to the DPC on Fundamentals for a Child-Oriented Approach to Data Processing3.

Section 32 of the DPA 2018 requires that the DPC encourage the drawing up of codes of conduct to promote best practices by organisations that process the personal data of children and young people. Technology Ireland, through the creation of its Online Safety Taskforce in 2019, is committed to engaging on the development of codes of conduct and supportive of the DPCs plans in this regard. The taskforce is a pro-active, member-

led, and inter-company taskforce which strives to develop, communicate, and support the implementation of agreed policy solutions relating to children & online safety matters. Any further guidance which the DPC produce on such codes of conduct would, of course, be very much welcomed.

Technology Ireland submission to Data Protection Commission on Fundamentals for a Child-Oriented Approach to Data Processing. Technology Ireland members, many of which operate internationally, would be willing to assist in research to determine best practice regarding the use of age verification and assurance mechanisms and methods for obtaining parental consent for online services.

Technology Ireland agrees that the protection of “other vulnerable groups” must be prioritised Some more guidance on this would be useful as the Fundamentals for a Child-Orientated Approach discussed earlier in 2021 may not be optimum for all groups.

4 - Bring clarity to stakeholders;

As per goal two, Technology Ireland agrees that the DPC should “adopt a collective approach to investigating systemic issues” but would like some clarity as to how this will operate in practice.

The DPC should provide clear guidance on the statutory procedures that will be followed for inquiries that are based on a collective approach, with particular regard to fair procedures and respecting confidentiality.

Technology Ireland welcomes the DPC’s explicit recognition “that most businesses and organisations are keen to meet their obligations under the GDPR” and that the focus should be on supporting “data controllers in their compliance efforts”, before resorting to punitive measures.

5 – Support organisations and drive compliance

Technology Ireland is glad to see that the DPC recognises that industry has consistently called for a risk-based approach, where only “instances of wilful negligence or deliberate infractions would be punished more severely”.

Technology Ireland fully supports the idea that “developing a culture of compliance will ultimately drive data protection efficacy” and is willing to assist the DPC with this goal, by continuing to act as a conduit between the DPC and our members, ensuring that our

members are kept fully informed as to their obligations and also helping the DPC to stay abreast of changes in technology or practices that could affect compliance.

To help maintain that “culture of compliance” in a rapidly changing tech sector, Technology Ireland suggests setting up a *Clearing House Structur*e to engage with industry on an annual or semi-annual basis. There are formal and informal examples of similar structures with other regulators like COMREG and the Central Bank of Ireland, who recently ran a consultation on Engaging with Stakeholders.4

Where the DPC acts as the Lead Supervisory Authority for cross-border inquiries, it is important that these cases are dealt with as efficiently as possible with optimum transparency and communication with peer DPAs and the subject of such investigations. This is vital to the smooth operation of the OSS and will mitigate any criticisms of it.

General comments

Technology Ireland supports the values set out by the DPC in the Draft Strategy but would suggest adding three more:

- Proportionate
- Evidence based
- Results driven

Conclusion

Technology Ireland is strongly supportive of the overall goals of the draft Regulatory Strategy for 2021-2026. We hope that our comments and observations in this submission are useful to this process.

We recognise that this consultation is only part of an ongoing dialogue with stakeholders. Technology Ireland and its members remain committed to supporting and valuing the work of the Data Protection Commission and look forward to participating in future discussions.

11. Three Ireland

1. Introduction

2. This document is the response of Three Ireland (Hutchison) Limited (Three) to the Data Protection Commission ("DPC") "Regulatory Strategy" Consultation dated April 2021. Three welcomes the opportunity to contribute to the DPC's strategy for the next five years, building on the positive impact that the DPC has had since the introduction of the GDPR and the Data Protection Act 2018, which radically reformed the legislative basis for the regulation of Data Protection in Ireland.

3. Three is Ireland's largest Broadband Mobile Network Operator and has 2.2 million customers, circa 1270 employees across our offices, in Dublin and Limerick, and has 63 stores.

4. Connectivity is key for the Irish economy. 4G rollout is completed and 5G is now launched also and will become more prominent during the period covered by the strategy. Three is leading the way in respect of these transformative changes. Three were the first to launch mobile broadband in Ireland and we drove all you can eat (AYCE), or truly unlimited mobile voice and data offers into the Irish market. Three carries more mobile data on our network than all the other mobile networks combined.

5. The electronic communications sector is going through a period rapid transition. Ireland is on the precipice of transposing the Directive 2018/1972 establishing the European Electronic Communications Code (EECC). In addition to the GDPR and the Act the specific data protection regulatory framework that applies to it, by way of S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ("ePrivacy Regulations), is subject to legislative review at a European level.

6. Three hopes that the forthcoming regulatory landscape changes will in the future take adequately into account the multi-sided markets which are at play in the area of electronic communications whereby over the top providers (OTTs) such as social media platforms will compete in what was once the reserve of traditional communications networks and in which the OTTs have essentially operated in a regulatory lacuna,

including in the Data Protection field. The new landscape shall for the first time bring the OTTs into the scope of the ePrivacy Regulations. Three would hope that OTT service providers such as WhatsApp, Teams, Zoom etc., shall be treated in the same manner as traditional telecommunications companies have been with regards to the full regulatory scope of Data Protection requirements and obligations of the ePrivacy Regulations.

7. As one of the largest network operators and service providers in the country, Three is pleased to comment on DPC's review of its strategy. It is timely in this case, to carry out a review. Many aspects of both the regulatory framework and the sector itself will have changed during the five years covered.

8. Responses to Regulatory Strategy Consultation

Three is hopeful that the DPC will include in its annual report an annual review of progress going forward as against its strategic goals as decided following on from this consultation, this would provide an ongoing signal indicating the areas which will need greater focus for the remaining term.

9. STRATEGIC GOAL 1: Regulate consistently and effectively.

9.1. The DPC should provide clearly defined process documentation outlining the engagement mechanisms (including amicable dispute resolutions) that will be provided to stakeholders to engage with own-volition and third-party commenced investigations and the method through which an investigation will lead to a determination.

9.2. The DPC should improve the online breach notification reporting tool in a manner that creates an online ticket system, such that notifiers can track the status of their breach from a DPC perspective from receipt, through engagement to closure. In particular Three believes that effective and consistent regulation is required to build trust in the public regarding those who process personal data. It is important that the DPC ensures that those who are responsible for personal data have all the support and guidance that they need to understand what it means to be transparent and how to embed these practices into their organisation.

In order to achieve this outcome, Three would propose that the DPC would prioritise the following actions: would ask that notifiers be provided with a Breach Number ("BN") at the conclusion of the initial notification process, in ease of subsequent communications.

9.3. The DPC should more actively promote within industry sectors the establishment of Codes of Conduct under Article 40 of the GDPR, outlining the benefits for Code adherents.

10. STRATEGIC GOAL 2: Safeguard individuals and promote data protection awareness.

10.1. Promoting the use of 'Plain English' in Privacy Statements and Cookie Notice through the publication of best practice examples, on an ongoing basis.

10.2. Promoting the establishment and use of the Certification mechanism provided for in Article 42 of the GDPR including the establishment of the register provided for in Article 42.8 of the GDPR. Three supports the DPC in their goal to improve standards of data protection practice through clear, inspiring, and targeted engagement and influence. The benefit of the tools and mechanisms provided for in the GDPR can maximised through the provision by the DPC of solid guidance, clear assurance and working in partnership with Data Controllers and Processors.

In order to achieve this outcome, Three would propose that the DPC would prioritise the following actions:

11. STRATEGIC GOAL 3: Prioritise the protection of children and other vulnerable groups.

The effective and proportionate regulation of Data Protection in so far as it impacts children needs to address the context of the reality of children's lives and circumstances. A survey by Childwise in the UK has found, based on a survey of 2,167 UK five- to 16-year-olds, that 53% of children owned mobile phones by around the age of seven and that by the age 11, 90% had their own device, and phone ownership was "almost universal" once children were in secondary school. Children, as a result, are engaging with Information Society Services, Social Networks, Large Scale Digital Service Providers as well as their Mobile Network Operators.

11.1. Support the Minister in conducting a review of the operations of Section 31.1 of the Data Protection Act 2018, from a practical perspective as opposed to an aspirational one. Consideration should be made to reducing the age to 13 to recognise the reality on the ground, but in parallel, increasing focus actively on promoting Codes of Conduct for Children.

11.2. Promote the establishment of Children's Privacy advocates in representative bodies and stakeholder groups. Provide a focal point for the distribution of material readily consumable by children in multi-media addressing privacy topics in a relatable

manner. Provide teaching materials for teachers to draw upon in teaching civics in both secondary and primary school settings.

Three believes that Children are a specific vulnerable and addressable cohort that could really benefit from being the focus of a pillar of DPC strategic goals.

In order to achieve this outcome, Three would propose that the DPC would prioritise the following actions:

12. STRATEGIC GOAL 4: Bring clarity to stakeholders.

12.1. Consider DPO Focus Groups in specific industry areas to ensure alignment with the DPC on emerging technological trends.

12.2. Establishing on online investigation portal that follows any investigation from commencement, through engagement, to closure.

12.3. Keep track on a public register of fines and other sanctions issued, and the actual recovery/implementation of those fines/sanctions.

Three believes that an innovative and broad approach to the regulation of Data Protection has the potential to maximise the impact of the finite resources available to the DPC. Involving and informing stakeholders is the key to building trust in the DPC as an organisation as it is in bringing the benefit of the work the DPC is doing to the general public.

In order to achieve this outcome, Three would propose that the DPC would prioritise the following actions:

13. STRATEGIC GOAL 5: Support organisations and drive compliance

13.1. The DPC might consider establishing a public register of cross-border inquiries, including their current status and stage, and likely timelines to moving forwards.

13.2. The DPC might publish a tabulated list of engagements with each cross-border DPA by subject area.

13.3. Promoting the establishment and use of the Certification mechanism provided for in Article 42 of the GDPR including the establishment of the register provided for in Article 42.8 of the GDPR.

Three shares the view that clarity and consistency regarding sanctions and enforcement actions is a necessary and welcome goal to support organisations responsible for data processing activities. Moreover, Three agrees that the DPC should prioritise prosecution, sanction and/or fining those infractions that result from wilful, negligent or criminal intent.

In order to achieve this outcome, Three would propose that the DPC would prioritise the following actions:

Ends

12. Article Eight Advocacy

Introduction

Article Eight Advocacy is grateful to the Data Protection Commission for giving us this opportunity to provide submissions to this public consultation on the DPC's Draft Regulatory Strategy 2021-2026.

Rather than respond individually to the strategic goals, desired outcomes and proposed actions we have identified some common themes and provided comment on these. We have also used some recent events to illustrate some persistent issues including a brief case study of some of the system-wide data protection problems which occurred relating to the conclusion of the Mother and Baby Homes Commission of Investigation and the transfer of its archive to the Department of Children, Equality, Disability, Integration and Youth.

Increased transparency and clarity

We welcome all the listed activities which will **provide more information for data subjects and data controllers regarding their respective rights and obligations**, and all the initiatives which will provide more visibility into the processes and procedures of the DPC.

More **frequent publication of case studies** will be of benefit to both data controllers and data subjects.

Development and approval of **codes of conduct** and certifications for specific industries and sectors and on the processing of children's personal data will be useful for all concerned.

Standardised procedures which are made publicly available are welcome**.**

The publication of summaries of decisions by the DPC1 which has been introduced since the last public consultation is very helpful both to data controllers / processors and data subjects. Where possible we would like to see the full decisions published as well.

All cooperation and collaboration with peer DPAs and the EDPB to achieve consistency of procedures and standardised enforcement across the EEA is naturally a positive, as are the actions listed relating to staff training, recruitment and securing increased budget allocation from government.

Guidance focus on children, vulnerable groups and smaller controllers

This is welcome as all of these groups could be regarded as underserved currently. A commitment to produce guidance in formats most appropriate for particular groups is welcome and the intention to engage with representative bodies and advocacy groups will inform this.

Prioritisation of resources

While accepting that the resources available to the DPC are limited we are concerned at the mentions of *"Prioritising the allocation of DPC resources to cases that have higher systemic impact on large numbers of people"* without further detail regarding the criteria which will be used to prioritise cases.

- Will these criteria be made public?
- Will individuals be informed if a complaint or concern they have raised has been de-prioritised or down-ranked?

Soft power, forbearance and time elapsed

We appreciate the DPC's intention to regulate fairly and consistently and to use soft power where appropriate as well as hard enforcement tools. However, we contend that certain recurring issues relating to what could be regarded as the 'bread and butter' aspects of data protection compliance should not be given the benefit of the doubt as over **three years have passed** since the GDPR became enforceable and over five years since it became law. To take a very recent example, in June of this year there were media reports[14] that some estate agents had been **seeking excessive amounts of personal data from individuals** in advance of viewing a property.

While the swift intervention of the DPC in this situation was welcome it should not have been necessary. When these reports emerged it was almost two years since guidance for a closely adjacent industry sector was issued by the DPC[15] which it is not unreasonable to expect the data controller(s) involved in the 2021 incident to have been aware of.

[14] Data Protection Commission investigating Savills 'proof of funds' demand for home viewing' , Irish Independent, 16th June 2021

[15] Guidance on Requesting Personal Data from Prospective Tenants' , Data Protection Commission, July 2019

In addition, none of the issues concerned were new in the GDPR. Data minimisation and purpose limitation as fundamental principles were present in the GDPR's predecessor and its domestic enabling legislation.

More generally, data protection by design and default is not well understood. All processing operations created in the last three years should abide by this. Necessity and proportionality assessments, whether in the form of a full Data Protection Impact Assessment or otherwise are often not being carried out.

Where Data Protection Impact Assessments are carried out it is frequently after the design work on the proposed system has been completed. An exception to this trend was the Data Protection Impact Assessment for the HSE COVID Tracker App[16], which was of a high standard and made publicly available. Feedback was solicited and incorporated. This should have set a benchmark for public sector Data Protection Impact Assessments.

The use of CCTV to combat illegal littering remains a popular issue with local and national politicians despite decisions issuing from the DPC in respect of the use of surveillance technologies by several local authorities. It seems there may be **a lack of political understanding of the nature of many of these issues** i.e. if a use by one local authority for a particular purpose is found to be non-compliant for then it is likely that a similar use for the same purpose by a different local authority is also likely to be non-compliant

While there are indisputably areas of complexity and contention within the DPC's broad mandate, many of the problems encountered by data subjects are the same problems which existed before the GDPR and persist now. In fact we are seeing continued instances of the **GDPR being cited as somehow preventing rather than enabling data controllers to give effect to the rights of individuals**.[17] [18]

Misunderstandings of the most basic concepts of data protection law and its purposes and principles should not be allowed to persist. These misunderstandings can only be shown leniency for so long.

CASE STUDY: Compliance culture versus full-stack systemic problems in the public sector

[16] Data Protection Impact Assessment for the COVID Tracker App – 26.06.2020'

[17] Tusla relying on 'flimsy grounds' to justify redacting records and birth certs' , Irish Examiner, 7th October 2019

[18] Work of Catholic Church safeguarding body limited by data protection rules' , Irish Times, 22nd June 2021

We welcome the DPC's intention to work towards what is termed a "compliance culture" in the draft strategy. This will undoubtedly be a large piece of work which will span the five years of the draft strategy and more.

It is unclear how long it may take for a compliance culture to take hold when non-compliance, failings and misunderstandings throughout the system continue. As a form of case study it is useful to look at the events surrounding the transfer of the archive of the Mother and Baby Homes Commission of Investigation to the Department of Children, Equality, Disability, Integration and Youth which happened earlier this year when the Commission of Investigation was dissolved, and the continuing difficulties data subjects are experiencing in gaining full access to their personal data, as is their right under the Charter.

The following touches on only some of the events which impacted on individuals' data protection rights. Many of these issues have not as yet been adequately resolved.

It is of particular note and should give rise to especial concern that these failings, from the drafting of legislation through attempted destruction of personal data without a lawful basis right down to persistent administrative issues in public sector data controllers should have happened in such a high-profile situation which attracted extensive national and international media coverage. It invites questions as to what systemic failures may be occurring in less high-profile situations.

Misunderstanding of the scope of the GDPR, September-October 2020

In September 2020 the Minister for Children, Equality, Disability, Integration and Youth published the Draft Scheme of what would become the *Commission of Investigation (Mother and Baby Homes and certain related Matters) Records, and another Matter, Act 2020*.

The Department and the Minister insisted until a few days *after* this legislation was signed into law that the GDPR did not apply to the archive of the Mother and Baby Homes Commission of Investigation.

Minister for Children Roderic O'Gorman said he consulted with the Office of the Attorney General who confirmed that GDPR laws do apply to the archive - meaning people will have a right to access personal information.[19]

[19] Groups welcome access to personal data on mother-and-baby homes' , RTÉ, 29th October 2020

This demonstrated a lack of understanding of the reach of data protection law, the principle of primacy of EU law and the obligation to set aside conflicting domestic legislation, as stated "repeatedly"8 in the case law of the CJEU.

This Bill therefore passed through the entire legislative process with the government maintaining the GDPR simply did not apply to the records in the Commission of Investigation's archive.

While we note from the DPC's 2020 Annual Report9 that a legislative consultation in relation to this Bill did occur, significant failings and confusion continued after it became law in the period until the Commission of Investigation was finally dissolved at the end of February and the archive was transferred to the DCEDIY and Tusla.

Redactions, deletions and added confusion

Section 6 of the Act included a mechanism for redaction of certain personal data should an individual request this before the archive was transferred. From correspondence between your office and the Commission of Investigation it seems clear that the Commission of Investigation did not have even a rudimentary understanding of the basics of data protection law.

"It is also important to note in this regard that consent is not the only legal basis for the processing of personal data that is recognised by Article 8 of the EU Charter, contrary to what you assert elsewhere in your letter."

It still remains unclear what criteria the Commission of Investigation used to carry out the mandated redactions. Nor was it ever publicly stated what the lawful basis was for the attempted deletion of hundreds of audio recordings of testimony to the Commission's Confidential Committee, which were subsequently retrieved from backups.

No apparent effort made to comply with Article 14

Once the archive transferred to the Department of Children, Equality, Disability, Integration and Youth and this Department became the data controller it had an obligation under Article 14 GDPR to inform data subjects. Commissioner Dixon provided

a concise explanation of the obligation Article 14 of the GDPR imposes during a recent session of the Oireachtas Joint Committee on Justice.

“Under Article 14 of the GDPR, if a data controller obtains data indirectly -- not directly from the data subjects themselves -- they have an obligation as soon as possible thereafter to inform data subjects. So typically that would be an obligation on them”[20]

It is undisputed that the Department of Children obtained the personal data contained in the Archive indirectly. A new unit was established within the Department specifically to handle requests relating to the archive of the Commission of Investigation.

A new Unit has been established to look after this hugely important and significant volume of work. This work has included ensuring that there is a range of expertise including data protection expertise within the Unit. In addition, the Department has engaged external data protection expertise to support the processing of requests from data subjects and to appropriately vindicate the rights of data subjects.[21]

Yet the Irish Examiner reported on the 23rd April that the Department had given it a response to a media query which stated the Department had not and did not intend to meet its obligations under Article 14 GDPR.

All of the records relating to the trials are now with the Department of Children. The Irish Examiner asked the department if it had a duty to inform people they were part of a vaccine trial, where it has that information.

It said such a process would give rise to "significant implications, including legal implications''.

"In particular, it would require a clear legal basis for accessing the archive for this purpose which would have to be provided for in primary legislation,” it said a statement.

The department pointed out that "everyone has the right to access their own personal data and can make a subject access request (SAR) to the department in respect of their own personal information".

They "would receive information on their involvement with vaccines trials where that is in the archive in relation to them".[22]

---

[20] Helen Dixon, Oireachtas Joint Committee on Justice Debate, 27th April 2021

[21] Minister for Children, Equality, Disability, Integration and Youth Roderic O'Gorman, Response to written Parliamentary Question, 6th May 2021

[22] Mother and baby home survivors demand vaccine trial records' , Irish Examiner, 23rd April 2021

The insistence that a "clear legal basis" would be required for the purpose of meeting Article[23] obligations appears to show a clear lack of understanding of the nature of the obligation imposed. That a data controller is prepared to give a statement such as this to a national newspaper should be of some concern.

Withholding of medical records

More recently it emerged that the Department is withholding health data based on S.I. 82/198914 as amended by the Data Protection Act 2018.

"Where there is 'health' data, the department is required by the regulations to engage in a consultation procedure with the requestor's health practitioner before supplying them with any of this data."[24]

The Department appears to have applied this exemption in a blanket fashion to all records it identified as health data, despite this not being a requirement in the Statutory Instrument, which should have been set aside[25] in any case.

Restrictions are only lawful when they are a necessary and proportionate measure in a democratic society, as stated in Article 23(1) GDPR[26]

No explanation of how this restriction is necessary and proportionate is present in the Statutory Instrument, nor was one provided to data subjects.

If a controller considers that it is justified in withholding certain information in response to an access or portability request it must identify an exemption under the GDPR or the Data Protection Act 2018, provide an explanation as to why it applies, and demonstrate that reliance on the exemption is necessary and proportionate.[27]

Improvements made in some areas but not others

The Subject Access Request form developed and published by the Department for requests relating to the archive of the Mother and Baby Homes Commission of

---

[23] S.I. No. 82/1989 - Data Protection (Access Modification) (Health) Regulations, 1989 , irishstatutebook.ie

[24] 'Survivors 'infantilised' by records being withheld' , Irish Examiner, 7th June 2021

[25] CJEU, Minister for Justice and Equality, Commissioner of An Garda Síochána v Workplace Relations Commission, C-378/17, 4th December 2018, para 38

[26] Guidelines 10/20 on restrictions under Article 23 GDPR' , EDPB, December 2020

[27] Access and Portability' , Data Protection Commission website

Investigation[28] features an acknowledgement that there is no legal requirement for a data subject to complete the form as part of a valid Subject Access Request, which is a positive step.

However the Department's general Subject Access Request form does not feature any such acknowledgement, creating a preposterous situation where one unit of the Department is abiding by the GDPR and the larger entity is not.

This array of non-compliant behaviour - whether deliberate or through extremely poor understanding of data protection law and data controllers' obligations - across multiple data controllers and Government over a period of close to a year when dealing with the personal data of the same group of data subjects is alarming.

We therefore very much welcome the DPC's commitment to continue its *"efforts to bring clarity and consistency to the application of data protection law, so that controllers can operate effectively and without undue anxiety"* and to clarify *"the bases for data sharing, so that individuals are not disadvantaged or at risk as a consequence of over caution on the part of data controllers".* As this case study illustrates, there is much work to be done in this area.

About Article Eight Advocacy

Article Eight Advocacy is an independent not for profit organisation which advocates for data subject rights in Ireland. We support data subjects by using all the tools available to us to ensure their fundamental right to protection of their personal data is respected.

We do this by providing easy to understand information on what data protection means for individuals on our datasubject.ie website, submitting complaints to the Data Protection Commission on behalf of individuals and managing the progress of these, initiating litigation where necessary, and carrying out research to uncover misuses of personal data.

[28] Subject Access Request Application Form – Records relating to the Mother and Baby Homes Commission of Investigation (April 2021), available at Transfer of records from the Mother and Baby Homes Commission of Investigation

13. Introduction National Voluntary Service Providers

The Data Protection Commission sets out an ambitious vision for what it believes will be five crucial years in the evolution of data protection law, regulation and culture in their Draft Regulatory Strategy for 2021-2026.

Over two thirds of disability services in Ireland are provided on behalf of the State by the voluntary sector. The National Federation of Voluntary Service Providers Supporting People with Intellectual Disability is the national umbrella organisation of not-for-profit agencies providing direct supports and services to people with intellectual disability in Ireland. Across almost 60 organisations, our members support more than 26,000 children and adults with intellectual disabilities and their families, providing services and supports throughout the lifespan. Our membership is made up of organisations funded under Section 38 and Section 39 of the Health Act.

The membership of the Data Protection Network comprises Data Protection Officers and staff working in the area of data protection. The network meets quarterly. The purpose of the network is to support the members in understanding and meeting the requirements of the Data Protection Act and the General Data Protection Regulations. The first meeting of this Network took place in February 2018. This network acts as a peer support group and also informs the wider National Federation membership. Our member organisations are registered charities and have limited resources most of which are placed at the front line.

The National Federation warmly welcomes the opportunity to participate in consultation on the ***Draft Regulatory Strategy for 2021-2026.***

In order to prepare this submission, the National Federation consulted with our Data Protection Network and the following is a collation of views on the Draft Regulatory Strategy 2021-2026. 2

Strategic Goals

1. Regulate consistently and effectively

Proposal

Clarifying the limits of legislation and setting expectations for stakeholders, including how and when corrective measures are imposed.

The Records of Processing Activity (ROPA)(Article 30) – the National Federation would welcome clarity in terms of the level of detail required, organisations are struggling with identifying the level of detail acceptable to the DPC.

Proposal:

Improving guidance to individuals, including vulnerable groups, in an appropriate format, promoting deeper understanding of data protection law and increased control over personal information.

The document later specifies its interpretation of vulnerable groups, which does not appear to include those with an intellectual disability. Guidance (to include easy read formats) to those individuals would be very helpful.

Proposal

More frequent publication of case studies illustrating how data protection law is applied, how non-compliance is identified and how corrective measures are imposed.

This will provide context and set precedence in a fashion similar to the publication of the Office of the Information Commissioner (OIC) issued Freedom of Information (FOI) decisions. We very much welcome this proposal. 3

2. Safeguard individuals and promote data protection awareness

Proposal

Raising public awareness of their data protection rights and how they can control the use of their personal data.

While raising awareness, we would welcome the inclusion of the limits of the Data Protection Act and GDPR e.g. data protection is not a complaints mechanism nor a forum for raising questions**.**

Proposal

Taking account of how data protection impacts vulnerable groups and engaging with advocacy groups to communicate this appropriately.

Although the Assisted Decision Making (Capacity) Act 2015 was signed into law on 30th December 2015, the systems required to implement the legislation have yet to be put in place. The Decision Support Service have stated their intention to be operational by mid-2022.

We would welcome a view from the DPC in relation to the impact of this Act on the DSARs process and any guidance on how to manage the expectations of the data subject as well as individuals acting on their behalf, especially those whose capacity to understand might be in question.

The interpretation of vulnerable groups should be expanded to include people with an intellectual disability.

Proposal

Regularly communicating with organisations on investigation procedures and final outcomes.

Organisations/Data Protection Officers (DPO's) would welcome communications from the Data Protection Commission (DPC) which support them in understanding and implementing the requirements of Data Protection legislation. There is great value and learning in sharing experiences and outcomes. We welcome any guidance on sharing the DPC process and investigative report with the Data Subject.

Proposal

Actively promoting the development of codes of conduct and certifications to enable sectoral best-practice and demonstrable compliance in processing activities.

We welcome codes of conduct and certifications and would be grateful if the DPC would clarify if there will be resource implications for our organisations. Will the DPC 'sanction/validate' appropriate training providers/standards/regulations/qualifications for DPOs? Will the DPC recognise prior experiential learning etc.? 4

3. Prioritise the protection of children and other vulnerable groups

Proposal

Actively promoting the development of codes of conduct on the processing of children's personal data.

We would welcome these codes of conduct in particular relating to establishing a child's capacity in making determinations of their own accord.

Proposal

Engaging and partnering with representative bodies and advocacy groups who act on behalf of vulnerable persons, to get their insight into how best to tailor guidance for their clients.

Varying the means of communication to include audio and illustrative guidance for those who prefer to access information in that way.

These proposals refer to illustrative guidance and the National Federation feel this is incredibly important as in our experience, illustrations are of great assistance to people with an intellectual disability.

Proposal

Clarifying the bases for data sharing, so that individuals are not disadvantaged or at risk as a consequence of over caution on the part of data controllers.

We would welcome examples of when an organisation should not provide data to representatives who claim they act on behalf of vulnerable persons.

We would welcome clarity on when a data controller should not facilitate any requests from a representative or what protocols should be in place to ensure that we protect the integrity, confidentiality and security of vulnerable persons.

We would very much welcome clarity around the sharing of information with our funders and other State agencies – including Data Sharing Agreements (templates would be very useful). 5

4. Bring clarity to stakeholders

Proposal

Maintaining and enhancing the DPC's technological foresight, to ensure it is equipped to regulate effectively into the future, in response to rapidly evolving technologies

We would be particularly interested in guidance on business use of social media platforms and messaging apps (e.g. WhatsApp, Videoconference Platforms, and File Sharing Applications), particularly in the new realities of Remote Working. It would be useful if the DPC identified those platforms that are compliant with Irish Data Protection legislation and those that are not and what measures could be introduced to support compliance in the use of these technologies.

5. Support organisations and drive compliance

Proposal

Actively pursuing codes of conduct and certifications to enable sectoral best-practice and demonstrable compliance in processing activities

We are very eager to engage with the DPC and would welcome clarity on how this will be carried out and what, if any, additional pressures will be placed on resources in order to achieve compliance with these expectations and what processes/funding streams will be put in place to support this objective.

Proposal

Working with DPOs to increase the knowledge and impact of their role

We welcome this proposal and seek clarity on how it will be rolled out, e.g. via workshops/website bulletins/official literature, liaising with established networks, etc. May we suggest a DPO Portal where discussion and advice could be shared?

We would also suggest the establishment of a team that is dedicated to providing guidance and support to data protection officers who may be undertaking this role on a part time basis without a supporting organisational structure.

Proposals

Publishing detailed case studies of our decisions in an accessible format so that controllers have a frame of reference when planning new undertakings.

Prioritising the development of guidance for micro, small and medium sized enterprises. 6

Working with DPOs to increase the knowledge and impact of their role.

We welcome these proposals and would be happy to engage with the DPC in progressing these.

The guidance relating to records retention for the health sector in Ireland has always been conflicting and confusing, for example we are directed to keep some data 'in perpetuity' and yet we are to consider data minimisation and one file one person. This all impacts on our ability to comply in full with Data Protection legislation and we would welcome any engagement between the DPC and the Health Service Executive to clarify data retention issues. 7

Conclusion

The National Federation appreciates the opportunity to comment on this important Draft Regulatory Strategy for 2021-2026. We are fully aware that the most important stakeholder is the data subject and we advocate on behalf of the people we support in various forums and take their rights to privacy very seriously.

In our response to this Draft Regulatory Strategy we are responding from the view of the data controller. We feel it is important to point out that one of the main hurdles for our sector is complying with the myriad of regulatory compliances with limited resources. Therefore any ambiguity in the application of the regulations cause a strain on those resource and we welcome the proposals by the DPC to produce further guidance documentation in relation to compliance. As a sector we hold personal and

sensitive data on the people we support and our employees. We wish to ensure that this data is protected to the best of our abilities and within the legislation.

We would also be grateful for any associated templates and the publication of case studies. We are very willing to engage with the DPC and as a sector wish to work towards full compliant with the regulations.

14. Castlebridge

DPC Regulatory Strategy 2021-2026

Consultation Feedback

Contents[29]

Introduction

Castlebridge welcomes this opportunity to provide comment on the Data Protection Commission's Regulatory Strategy for 2021 to 2026.

The strategic ambitions of the Data Protection Commission are of fundamental importance to a global population far greater than just the population of Ireland. As a nation we are famous for our global diaspora, the emigrants and descendants of emigrants who represent Ireland around the world. However, recent years have given

[29] Please note that the pagination in this table of contents refer to the pages of the original submission and not to this consolidated response report.

rise to a ‘digital diaspora’, those people around the world who are tied to Ireland and our regulatory systems by nothing more than the establishment of a company that is processing their personal data within this jurisdiction. The Data Protection Commission has a key role to play in upholding the rights and freedoms of this global population which requires a strategic ambition that is adequately and appropriately resourced so that it can be realistically achieved.

In other forums we have referred to the challenges of effective regulation for data protection as a “wicked problem”, a problem that is difficult or impossible to solve because of incomplete, contradictory, and changing requirements that are often difficult to recognise. In this context, we see the Commission’s Regulatory Strategy as being just one component of the wider set of solutions that need to be pursued to improve data protection compliance in Ireland and the EU, and the wider set of initiatives that will be required to raise data protection standards globally.

In this context, we would hope that the Irish Government will match the objectives and vision of this Regulatory Strategy with appropriate investment in Data Protection by Design in public policy initiatives, the provision of resources to enable and encourage organisations (in particularly SMEs and Micro-Enterprises) to improve their data protection compliance, and the appropriate resourcing and training of Data Protection functions across the Public Sector.

Format of Response

Our response to the Regulatory Strategy will follow the structure of the Data Protection Commission’s draft document. Castlebridge has endeavoured to provide comment in respect of each section.

Mission, Vision and Values

Mission:

The Mission, as currently framed, does not adequately tie the enforcement role of the Data Protection Commission to the role of “upholding the consistent application of data protection law”. It is our view that this is a weakness of drafting rather than a weakness of intent.

We would suggest an alternative phrasing that better reflects what the Regulatory strategy and statutory role of the Data Protection Commission:

"Promoting compliance with data protection legislation and the protection of fundamental rights through consistent enforcement, robust supervision, and relevant engagement"

This rephrasing of the Mission of the Commission does not preclude or exclude any of the actions identified in this section of the Regulatory Strategy but presents the mission in a more direct manner.

Vision:

Castlebridge has limited comment on the vision as set out by the Commission in this draft Regulatory Strategy.

- We would query the focus on the "early years of the General Data Protection Regulation" when a more ambitious vision could consider the impact of the Commission on GDPR as a whole and the potential for the Commission to contribute to the development of global standards for data protection and regulatory enforcement.
- It is important that the Vision is interpreted and applied in a manner that does not deflect from protection of fundamental rights of individuals, notwithstanding the need to balance the application of resources in a way that achieves the maximum benefit for the greatest number of people. Data Protection rights are *individual rights* and a Regulatory Strategy that loses sight of that in its vision would be inherently flawed.

Values:

Castlebridge has no comment in respect of the Values set out in this Regulatory

Mandate:

Castlebridge has no comment in respect of the Mandate of the Data Protection Commission as set out in the Draft Regulatory Strategy.

However, as the scope of the Commission's role and mandate is often misunderstood by stakeholders it would be important as part of the implementation of this Regulatory Strategy for there to be clear communication as to the scope of the Commission's mandate. This is particularly important in the context of comparisons with other regulators in other jurisdictions whose actions against Data Controllers may be grounded on regulatory mandates that are different to those which apply to the DPC.

Strategic Goals

Castlebridge has examined each of the five high-level strategic goals and we provide comment on each individually below.

Regulate consistently and effectively

The commitment to improved transparency and provision of information about the

Commission's Regulatory functions is welcomed.

It is our view that improved certainty of process and outcome would be a key contributor to improved compliance. The academic research on regulatory change and behaviour change regulatory contexts is clear: behaviours change, and compliance improves when:

1) There is certainty of enforcement action being taken

2) There is procedural fairness in the implementation and execution of sanctions

3) The time lag between the infringement and the penalty is short.

Knowledge management and staff retention within the Commission are correctly identified as contributors to this consistency and effectiveness of regulation. Post-Covid, this will be increasingly the case as organisations adapt to hybrid connected working models. The actions proposed by the DPC in respect of training and other measures are to be welcomed. We would suggest that an action should be added to explicitly address implementation of processes and systems for knowledge management in the Commission to match the commitment on engagement in respect of physical office locations.

Safeguard individuals and promote data protection awareness

It is recognised that the Commission faces a difficult balancing act in respect of the handling of individual complaints against the resource requirements of larger case investigations. In this context it is understandable that "*would prefer instead to prioritise cases that are likely to have the greatest systemic impact for the widest number of people over the longer-term, and to allocate its investigative resources on that basis*."

However, this **must** be done in a manner that does not downgrade the protection of individual rights, the investigation of individual cases, or the enforcement against individual Data Controllers and Processors. Additionally, it must also avoid negatively impacting on the application of fair procedures in the execution of investigations and enforcement action.

In this context, we would suggest that the Commission consider the options that are presented to them arising from the recent *Facebook Ireland Ltd v Data Protection Commission1* in terms of the discretion the Commission has in respect of how it conducts investigations to develop consistent and effective processes for addressing the high volume of cases which relate to individuals with complaints relating to more

straightforward matters to reduce the time taken to engage with, assess, and enforce in these matters.

The enforcement approach of the Spanish Supervisory Authority is one potential reference model. Other potential reference models can be found in other areas of regulatory enforcement such as:

- Road Safety enforcement
- 'Voluntary disclosure' policies in the context of taxation law compliance.

Again, the key determinants of successful change in regulatory enforcement have been shown to be:

1) There is certainty of enforcement action being taken

2) There is procedural fairness in the implementation and execution of sanctions

3) The time lag between the infringement and the penalty is short.

The implementation of the Commission's Regulatory Strategy must address these three factors to improve the safeguarding of individual rights.

Prioritise the protection of children and other vulnerable groups Castlebridge welcomes the explicit attention to the protection of the rights of children and other vulnerable groups in the DPC's Regulatory Strategy.

However, we would comment that the actual protection of these vulnerable groups depends more on the actions of policy makers, public bodies, and private sector organisations in their implementation of policies, procedures, and technologies affecting such groups.

Protection of children and vulnerable groups will only be meaningful if it is matched by timely and effective enforcement when rights are not upheld or where principles such as Data Protection by Design and by Default are not applied.

Castlebridge's view is that the development of Codes of Conduct on a sectoral basis is a valuable contributor to the development of standards of protection in these areas.

However, we would highlight that the current guidance and requirements for approval of Codes of Conduct do not necessarily lend themselves easily to the establishment of Codes in disparate sectors working with vulnerable persons such as Elder care or support services for survivors of sexual abuse where there is no single over-arching governing body.

Bring clarity to stakeholders

The Commission's recognition of the need to ensure clarity for stakeholders is welcomed. This clarity needs to address:

- Transparency of processes and operations
- Transparency and impartiality of complaint handling
- Consistency of decision making

As mentioned elsewhere in this submission, research has consistently shown that effective regulatory sanctions are dependent on three key factors:

1) There is certainty of enforcement action being taken

2) There is procedural fairness in the implementation and execution of sanctions

3) The time lag between the infringement and the penalty is short.

Therefore, the drive towards clarity for stakeholders by the DPC must address these three factors at a minimum.

The effective and proportionate allocation of resources to the handling of complaints must support the delivery against these criteria but must do so in a way that does not deprive individuals as stakeholders of their clarity that complaints raised by them will be addressed and their rights will be upheld.

A key area of clarity for stakeholders that is required is improved consistency of reporting across Supervisory Authorities in terms of execution of enforcement processes or other regulatory functions. This will require a degree of standardisation of terminology (e.g. "complaint" vs "concern") and improved alignment of processes such that an objective assessment of the performance of Supervisory Authorities can be made that compares apples with apples.

In the context of regulatory enforcement, the Commission must ensure sufficient clarity on the procedural aspects of complaint handling that the procedural fairness of investigation and sanctions processes is clear to stakeholders. That must be accompanied by clarity and certainty of proportionate enforcement action through a predictable escalation path that ensures there is no disproportionate delay between the infringement and any enforcement action being taken.

Within GDPR and the LED there are a number of relatively binary procedural concepts (e.g. the requirement to conduct DPIAs in certain circumstances) which could perhaps lend themselves to a "fixed penalty charge" enforcement regime similar to that employed for Road Traffic compliance.

Support organisations and drive compliance

The Regulatory remit of the Data Protection Commission presents an inherent challenge in ensuring that organisations are effectively supported in understanding their compliance obligations and that appropriate incentives are in place to encourage compliance. This encouragement of compliance can and should be through the either the imposition of administrative sanctions (negative incentives / punishment) or through positive incentivisation by way of recognition for good practices or initiatives to develop good practice.

It is welcomed that the DPC has made a clear statement of intent to prosecute, sanction, and fine infractions that result from wilful, negligent, or criminal intent. Castlebridge would suggest that more explicit reference should be made to the potential for personal liability under the Data Protection Act 2018 for directors, officers, or managers of corporate bodies. In saying this however we are equally conscious of the absence of any equivalent sanctions mechanism for public sector staff whose consent, neglect, or connivance result in an offence being committed under the Act.

The pursuance of Codes of Conduct is welcomed as a model for developing sectoral best practice. However, our experience in developing Codes of Conduct has highlighted potential scenarios in respect of the establishment of appropriate governance models which are not yet addressed in the published guidance. For Codes of Conduct to be a robust tool to benefit data subjects, organisations, and the Commission, further engagement will be required to address the different models of governance and oversight that will be required, and to ensure that organisations in the Voluntary sector in particular have sufficient support when seeking to make the case for funding or other supports to ensure the effective implementation of Codes of Conduct.

While Guidance and engagement are correctly recognised by the DPC as a form of ‘soft power’ to support and encourage compliance, it is essential that these tools are seen as complementary to harder models of enforcement rather than as alternatives. For this to be effective, there must be clarity for organisations on the importance and implications of guidance that is issued by the Data Protection Commission and its significance in an enforcement context.

There must be a degree of certainty that non-compliance with guidance will result in some degree of enforcement action. This means that the time-period between the issuing of guidance and the enforcement of that guidance must be appropriate and proportionate to the nature of and complexity of the issues addressed within that guidance. Absent this, irrespective of the quality of guidance that may be issued, there will be no incentive for organisations to adapt processes and practices.

In the context of engagement with Data Controllers and Data Processors, the Commission must ensure that engagement is executed in a manner that does not

prejudge or preclude any enforcement action that may be required. A balance is required between the Commission providing a mechanism for Controllers or Processors to raise questions in respect of proposed processing activities or development of new technologies or to bring matters to the attention of the Commission and the potential perception of such engagements as 'free consultancy'.

Regarding the support of Data Protection Officers this is a critical issue for many organisations. While the Commission's Regulatory Strategy currently addresses the need to engage with DPOs to raise awareness of the knowledge and impact of their role, it is equally important that the Commission take action to ensure that the role of the Data Protection Officer is being resourced adequately and given the appropriate status within organisations. Key issues of concern include:

- Data Protection Officers holding conflicted roles in organisations (e.g. CEO or Head of Marketing as DPO)
- Organisations appointing DPOs to positions without due consideration to the requirements of Article 37 of GDPR (and its equivalent provision in the Law Enforcement Directive and Section 88 of the Data Protection Act 2018).
- Ensuring organisations recognise the need for ongoing investment in skills, competencies, and resources for Data Protection Officers.

Gaps In Strategy

It is an unenviable task for a Regulator such as the Data Protection Commission to craft a Regulatory Strategy that will inevitably be criticised by various stakeholders. Such criticisms may be justified or unjustified, but they are inevitable. This is particularly true in a rapidly evolving area of policy and regulation such as Data Protection. This is the textbook definition of a "wicked problem" from a policy and governance perspective. Castlebridge notes that throughout the Regulatory Strategy document there are references to engagement with Civil Society organisations and other stakeholders.

While this is in the context of the implementation of this Regulatory Strategy, we would hope that the Commission would also consider feedback on the overall Strategy during the five-year period it will cover and that a core value of Continuous Improvement will be implemented to ensure that the Strategy remains relevant and is effective.

Equally, however, Castlebridge would hope that Civil Society organisations and other stakeholders would engage constructively with the Commission to support the implementation of their Strategy.

We also recognised that the effective implementation of this strategy will require the Government to provide necessary resources. This is particularly true in respect of the evolution of the strategy in the face of a changing environment. The Data Protection

Commission must be able to adapt with a degree of agility to changing circumstances, albeit within parameters that ensure procedural certainty and regulatory clarity.

Conclusion

Strategy documents such as this are often high on aspiration and falter in implementation.

It is essential that the Data Protection Commission's Regulatory Strategy delivers clear and tangible results in a timely manner. While it is incorrect to focus on fines alone as a benchmark for regulatory effectiveness, it is essential that the Data Protection Commission is seen as a fair, effective, and relevant Regulator on the global stage.

Castlebridge has previously provided a written submission to the Oireachtas Justice Committee on the challenges facing the Data Protection Commission. We include a copy of that for consideration as part of this submission.

15. The Association of Data Protection Officers

The Association of Data Protection Officers welcomes the Data Protection Commission's draft regulatory strategy document. It provides very helpful clarity as to the Commission's planned implementation and enforcement of the GDPR and other data protection laws. Meeting the Commission's invitation for submissions we make the following observations, based on combined feedback from our members:

1. Technology Strategy: The DPC might give thought to the development of a separate technology strategy that would provide guidance to organisations about how to address data protection risks arising from technology, as well as how data protection compliance might be compatible with sustainable innovation and drive a responsible digital economy. Specific technology priorities could be set in areas such as cyber-security, A.I., big data, machine learning, and web and cross-device tracking.

2. Digital Strategy: As part of its efforts to communicate with all relevant stakeholders, the strategy might benefit from the inclusion of a digital strategy. This could detail the DPC's approach to utilising its website and other digital media to convey updates, and to reinforce key messages. The sustained use of digital media may also assist the DPC in its goal to raise data protection awareness amongst minors, many of whom use digital media as their primary source of information.

3. Balancing the regulation of international technology companies with the regulation of domestic Irish companies: Given the almost unique supervisory brief of the DPC, covering, as it does, numerous large international technology companies such as Facebook and Google, as well as the full range of domestic Irish, private and public sector data controllers, it would be very important for the DPC to outline how it plans to manage these somewhat divergent responsibilities and, specifically, how this workload might affect its prioritisation of time and resources over the span of this regulatory strategy.

4. Extending Outreach Activities: With the respect to the strategy's communication goals, although, a DPO network has been created by the DPC, consideration should also be given to the very large numbers of people who work in data protection, but do not have the DPO designation. This constitutes a very significant proportion of data protection professionals who work under titles such as 'Head of Data Privacy, 'Privacy Officer' etc. Might the strategy clarify that this cohort of data protection professionals is deserving of special note when it comes to developing communications and networks plans.

5. Investment in Technology Teams: Given the pace of technological change, and the significant technical expertise that large technology companies can bring to bear during

investigations and inspections, it would be beneficial for the strategy document to outline what plans the DPC might have as regards expanding/modifying its own technology teams, and whether or not it is envisaged that these teams would need to grow to match the evolution of the industry.

6. More Interaction with professional bodies: Increased, formal interaction with data protection professional bodies, including the Association of Data Protection Officers, such as through annual roundtable meetings, would be an important part of communicating the DPC's message effectively, and of receiving on-going feedback on the success of its regulatory strategy. These professional bodies can, in turn, reinforce the DPC's message through interaction with their own membership bases.

7. Targeted Complaints Handling: With reference to Section 4 of the DPC Regulatory Strategy, with regard to complaints, the Association of Data Protection Officers agrees that it would be more beneficial to focus on systemic cases that disclose issues of fundamental importance, rather than running multiple parallel investigations into similar complaints. A risk-based, collective approach should, ultimately, lead to a greater vindication of data subjects' fundamental rights and freedoms.

Nevertheless, supervisory authorities are obliged to handle all complaints lodged by data subjects, investigate the complaints to the extent appropriate, and inform each complainant of the progress and the outcome of investigations within a reasonable period. In the interest of complainant data subjects, and controllers or processors subject to complaints, the strategy should indicate to both parties clear standards the DPC will apply in its determination of the appropriate extent of complaint investigations and, in particular, what the DPC considers to be a reasonable period of time for reaching investigation outcomes.

8. International Data Transfers: The strategy only mentions international transfers once, namely, at Section 1, where it states: 'The DPC proposes to work closely with the European Data Protection Board to develop legal certainty for international transfers of personal data.' Considering the significant of this topic and the impact that it is having on all data controllers, greater detail on the DPC's plans in this area would be very welcome. In particular, whether or not up-to-date guidance is anticipated would be important given the uncertainty in this area. Additionally, an outline of the DPC's international strategy would be a helpful guide.

9. BREXIT: Considering that the future of the data protection relationship between the EU and the UK remains in doubt, the uncertainty that the recently adopted GDPR & LED adequacy decisions will endure in the medium to long term, given that there is a substantial dependency in Ireland upon the UK economy, and in particular the need for

avoidance if at all possible of a “hard border” of personal data transfers within the island of Ireland, detail on the DPC’s ongoing contingency plans would be welcome.

10. Investigations/Inspections: The strategy does not clarify what broad approach the DPC will take to inspections and investigations. For instance, in the assignment of resources, will themed, cross-industry inspections continue to form a part of the DPC’s activities?

11. Approach to Small-and-Medium-Sized Enterprises (SMEs): The SME sector, both in the e-commerce and traditional commercial space, continues to struggle with implementation, and awareness, of the GDPR and the ePrivacy regulation. Specific focus on that sector would be timely, taking into account the relative lack of knowledge, technological sophistication and limited resources of such businesses. In particular, tailored guidance and tools would be highly beneficial for this sector.

About the Association of Data Protection Officers

The Association of Data Protection Officers (ADPO), founded in February 2012, is the Irish membership organisation for those who are working professionally in data protection, including but not limited to Data Protection Officers. The Association offers its members an opportunity to share ideas, voice concerns, seek clarity on new legislation, and offer their own insights on the demands and challenges of the job.

ADPO’s objectives are to provide relevant training, certification and professional development to its members, provide clarity on data protection issues, raise awareness of the legislation and to offer its members a forum for discussion of such topics. Membership numbers currently stand at ca. 2,200. ADPO is affiliated to the Confederation of European Data Protection Organisations (www.cedpo.eu).

16. Insurance Ireland

INTRODUCTION

Ireland is a thriving global hub for insurance, captives & reinsurance and Insurtech. Ireland's insurance market is the fifth largest in the EU, and our Reinsurance market is the second largest. Our members represent around 95% of the companies operating in the Irish market, making Insurance Ireland a strong leadership voice for the sector. Insurance Ireland members are progressive, innovative and inclusive, providing competitive and sustainable products and services to customers and businesses across the Life and Pensions, General, Health, Reinsurance and Captive sectors in Ireland and across the globe.

In Ireland, our members pay more than €13bn in claims annually and safeguard the financial future of customers through €112.3bn of life and pensions savings. Our members contribute €1.6bn annually to the Irish Exchequer and the sector employs 28,000 people in high skilled careers.

The role of Insurance Ireland is to advocate on behalf of our members with policymakers and regulators in Ireland, Europe and Internationally; to promote the value that our members create for individuals, the economy and society; and to help customers understand insurance products and services so that they can make informed choices.

Insurance Ireland advocates for 135 member firms serving 25m customers in Ireland and globally across 110 countries (incl. 24 EU Member States), delivering peace of mind to individuals, households, and businesses, and providing a firm foundation to the economic life of the country.

OVERALL OBSERVATIONS

Insurance Ireland welcomes the opportunity to respond to the proposed regulatory strategy as set out in the Data Protection Commission (DPC) consultation. We believe the next five years will be an important period in the evolution of data protection practices and regulation as data protection is a fast evolving and advancing area of law, which will need to take account of rapid innovation and technological change.

The insurance industry particularly welcomes the commitment of the DPC to engage with stakeholders in clarifying the limits of the legislation and setting expectations. This type of engagement with industry, to share insights, promote understanding, and debate and clarify interpretation of the law, is to be welcomed, as these engagements will supplement our members in their efforts to comply and apply best practice to DP

requirements. This engagement is essential for insurance firms to understand the DPC's approach to the supervision of appropriate data protection policies, procedures and systems. It is also important to help consumers to understand the limits around insurance firms' ability to process certain types of data and the legal basis upon which certain types of information is requested. As a trade body representing 95% of the insurance market in Ireland, we value our engagement with the DPC and look forward to continuing this to support the industry's DP compliance and fair outcomes for our consumers.

We also welcome the proposals to provide more frequent publication of case studies illustrating how DP laws are applied and what constitutes non-compliance. Highlighting the trends in complaints vis-à-vis enforcement action, sectoral awareness, thematic reviews and other publications could be considered to provide clarity where necessary. Readily available, industry level feedback on systemic concerns and issues identified by the DPC would help the industry to consider the root cause of the issues.

We agree that the DPC should focus its resources on systemic issues. It is important that data supervision works for the majority of consumers. Significant change to the DPC approach or legislation underpinning the DPC objectives should be driven only by issues where there is evidence of systemic harm. Given the pace of technological change there is a need to increase certainty and stability in how data protection law is applied.

We have concerns that, in some instances, the DPC can take a holistic approach in its feedback to the insurance industry and does not take account of the specific nature of the industry in the collection and retention of data. There is a material difference in the nature of products provided by insurers when compared to other industries such as Telecoms and Utilities.

The insurance industry is bound by regulatory rules under the Criminal Justice Act (CJA), the Central Bank of Ireland (CBI) and the Consumer Protection Code (CPC) as well as the requirement to appropriately price insurable risk. While we understand that both regulators are in dialogue, in practice our members have reported challenges to the data processes and procedures that are required to meet CBI rules and have been accepted by the CBI as being necessary to meet regulatory obligations. We suggest that a more formal Memorandum of Understanding (MoU) should be in place for the CBI and the DPC to support the insurance industry in complying with each separate regulatory requirement.

Ends

17. AIB

AIB welcomes the opportunity to respond to the Data Protection Commission's (DPC's) Regulatory Strategy Consultation.

The bank is very supportive of the DPC's stated aim of *doing more, for more,* and seeks clarity on the stated goals, as follows:

DPC Goal	**AIB comment**
Regulate consistently and effectively	**Regulatory environment** There are different lenses to a complaint depending on the regulator, e.g. DPC, FSPO, CBI and other regulators outside of Ireland. AIB note that better customer outcomes could be delivered through integrated guidance across impacted regulators and from guidance on how complaints should be managed with the DPC and other regulators. Guidance on the time granted to respond to a complaint by the DPC would be beneficial and support planning and resourcing. **EU case law** Case law decisions across the EU can have an impact on how organisations propose to manage their data and interactions with customers and regulators. Guidance on emerging case law across the EU, where relevant, would be helpful to Data Controllers. **Improving Guidance** Guidance on whether the DPC intends to align to an existing standard, e.g. the Crystal Mark as part of improving guidance to individuals, would be useful.
Safeguard individuals and promote data	**Codes of Conduct and Certification**

protection awareness	AIB intends to apply for GDPR certification as and when it becomes available, via the Irish scheme and/or EU wide scheme or “seal”. In advance of the publication of these schemes, information on whether the DPC will work with any professional services bodies (e.g. the Institute of Bankers, the Association of Compliance Officers Ireland) to develop codes of conduct would support certification preparations. Further to the guidance note published by the DPC on GPDR Certification in September 2020, has the submission process for the formal approval of GDPR certification criteria been developed and will this be published?
Prioritise the protection of children and other vulnerable groups	**Vulnerability and interaction with other legislation** Financial Sector firms have existing obligations to vulnerable customers, including children, as defined in legislation including the Consumer Protection Code and the Assisted Decision Making (Capacity) Act. Clarity on how the DPC envisages interacting with this and other existing obligations and regulations would be helpful. **Interaction with other public institutions** When considering vulnerability, is the DPC engaging with stakeholders, including the Decision Support Service and the BPFI, on the Assisted Decision Making (Capacity) Act (ADMA) and supporting Codes, including the assessment of capacity of vulnerable customers?
Support organisations and drive compliance	**Evolving sector** There is overlap between data protection regulation and other data regulation, including regulation governing information security and digitalisation. Will the DPC be advising on data protection considerations with other regulations (e.g. NIS Directive, the Digital Services Act) and regulators?

DPC engagement with other Supervisory Authorities

Where the DPC does communicate with other EDPB supervisory authorities, how does the DPC plan to communicate the outputs and findings back to firms which it regulates? Where the DPC intends to publish detailed case studies of decisions, will this also include case studies across the EU and from the EDPB?

Culture

AIB has a stated commitment to sustainability including data protection and would like to ensure that this commitment aligns to the DPC goal of promoting a cultural shift towards compliance. Can the DPC advise if guidance will be issued on promoting this cultural shift, and what supports might the DPC provide to firms to proactively promote compliance?

DPC Breaches

The existing process for recording breaches on the DPC website is quite manual. Will the DPC strategy give consideration to enhancement of the DPC Breach process to improve the time required to report a breach and reducing the risk of manual error when reporting a breach? Guidance from the DPC on different levels of breaches (i.e. Low, Medium, High), including through the use of an established Risk Methodology for grading breaches, would be helpful for data controllers.

Guidance and Support

AIB recognise and fully support the guidance for SMEs. AIB also note that Corporates can hold higher volumes of customer data with a greater scale of processing. Data Controllers from Corporates would benefit from a dedicated contact or team with whom they could proactively engage.

18. Sage Advocacy

Introduction

Sage Advocacy is a support and advocacy service for vulnerable adults, older people and healthcare patients. Every year we receive a large number of referrals for advocacy and requests for information and support issues.

Through our advocacy case work, Sage Advocacy is very aware of issues regarding the use, collection and sharing of data and our observations are driven by our experience.

Similarly, in the exercise of our functions, Sage Advocacy has encountered situations in which relatives of clients have tried to seek access to data belonging to their relative, and/or data submitted by family members related to the client.

Overview of Strategic Goals

The Commission lists 5 Strategic Goals;

1. Regulate consistently and effectively,

2. Safeguard Individuals and promote data protection awareness,

3. Prioritise the protection of children and other vulnerable groups,

4. Bring clarity to stakeholders,

5. Support organisations and drive compliance.

Sage Advocacy has provided feedback under two goals, specifically

a) Safeguard Individuals and promote data protection awareness, and,

b) Prioritise the protection of children and other vulnerable groups

Safeguard Individuals and promote data protection awareness

Generally, there is a need to raise data protection awareness, particularly among adults who are at risk of abuse, families and professionals who may be working with older people or people with disabilities.

This will include a variety of approaches and methods to deliver information to support such as easy to read and Plain English.

Through our advocacy work, Sage Advocacy has identified that that there is considerable uncertainty and lack of clarity among individual professionals and within statutory, voluntary and business organisations on what, if any, information can be shared between individuals and organisations where there are concerns of abuse, neglect and/ or exploitation of a vulnerable adult. This lack of clarity is, by itself, creating and amplifying risk.

In many instances, the sharing of information can be vital in helping to prevent or stop abuse of a vulnerable adult. Lack of clarity arises particularly in cases where a) The vulnerable adult lacks capacity to give consent for sharing of information. b) There is a need to share concerns/ information between agencies in order to prevent/ stop abuse.

Most recently, through our case work Sage Advocacy has become aware of specific concerns relating to sex-offenders and nursing homes. The issues related to a lack guidance around the sharing of relevant (high risk) information between an Garda Siochána and private nursing homes providers and the lack of guidance around an Garda Siochána's duty to notify nursing homes providers of known sex offenders in the community who become residents of nursing homes.

While there are clear reporting guidelines in place regarding reporting sexual abuse when it allegedly occurs in a care setting to HIQA, HSE Safeguarding Vulnerable Adults Teams and an Garda Siochána, there are no similar guidelines regarding the sharing of information when;

- An alleged offender is moving from the community to a nursing home setting,
- An alleged offender is moving between care settings,
- An alleged offender is moving from a nursing home setting to an acute hospital setting.

In practice, this lack of clarity and absence of guidelines relating to relevant information has resulted in serious matters giving rise to safeguarding concerns and the potential and alleged abuse of vulnerable adults.

In this context, it is welcome that the DPC has included an action to take account of "how data protection impacts vulnerable groups and engaging with advocacy groups to communicate this appropriately" and that it is proposed that codes of practice will be developed in this regard.

The experience of Sage Advocacy is that the sharing of personal data may be appropriate where it is in the public interest to do so and where the safeguarding of vulnerable adults is at hand. Section 60 of the 2018 Act provides that the rights of controllers and data subjects may be restricted in the 'public interest' but needs regulations to provide for this.

It is important that the DPC include a specific action relating to data sharing in this section.

Additionally, Sage Advocacy is aware of circumstances where data sharing in relation to previously convicted sex offenders has resulted in a person being unable to find appropriate accommodation or having their movement restricted.

A data sharing protocol to protect a person's right to liberty and freedom of movement is required as well as protecting the rights of others.

Prioritise the protection of children and other vulnerable groups

In our submission to the Data Protection Commission (DPC) in February 2020 we noted that the outcomes stated that "children are specifically protected" and that there was no mention of vulnerable adults. Therefore, it is welcome that the protection of children and other vulnerable groups is included.

In our submission of February 2020, we suggested that a separate section specifically focusing on vulnerable adults could be included and that linking children and vulnerable adults suggested that both issues are similar and this is not the case. Sage Advocacy remains concerned that there is a strategic goal included in this strategy that conflates children and vulnerable adults.

We suggest that distinct goals are set for both groups, however at a minimum that the goal would be renamed "prioritise the protection of those who may be vulnerable" and to include children, older people and people with disabilities etc. within the "desired outcome" definition.

With regard to the specific actions involved, Sage Advocacy welcomes the commitment to developing and promoting codes of conduct on the processing of the personal data of vulnerable adults. Sage Advocacy had called for this to be included in our earlier submission.

We also welcome the commitment to consult with stakeholder agencies as we believe that it is by using the experiences of independent support and advocacy services, such as Sage Advocacy, in developing guidance for individuals and organisations based on the experience of practitioners on the ground that robust and practical codes of practice will be developed.

Actions relating to “conducting detailed research on how data protection law applies to children” and “defining the specific protections required to safeguard the rights of children in the protection of their personal data” are very important and specific provision on both of these matters should also be provided for vulnerable adults. Vulnerable adults include not only those whose decision-making capacity is in question but also those who may be at risk due to, for example, mental health difficulties.

Although it is welcome that there is a statement that “obtaining information is not impeded by language, capacity, financial or other barriers”, it is disappointing that there is no mention of the Assisted Decision-Making (Capacity) Act, 2015 and the need to link data sharing decisions with decision-making capacity and in assessing data protection concerns. Agencies and organisation should address issues of consent in relation to vulnerable adults.

In many instances, the sharing of information can be vital in helping to prevent or stop abuse of a vulnerable adult. Lack of clarity arises particularly in cases where an individual lacks capacity to give consent for sharing of information or, as is mentioned earlier, there is a need to share concerns/ information between agencies in order to prevent/stop abuse.

Conclusion

Sage Advocacy believes that there are some very welcome provisions included in this strategy and welcome the opportunity to make a submission.

It is critically important that clear communication on data protection to all of those who may benefit or be protected takes place, including clarity on when data may be shared in the public interest.

Additionally, the protection of vulnerable adults is welcome, however care must be taken not to conflate children and adults in relation to safeguarding.

Finally, Sage Advocacy welcomes the inclusion of a commitment to consult with stakeholder agencies and look forward to future engagement with the Commission.

19. Government DPOs (Informal Network)

I refer to the invitation by the Data Protection Commission (DPC) for submissions on its draft Regulatory Strategy for the period 2021-2026 as part of an open public consultation process.

We are an informal network of Data Protection Officers who represent the 18 current Government Departments (*listed below).

This DPO network welcomes the strategy and is broadly supportive of the DPC in this regard. We wish to make some comments and observations (both general and specific) in relation to the draft Regulatory Strategy as follows:

Stakeholders and the Data Protection Officer Role

The strategy document regularly refers to 'stakeholders' but does not specify who they are. While stakeholders may be called out in other DPC publications, it would be useful to have an indicative listing included here. In this regard we submit that, as the Data Protection Officer is one of the very few roles specified in data protection legislation, the DPO should be listed as a stakeholder and the strategy should commit to developing specific supports and guidance for DPOs.

In addition, as the DPC acknowledges the criticality of the role[30], we are of the view that the DPC should explore how the role might be 'professionalised' to ensure that organisations can be confident of recruiting/developing competent[31] DPOs. We further submit that, as the strategy seeks to develop a culture of data protection across society, a commitment to consultation and communication with the DPO networks across the public and private sector should be included as an action item. Utilising such networks will greatly increase the DPC's reach in seeking to 'spread the word'.

The following are our observations on the narrative surrounding certain of the DPC's strategic goals:

[30] Current DPC Guidance on appropriate DPO qualifications https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-officrs/guidance-appropriate-qualifications

[31] We note that the Safety Health and Welfare at Work Act 2005 establishes the fundamental cores of competency as "training, experience and knowledge" taking account, as appropriate, of the Qualifications (Education and Training) Act 1999. https://www.hsa.ie/eng/Publications_and_Forms/Publications/Safety_and_Health_Management/Guide_to_SHWWA_2005.pdf

1. Regulate consistently and effectively

a. In relation to this statement "*The DPC is of the belief that compliance in general will be greatly improved when stakeholders are clear in their understanding of how the law is enforced"*

We believe that it is important that stakeholders have an understanding of the various lawful bases for organisations to collect and manage their data. In particular, greater understanding is needed in relation to data subjects' interaction with public bodies and that legislation (as opposed to 'consent') allows for the processing of their data in order to provide services.

b. We recommend also that legal interpretation/guidance handed down by DPC should include 'plain English' explanations to ensure that individuals with a non-legal background can understand and follow the guidance provided.

c. Procedures for complaint handling and inquiries

We welcome the DPC's proposal for standardising and publishing the procedures for complaint handling and inquiries. Mindful that Government Departments regularly receive Data Subject Access Requests (D/SARs) from individuals seeking access to their personal data; there are occasions where the data subject might wish to follow up on a D/SAR response by contacting the DPC directly. It is important that these individuals have confidence in the process and are clear about how their complaints/follow-up queries will be handled and how their expectations are addressed.

2. Safeguard Individuals and promote data protection awareness

a. Allocation of resources

We understand and accept the DPC's desire to rebalance the way it approaches individual complaints to ensure that its resources are being used in the most efficient way possible. We note that the DPC's new strategy is to prioritise cases that are likely to have the greatest systemic impact for the widest number of people over the longer-term, and the proposal to allocate its investigative resources on that basis.

We consider that this new strategy needs to be balanced with increased communication of information, guidance and support for individuals in order to promote deeper understanding by them of their rights and entitlements (including the scope of the

legislation) under data protection law and how to better control and manage their personal data.

b. Increasing awareness

We suggest that scenario type examples should be considered for increasing awareness of data protection at a practical level. We are also of the view that on occasion, media headlines and social media discussions can distort data subjects' understanding of data protection requirements. We suggest that the DPC should consider active oversight of public discussion and establish a 'myth buster' type of approach (short focussed communication & website messages) to counter misinformation. Scenario type examples should be considered for increasing awareness at a practical level.

Of particular concern in relation to awareness is the use of cookies on websites and the individual's understanding of the 'pop up' cookie message – 'Accept or Manage Preferences' – A national campaign to enhance awareness of the implications for the individual's data of clicking '*accept all*' is recommended.

3. Prioritise the protection of children and other vulnerable groups

No comments on this Section

4. Bring clarity to stakeholders

We consider that it would be useful to have additional information made available on the DPC's website in relation to the practical application of the law.

We are of the view that the paragraph on page 17 "*Recognising that most businesses and organisations are keen to meet their obligations under the GDPR - but sometimes lack clarity about how those obligations are best operationalised - the DPC will support data controllers in their compliance efforts, so that current and future undertakings have clear guidance on incorporating data protection in their business practices. Increased and informed compliance will have the effect of mitigating potential harms to individuals before they occur, which accords with the DPC's mandate to safeguard individuals' rights*." would fit more comfortably under **Strategic Goal 5** - **Support Organisations and Drive Compliance.** The Desired Outcome S.G. 5 is "*Businesses and organisations of all sizes are informed and accountable for their data processing activities and there is clarity and consistency regarding sanction and enforcement actions."*

5. Support organisations and drive compliance

We are of the view that the emphasis here currently is more on enforcement and sanction rather than support. It is important to emphasise the positive role that the DPC

has as a regulator in providing advice and support to organisations who are trying to improve processes for their customers while safeguarding their personal data. This often involves grappling with new and changing technologies. Findings or feedback from case studies would be helpful in assisting data controllers to determine the best course of action on queries that might arise.

See also our comments in relation to S.G. 4 above

These comments are submitted on behalf of the DPOs of the current Government Departments:

1. Department of Agriculture, Food and the Marine
2. Department of Children, Equality, Disability, Integration and Youth
3. Department of Defence
4. Department of Education
5. Department of Enterprise, Trade and Employment
6. Department of Environment, Climate and Communications
7. Department of Finance
8. Department of Foreign Affairs
9. Department of Further and Higher Education, Research, Innovation and Science
10. Department of Health
11. Department of Housing, Local Government and Heritage
12. Department of Justice
13. Department of Public Expenditure and Reform
14. Department of Rural and Community Development
15. Department of Social Protection
16. Department of the Taoiseach
17. Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media
18. Department of Transport

20. Fergal McHugh, Digital Strategist

The release of the DPC's proposed 5-year strategy and associated public consultation is a welcome event. The DPC's strategy is clear, succinct, ambitious, and largely headed in the right direction. Nevertheless, I have concerns about the DPC's proposal to achieve a balance between the requirements of handling individual complaints and the need to make progress with respect to "systemic" challenges.

The strategy distinguishes between a situation where the DPC is: "*[r]unning multiple parallel investigations [which are] costly in terms of time and resources and [do not] deliver improvements for individuals beyond those to whom the particular case relate"* (p.16), and a regulatory approach with a goal to, "*ensure that DPC resources are allocated appropriately and proportionately, such that systemic issues or issues having a significant impact on fundamental rights and freedoms are addressed in a timely manner and not caught in a build-up of cases"*(p.16). The first excerpt is a description of where the DPC currently are, the second where they wish to be.

The goal is sensible. The DPC *should* deploy its resources in a way which maximizes its impact. Nevertheless, there is a relationship between the individual complaints and the wider systemic issues the DPC needs to tackle. As such the DPC acknowledge the need for complaint aggregation and analysis. For example, as part of the effort to move from lowimpact, non-systemic case management to high-impact, systemic case management the DPC proposes to: *"[identify] trends and themes within individual complaints so that [they] can achieve strong collective outcomes*" (p.11). Admittedly this is one of several proposals for action, but it is a crucial one. This approach is likely to be at its most effective if the complaint volume is sufficiently representative of the systemic issues. The DPC certainly have volume. The strategy notes that "*In the two years between May 2018 and May 2020, the DPC received in excess of 80,000 contacts to its office, on foot of which it opened 15,025 cases on behalf of individuals*" (p11).

But on the other hand the DPC reports that "*vast majority of these cases were narrow in scope, involving just one individual and centred on issues that have no major or lasting impact on the rights and freedoms of the individual*"(p.11). If we take these statements at face value it is difficult to determine a) how analysis of individual complaints will point the DPC in the direction of the desired systemic issues, and b) what other means are at the disposal of the DPC to identify systemic issues?

Let's to put aside the concern at (a) for a moment and address the question at (b). I will return to (a) at a later stage. I agree — from personal and professional experience — that there are indeed systemic issues with respect to data protection. These issues are systemic because they are structural. They belong to how our institutions, our

businesses, our universities, schools are organised. They are embedded, often difficult to identify, and have the potential to impact behaviour and decision-making without the relevant actors necessarily being aware of them. A good example of a structural issue is one which the DPC describes from their stakeholder consultation.

Stakeholders felt that organisations were more intent on indemnifying themselves against future action, as opposed to processing information in accordance with transparent and legitimate standards(p.17)*.*

There is strong evidence that the stakeholders are correct. One way of considering this issue is part of what social scientist sometimes call a “solutionist paradigm”. Organisations often see data protection as a problem to be solved, or a barrier to effective business operation, something to be managed rather than as an opportunity to interact with data subjects in a manner which appropriately responds to the salience and importance of their data rights.

The strategy rightly identifies building awareness, understanding of data protection rights across both organisations and individuals as an important activity. It proposes the inauguration of a culture of “default” compliance as a pillar of their strategic approach.

“Solutionism” is a structural systemic issue mandating a structural response. Broad, sustained behavioural change is indeed the goal here. Nevertheless, it is important to acknowledge the depth and tenacity of systemic issues. Attempting to induce change at this scale and depth is a significant, multi-facetted challenge.

Solutionism is a broad and rather abstract phenomenon, albeit with important realworld effects. It is often difficult to address structural problems without something concrete.

Our understanding of and responses to systemic problems can be enhanced by research and analysis, academic studies etc. And in some, though often limited cases, key areas of address can be identified, and a course of action defined. Nevertheless, scholarship relating to systemic issues often carries its own assumptions, assumptions which can blind decision makers to what is happening on the ground. Advocacy groups are also important, but it remains likely that individual complaints will remain an important guide to where the systemic issues lie.

As noted above the DPC intend to search for patterns across individual complaints to identify candidates for response which offer the most impact. There appears to be a contradiction here. The DPC have noted that historically individual complaints do not do a good job at predicting where the high-impact issues are. The strategy notes a reason for this: individuals are often not sufficiently aware of what is and what is not an infringement of their rights and this impacts on complaint relevance and quality.

Nevertheless, the DPC has a remedy in mind. Stakeholders of all kinds, from individuals to organisations, need to acquire a better understanding of their rights, and make the right kinds of behavioural changes as part of a wider cultural response. It seems that if this is successful then the DPC should see both a decrease in the quantity of complaints and increase in the likelihood of any individual complaint indicating a systemic issue. As such this approach delivers a bonus: a reduction in volume, an increase in quality! A concern remains. At what point do we achieve significant penetration with respect to the knowledge and understanding of individuals to create an appropriate complaint pool? It seems to us that the transition cannot be immediate. That is not of itself a problem. The DPC already has a strong sense of systemic issues that can be reasonably pursed in the meantime. But how quickly can the DPC shift resources and attention from underperforming individual complaints to the systemic issues? That is a different question, and the strategy offers no clear answer here.

This brings me to a more fundamental concern. It is unfortunate that the DPC appears to have been forced into making a choice between acting on individual complaints and acting on systemic issues. This is presented in terms of a broader question concerning how to put the "finite resources" of the DPC to work with greatest potential for impact. Of course, all organisations have finite resources at their disposal; the aim of any organisational strategy is to put those resources to work to maximum advantage. But we also need to ask if those resources are sufficient. Sufficient for what? Sufficient, for example, to prevent a situation where the DPC must choose between being able to follow up (thoroughly and efficiently) on individual complaints with and addressing the systemic issues as currently acknowledged and understood. What is perhaps more concerning is the bar for sufficient resourcing here is likely to increase. The strategy acknowledges we are in the midst of significant foment and change: "*very early years of radically reformed data protection legislation*" (p.3). I acknowledge the very real cost associated with the volume and legitimacy of complaints produced within this kind of social, legislative, and indeed economic setting. But surely it is a cost worth bearing? What is at issue here? As the DPC acknowledges its mandate extends to an protecting an individual's "*right to have one's personal data protected as a fundamental human right*"(p.10). When dealing with fundamental human rights at a time of flux, it seems that more rather than less vigilance is required.

The DPC argues that as regulatory body with a risk-reduction mandate (it notes that the GDPR is "risk-based" regulation) it is appropriate that it takes a risk-based approach to the balancing of its investment in handling individual versus systemic cases. This seems sensible enough, but there may well be a slippery slope here. Yes, the DPC has a role in reducing the systemic risk that data subjects' rights will be violated. Yes, they need to intervene in a that system using the tools at their disposal, in judicious, strategic manner. But conceptualising the issue as being about risk conceals something

important about the DPC's framing of their choice. Is this approach being drive by "finite" resources or insufficient resources? My view tends toward the latter. And over time risk-mitigation strategies of this kind may well actually increase rather than reduce levels of systemic risk.

It seems to me that this issue of finite/sufficient resources has presented the DPC with a philosophical dilemma of sorts. The proposed broad-based utilitarian risk-based approach to individual cases sits uncomfortably with the picture of the individual as imbued with inherent, inalienable rights. For better or worse the philosophical underpinnings of the GDPR are profoundly dignitarian. This may be an inconvenient fact, nevertheless its inconvenience does not alleviate the challenge it poses for the DPC's future steps.

I believe that the DPC finds itself in a difficult situation which is not, largely, of its own making. I noted above the problem of solutionism. Solutionism with respect to data protection (and privacy more broadly) is a genuine feature of the social, economic, and political status quo in Ireland. The current government exemplifies the way in which solutionism can structure the range of possible responses. Of course, they want to see their citizens data rights respected, but only insofar as it does not get in the way of business. The strategy details the DPC's commitment to: "*engage iteratively with the Government regarding the expanding resources necessary to ensure the operational effectiveness of the DPC, now and into the future*" (p.8). I wonder how successful this is likely to be. It is clear given the current funding and support given by the government to the DPC that data protection is not a sufficiently high priority for the current administration. Unfortunately, the outlook and approach of the current administration is one of the systemic barriers to a "default" culture of effective data protection, not least since is currently failing its duty to appropriately fund the DPC.

It is worth noting that one can reject my entire characterisation of the DPC's dilemma without prejudicing the idea that the DPC needs to be better funded. The task of identifying and sorting complaints which "disclose no significant impact" requires analysis, which is in many cases is likely to be more than perfunctory. Even the task of *relegating* such complaints (and doing the bare minimum) can come with an administrative cost which can often be surprising in the aggregate. There is also the question of the wider systems improvements required to genuinely free up resources if this approach is taken.

Of course, I have a stronger view. The DPC should be enlarged to manage both its current and anticipated caseload (which is likely to increase as new and more complex legislation is introduced) without impacting its ability to conduct investigations, campaigns, and other relevant activities to counter systemic issues and to promote the required cultural/behavioural change. A choice between individual and the "greater

good" is not a choice that a regulatory body with the DPC's mandate should have to make. Not least because complaints made by individuals will remain a crucial (if admittedly high cost) guide to where systemic issues might be present. The instrumental value of individual complaints lies in the aggregate, and so without the tools and systems and skills to collect, collate such complaints their ability to indicate wider trends will be limited.

But as I have suggested above the issue goes a great deal deeper than this. In this time of radical change, in the face of systematic abuses of what is not just widely acknowledged as a fundamental human right but legally enshrined as such it seems more necessary than ever to grant every individual a voice an opportunity for a response as full and as proportional as our democracy allows. The DPC strategy reflects a stark reality: the body has been placed in the impossible position of making a choice between two facets of its mandate. It should not have been placed in this position. The DPC should be given the opportunity to craft not just a minimum viable strategy, but instead a maximal strategy.

21. CIPL (Centre for Information Policy Leadership)

CIPL welcomes the Consultation on the Regulatory Strategy for 2021-2026 (the Strategy). We appreciate the thoughtful and thorough approach the Data Protection Commissioner (DPC) has taken to the development of the Strategy, undertaking Round 1 of the public consultation on Target Outcomes followed by stakeholder engagement across a range of sectors.

CIPL recognizes that, as the Lead Supervisory Authority (LSA) in the European Union (EU) for many of the main actors in the digital environment, the DPC has an important role in fostering compliance with the General Data Protection Regulation (GDPR). CIPL also appreciates the challenges this role can entail. We consider that clarity and transparency in setting out how the DPC will approach its regulatory role is extremely helpful. Given the DPC's crucial role as LSA, we hope that the regulatory strategy sets a precedent for others supervisory authorities (SAs) and reaffirms the DPC's leadership as a modern, fair and effective data protection regulator.

1. Overall Approach

CIPL supports the DPC's willingness to take account of emerging work on effective regulation and behavioural economics which is flagged in the Foreword of the Strategy. Effective regulation and behavioural economics are also important for the discussion on fines and other ways of influencing behaviour under Section 5 of the Strategy "Support organisations and drive compliance." CIPL would welcome further elaboration on this topic to demonstrate explicitly how the DPC anchors its strategic thinking in this approach.

CIPL shares the commitment to a risk-based approach which was envisioned when the GDPR was being developed and underpins its application. CIPL agrees that a risk-based approach to the regulatory work of the DPC is essential. We would welcome a more explicit statement for the need to always take into account and develop further the GDPR's risk-based approach, both by regulators in their supervision and enforcement roles and by organisations when building accountable privacy management programs. We would also welcome the addition of references to the importance of the regulatory approach being evidence-based and results-focused. CIPL appreciates that this may seem a statement of the obvious. However, while CIPL and more sophisticated and mature organisations are well aware of the careful and thorough approach of the DPC to its investigatory work, the Strategy will have a wider audience and it may be useful to reinforce the point. In the same vein we would welcome a reference to the importance of the principle of proportionality in framing appropriate regulatory responses.

2. Strategic Goals

CIPL notes that the “Strategic Goals” and “Desired Outcomes” of the Strategy are derived from the work carried out in the first round of the consultation process. We would suggest that it be made clear that (1) the goals are not listed in order of importance but are all equally important and (2) that the goals are linked to one another and inter-dependent (for example promoting awareness of individuals will also benefit businesses). Lastly, it might add clarity if the Goals were specifically linked to the relevant stakeholder community, for example the Goal “5. Support organisations and drive compliance” might usefully be linked to controllers and processors as the main stakeholders.

3. Regulate consistently and effectively

While CIPL recognizes that this may be primarily a matter for the Irish Government, and indeed the EU Commission, we would raise the importance of clarity and consistency between data protection and other regulatory developments. Organisations are increasingly subject to multiple regulations in the digital area (both nationally and at EU level) and face concerns that different regulatory approaches may impose competing requirements. We would urge the DPC to also consider consistency with other applicable regulatory regimes and possibly to aim to establish liaison relationships with other national regulators operating in the same space or in tangent areas.

CIPL supports the need for the DPC to have adequate resources to carry out its work. This is particularly important given the central role the DPC plays in the implementation of the GDPR acting as a LSA. If the DPC is starved of resources to undertake the complex and difficult work involved in its regulatory role, it raises the risk of reputational damage to Ireland.

In relation to the proposed areas of activity to achieve the targeted outcomes, CIPL would urge the inclusion of reference to the use of settlements to set expectations for stakeholders, including how and when settlement may be considered or agreed. We support the development of case studies which can illustrate how the law is applied and would particularly encourage the inclusion of case studies on international aspects including how matters may be determined between CSAs and the LSA. It would be ideal if such case studies could be worked through with other SAs. The theme of cooperation and communication with peer SAs also resonates with CIPL. The aim of regulators in this field should be to avoid the creation of a “splinternet” form of regulation where different regulators have different standards and expectations. By the same token, CIPL and our members would welcome further specific information being included on the plans to seek clarification and consistency on procedures under the One Stop Shop mechanism and work with the EDPB on international transfers.

4. Safeguard individuals and promote data protection awareness

CIPL supports the DPC's continuing work on sectoral codes of conduct and certifications to help develop best practices to foster trust and assurance. This is one of the areas where the GDPR that has not been fully utilised and developed, and CIPL would like to see all SAs take a more proactive, encouraging and enabling role to get industry to develop and adhere to codes and certifications.

While accepting that it is important to resolve issues for individuals, CIPL also recognises the importance of a regulator taking a strategic, overall approach, rather than being always driven by individual complaints. CIPL is aware of the lessons to be learnt in this area from other regulatory regimes where a focus on individual complaints has sometimes obscured the bigger, long-term strategic challenges with accompanying negative consequences.[32] A focus on complaints may also be perceived as a fairly common response by regulators to assert their powers, but may result in a failure to address strategic issues. Nevertheless, CIPL would like to see more details on how the DPC proposes to tackle this change in direction and looks forward to doing so.

CIPL recommends giving consideration to procedures adopted in other jurisdictions which require complainants to seek redress from the responsible organisation and use other reasonably available avenues to raise their complaint before asking the DPC to intervene. It also recognises that some complaints are at best peripheral to data protection and at worst verging on vexatious, where the real issue of complaint is customer service. CIPL would welcome guidance on how such matters will be handled.

In relation to the aim of working with peer SAs to introduce consistent and consolidated enforcement across the EU, this would be warmly welcomed and supported by CIPL and many multinational organisations. However, it is not apparent how it is to be achieved, or how conflicts between jurisdictions are to be resolved. Potentially, this may be an opportunity to call on the EU Commission to intervene and take on its role as the guardian and arbiter of the EU regulations.

Finally, CIPL members would be interested in working with the DPC to find ways to voluntarily address complaints and resolve issues for individuals without the need to burden the DPC, for example developing "sandboxes" to understand and find solutions to common complaints. Complaint handling is also an element of organisational accountability and more can be done to emphasise the expectations of organisations to respond and deal with the complaints in the first instance.

5. Prioritise the protection of children and other vulnerable groups

[32] See the review of financial regulation in the UK following the financial crisis https://assets.publishing.service.gov.uk – A new approach to financial regulation.

CIPL broadly supports this desired outcome. Some further understanding of the nature of other groups regarded as being vulnerable would be useful and we look forward to seeing this in due course. CIPL also supports the DPC work on the “Fundamentals for Children” and looks forward to further developments in this area.

6. Bring clarity to stakeholders

CIPL welcome these proposals. However CIPL would also ask the DPC to include further transparency material covering:

- The internal complaint handling processes and procedures for investigations and audits; and

- Guidance on the fines structure to be adopted including aggravating and mitigation factors to be taken into account.

A further suggestion is to work towards developing a mechanism to measure successful compliance interventions, including those which do not require regulatory action, such as assessing the number of matters which were resolved by businesses following DPC compliance advice, warnings or notices.

The proposed collective approach to investigating systemic issues raises an interesting new option and CIPL welcomes further elaboration on the specifics of this part of the proposal.

7. Support organisations and drive compliance

Please see our comments under “Overall approach” earlier in respect of the material on methods of effective regulation.

Specifically, we would welcome a stronger emphasis on organisational accountability and what the DPC can do to encourage and reward those organisations that are investing in their privacy programs and trying to do the right thing, sometimes even beyond legal requirements. Organisations face competing priorities and regulatory recognition of the “return on investment” for privacy commitments would be a potent measure in evangelising accountability across all sectors, types and sizes of organisations. Specifically referring to organisational accountability as a factor in determining the nature of enforcement action or the application of mitigation measures would be helpful to organisations.

In view of the importance of the One Stop Shop mechanism and its regulatory effectiveness, CIPL would welcome further discussion around Article 60 operations and how a cooperative approach can be fostered among peer SAs.

Further elaboration of the DPC approach by providing examples of regulatory events and corresponding likely corrective measures could be added to the actions as could more detail on engaging with SAs outside the EEA.

Conclusion

CIPL considers this proposed Strategy to build effectively on previous work and looks forward to the next stage. It reiterates the importance of adopting a risk-based approach to regulation and a proportional and consistent response.

CIPL is grateful for the opportunity to provide recommendations on the DPC's Consultation on the Regulatory Strategy for 2021-2026.

22. Fexco Unlimited Company (Fexco)

About Fexco: With operations in 29 countries, worldwide, Fexco is Ireland's privately-owned financial services business. With a particular focus on payments, foreign exchange and business solutions, since inception in 1981, Fexco has invested in technology to develop and deliver the best solutions to meet customer needs. Fexco processes upwards of €14bn in transactions per annum across FX, treasury, digital tax and government-backed financing sectors. The organisation has developed deep expertise in governance and risk management, as well as lasting relationships with international financial institutions and banks.

Fexco has developed an unmatched capability in building, operating and supporting the delivery of complex mission critical technology platforms for both its own Fexco products and those of its partners. It brings the same rigorous methodology and management focus to all of its projects, leveraging in-house architecture, design, software development and IT infrastructure.

The below comments constitute the responses of Fexco to the Data Protection Commission's (DPC's) Regulatory Strategy 2021 (hereafter 'strategy' or 'regulatory strategy').

1. **International Data Transfers:** The strategy mentions international transfers, namely, at Section 1, where it states: 'The DPC [Data Protection Commission] proposes to work closely with the European Data Protection Board to develop legal certainty for international transfers of personal data.' Considering the significance of this topic and the impact that it is having on all data controllers, greater detail on the DPC's plans in this area would be very welcome. In particular, whether or not up-to-date guidance is anticipated would be important given the uncertainty in this area. Additionally, an outline of the DPC's international strategy would be a helpful guide.

2. **BREXIT:** Although much uncertainty surrounding BREXIT and personal data transfers has been removed by the EU Commission's decision to grant adequacy to the UK on 28 June, 2021, some uncertainty will endure in the medium- to long-term owing to the conditions attached to that decision. Given that there is a substantial dependency in Ireland upon the UK economy, and in particular, that there is a need to avoid, if at all possible, a 'hard border' of personal data transfers within the island of Ireland, detail on the DPC's ongoing contingency plans would be welcome.

3. **Extending Outreach Activities:** With the respect to the strategy's communication goals, although a data protection officer (DPO) network has been

created by the DPC, consideration should also be given to the very large numbers of people who work in data protection, but do not have the DPO designation. This constitutes a very significant proportion of data protection professionals who work under titles such as 'Head of Data Privacy', 'Privacy Officer' etc. Fexco suggest it may be beneficial if the strategy would clarify that this cohort of data protection professionals is deserving of special note when it comes to developing communications and networks plans.

4. **Investment in Technology Teams:** The strategy notes that the DPC will seek 'sanction from government to conduct specialist recruitment campaigns to increase skills and capacity in necessary areas.' Given the pace of technological change, and the significant technical expertise that large technology companies can bring to bear during investigations and inspections, it would be beneficial for the strategy document to outline what plans the DPC might have as regards expanding/modifying its own technology teams, and whether or not it is envisaged that these teams would need to grow to match the evolution of the industry.

5. **More Interaction with Professional Bodies:** Increased, formal interaction with data protection professional bodies, such as through annual roundtable meetings, would be an important part of communicating the DPC's message effectively, and of receiving on-going feedback on the success of its regulatory strategy. These professional bodies can, in turn, reinforce the DPC's message through interaction with their own membership bases.

6. **Targeted Complaints Handling:** With reference to Section 4 of the DPC Regulatory Strategy, with regard to complaints, Fexco agrees that it would be more beneficial to focus on systemic cases that disclose issues of fundamental importance, rather than running multiple parallel investigations into similar complaints. A risk-based, collective approach should, ultimately, lead to a greater vindication of data subjects' fundamental rights and freedoms.

7. **Technology Strategy:** The DPC might give thought to the development of a separate technology strategy that would provide guidance to organisations about how to address data protection risks arising from technology, as well as how data protection compliance might be compatible with sustainable innovation and drive a responsible digital economy. Specific technology priorities could be set in areas such as cyber-security, A.I., big data, machine learning, and web and cross-device tracking.

8. **Digital Strategy:** As part of its efforts to communicate with all relevant stakeholders, the strategy might benefit from the inclusion of a digital strategy.

This could detail the DPC's approach to utilising its website and other digital media to convey updates, and to reinforce key messages. The sustained use of digital media may also assist the DPC in its goal to raise data protection awareness amongst minors, many of whom use digital media as their primary source of information.

9. **Inspections:** The strategy does not clarify what broad approach the DPC will take to inspections. For instance, in the assignment of resources, will themed, cross-industry inspections form a significant part of the DPC's activities, or will activity be primarily directed by complaints and breach notifications? Additionally, will certain areas of data protection compliance receive prioritisation when inspection activity is being planned?

23. Health Research Board

Stakeholder #1: Health Research Board

Stakeholders #2: Secretariat of Health Research Consent Declaration Committee (HRCCDC)

Stakeholder overview:

The **Health Research Board (HRB)** is committed to advancing health research, data and evidence for the benefit of Ireland's people, society and economy. Health and social care data, along with research and statistical data, has the potential to transform healthcare delivery and health management. The HRB enables the use of health data to shape health policy, enhance healthcare delivery and drive broader research and innovation initiatives. It achieves this through its funding schemes and management of the national health information systems. This commitment is set out in the HRB Strategy 2021-2025[33], specifically under strategic object 3 'Trusted data'.

The HRB currently manages four national health information systems in the areas of disability, drugs and alcohol and mental health. The HRB acts as data controller for these systems. Over the last number of years the HRB has consulted the DPC on issues related to the running of these systems.

The Research Strategy and Funding (RSF) Directorate of the HRB has an active portfolio of research grants comprising in the order of 350 awards at any point in time, spanning translational and clinical research, health services research and population health. It supports individual and group-based training for researchers and research-active health practitioners from early-stage through to senior, leadership positions. It funds research in Ireland, across the island, at EU and international levels and invests significantly in research infrastructure and networks spanning the interface between the academic and the healthcare delivery systems. RSF has played a significant leadership role in the years since the introduction of the GDPR (and Data Protection Act) through its awareness raising, funding supports, terms and conditions and policies/guidelines. This has involved very close engagement with the research community, public, patients and carers, the Department of Health and the DPC on a wide range of matters. RSF welcomes the opportunity in the years ahead to continue this engagement with the DPC in respect of health and social care research, and we believe that working with lead organisations like the HRB (and our associated networks) will enable the DPC to have the greatest systemic impact within its limited resources.

[33] https://www.hrb.ie/strategy-2025/

The HRB also hosts the Secretariat to the Health Research Consent Declaration Committee[34] (HRCDC), an independent statutory body established in 2019 by the Minister of Health under the Health Research Regulations 2018[35] ('Regulations'). The Regulations were made under Section 36 of the Data Protection Act 2018 and make explicit consent a mandatory safeguard when processing personal data for health research. In the absence of explicit consent, the HRCDC may make a consent declaration enabling a data controller organisation to process personal data for health research, where the public interest in carrying out the research significantly outweighs the public interest in requiring the explicit consent. For the first time in Ireland, health research is underpinned by a legislative framework which is regulated by the DPC.

A significant development in the national research landscape since the lead-in and implementation of GDPR is the establishment (hosted by the HRB) of a National Office for Research Ethics Committees. National Research Ethics Committees (NRECs), in areas prescribed by the Minister of health, will ensure best practice ethical review and monitoring of decisions, ensuring consistency and compliance with ethical standards. Open and ongoing dialogue between data protection authorities and ethical review boards is critical to ensure common understanding with respect to the similarities, differences and complementary, and to work in concert to ensure ethical and data protection compliance for health research.

The HRB and the HRCDC view the **DPC as a valued stakeholder** that has been supportive of its work and especially so in recent years as the data protection regulatory landscape for health data and research has evolved. The National Health Information Systems (NHIS) Unit of the HRB has always viewed the DPC as an important source of advice in relation to data protection matters especially with the introduction of GDPR. The HRCDC Secretariat has worked collaboratively with the DPC, the HRB and Department of Health over the past year on the recently made amendments to the Health Research Regulations, specifically in relation to guidance material and participation in information webinars. Clarity and consistency in navigation and interpretation of the data protection legislation for the Department of Health, the HSE and health researchers is critical to instil confidence and public trust in health research and the use and re-use of patient and public health data.

The strategic goals set out in the DPC Regulatory Strategy 2021 are welcomed and the following observations are put forward for consideration:

Strategic goal #1 - Regulate consistently and effectively.

[34] https://hrcdc.ie/

[35] http://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf

The health research sector is innovative, diverse and complex, and heavily reliant on the collection, use, sharing and analysis of valuable health data. Such 'processing' of personal data for health research can be multi-faceted leading to challenges with interpretation and compliance of data protection legislation. A recent assessment of EU member state rules[36] on processing health data highlights the variability and complexity of ensuring compliance with data protection legislation and in parallel enabling cross-border exchange of data and re-use of data. To enable this strategic goal, the DPC should continue its engage with health research stakeholders to bring clarity to data protection legislation and consistency in implementation:

- The **guidance and technical support** from the DPC, through its health and voluntary consultation units (David Murphy, Vivienne Byrne) has been invaluable to the HRB and the broader community in carrying out its duties in relation to health data and research.

- The DPCs engagement and collaboration through the **Health Research Data Protection Network** has afforded DPOs an opportunity to seek guidance and clarity on complex data protection matters as they pertain to the health research sector. The HRB welcomes the commitment in the Strategy to continue this proactive engagement.

- Importance of **Data Protection Officers (DPOs)** for Health research: The responsiveness and capacity across the research and evidence ecosystem in terms of DPOs has varied greatly. Many DPOs are overseeing and advising on all processing activities across large and diverse organisations, including technically complex areas of health research. This has inevitably resulted in delays in the progress of many research activities within research performing organisations and across collaborative research programmes, nationally and internationally. The HRB welcomes reference in the Strategy to the actions to (1) work with the DPOs to increase their knowledge and the impact of their role and (2) to engage proactively in technological foresight activities, (3) to actively pursue codes of conduct and certifications in certain areas and (4) to advance clarity and solutions in respect of international transfers. There are all highly relevant to health research and would greatly enhance and support the work of DPOs, and the community more broadly.

Strategic goal #2 - Safeguard individuals and promote data protection awareness.

[36] https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf

- Transparency and awareness of data protection rights of both **public and patient participants in health research** should be given specific consideration.
- Clarity and guidance should be provided to health researchers as to how **data protection rights can be communicated** to research participants, which is non-technical yet comprehensive.
- The HRB strives to provide clear, easy-read information to those who are included in its information systems. Copies are available on request.

Strategic goal #3 - Prioritise the protection of children and other vulnerable groups.

- Safeguarding the data protection rights of children and vulnerable groups is paramount. In the context of health research, it is equally important that these groups are afforded the opportunity, if it arises, to **participant in health research** that may benefit these groups. Specific guidance on appropriate and additional data protection safeguards should be developed for the health research sector where possible, especially in the area of consent, and data sharing.
- Consideration should be given to engaging with **the Department of Children, Equality, Disability, Integration and Youth** on health research, data protection safeguards and interplay with upcoming legislation such as the **Assisted Decision-Making (Capacity) Act 2015.**

Strategic goal #4 - Bring clarity to stakeholders

- The HRB works with all of its stakeholders at national, EU and international level to ensure that data protection issues are foremost to any of the work it undertakes.

The HRB plays a lead and active role in Europe as well as nationally on behalf of the health research and data community in Ireland. The HRB is currently participating in the EU Joint Action- Towards a European Health Data Space (TEHDAS), seeking to influence discussions and resultant activities to optimize the responsible sharing, use and re-use of health and social care data, statistical data and research data for research and innovation and improved policy making. As noted earlier, there is ongoing debate and discussion in Europe about the lack of harmonized interpretations of GDPR across

member states arising from varied responses to the opportunities in GDPR to introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. Clarity, certainty, consistency and codes of conduct in areas such as biobanking, genomics, personalised medicine, artificial; intelligence and big data would be most welcome for the health research community and funders in Ireland- to frame the conditions and safeguards necessary for the processing of personal data for research as a primary purpose and as a secondary purpose.

On 8 July 2020, the European Commission (DG Justice and Consumers) submitted to the European Data Protection Board (EDPB) under Article 70 of the General Data Protection Regulation a request for clarification on the consistent application of the GDPR, focussing on health research, and provided a list of concrete questions related to data processing for health-related research (prepared by DG Research and Innovation). The initial response of the EDPB (February 2021) was most welcome and helpful but many questions remain unanswered, highlighting the complexity of the health research and innovation system, especially where the lines become increasingly blurred between the health delivery system and the research system (e.g., personalised medicine). The HRB eagerly awaits the EDPB guidelines (currently in preparation and due in 2021) on the processing of personal data for scientific research purposes, where they will elaborate further on these issues while also aiming to provide a more comprehensive interpretation of the various provisions in the GDPR that are relevant for the processing of personal data for scientific research purposes. The HRB is available to engage with the DPC as appropriate to both support and inform the DPC's participation and influence in these and other EDPB/EDPS deliberations and to facilitate broader dissemination to the research community in Ireland.

In February 2020, the European Commission presented a digital reform package including a European strategy for data, notably for policy measures and investments to enable the data economy for the coming five years. The Commission's vision of creating a single European data space by 2030 foresees as legislative key actions a cross-sectoral (horizontal) governance framework for data access as well the establishment of common (sectoral) European data spaces in strategic sectors and domains of public interest including a common European health data space (EHDS). Within the proposed horizontal framework of the common data space, the Commission foresees a legislative framework for the governance of common European data spaces and, as appropriate, a Data Act.

As the first of a set of measures announced in the 2020 European strategy for data, the proposed Data Governance Act (DGA) is aimed at facilitating data sharing including reinforcing trust in different types of data intermediaries handling both personal and

non-personal data. With that, both the General Data Protection Regulation (GDPR) and ePrivacy Directive come into scope, providing a potentially comprehensive legal framework. In addition, a health sector specific regulation – the proposed European Health Data Space (EHDS)– may be advanced. These are all welcome developments, but the HRB also acknowledges the joint response of the EDBP/EDPS to the initial DGA proposal where they stressed the need to "ensure consistency with the GDPR with regard to the competence of supervisory authorities, the roles of the different actors involved, the legal basis for the processing of personal data, the necessary safeguards and the exercises of the right of data subjects". It will important that clarity and certainty emerges amongst the various Acts, actors and responses in Europe, and the HRB wishes to play a proactive and participative role in this regard to enhance health research and innovation and health transformation, but to do so in a manner which is responsible, transparent and earns and maintains the high levels of trust by the public in health research in Ireland.

The establishment of national data hubs or authorities facilitates secure and restricted access within safe environments to communities of certified users with clearance adapted to the sensitivity of data. This, along with governance and legislative framework, ensures optimal use of health and social care data for primary and secondary purposes, in a manner which instils transparency, public trust and confidence. In May 2016, the Health Research Board (HRB), in close collaboration with the Central Statistics Office (CSO), published a discussion document 'Proposals for an Enabling Data Environment for Health and Related Research in Ireland'[37], which proposed what it referred to as a DASSL (data access, storage, sharing and linkage) model. The DASSL-type infrastructure proposed drew on the experiences and models in development in the UK, many European countries, Canada, Australia and New Zealand to maximise the value of national data sets for primary and secondary purposes. The HRB is currently funding a Proof-of-Concept project to establish a prototype technical portal/hub which seeks to demonstrate how researchers can be provided with secure and controlled access to anonymous and linked health and social care datasets in Ireland. More recently, the HRB has supported the Department of Health in providing access to the CSO Covid-19 data hub for the purposes of facilitating statistical analyses for inclusion in health research projects. We thank the DPC for their engagement, advice and support in the planning discussions and we would welcome an ongoing dialogue on future developments in relation to a data hubs/safe havens to enhance health research and innovation in Ireland in a manner that ensures compliance with the GDPR.

[37] https://www.hrb.ie/publications/publication/proposals-for-an-enabling-data-environment-for-health-and-related-research-in-ireland

Strategic goal #5 - Support organisations and drive compliance.

- Through its engagement with the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS) and other European groups, the DPCs involvement at this level is essential to ensure Irish data protection legislation and Health Research Regulations enables researchers to use and share health data in a trusted and safeguarded manner, across member states.

- It is even now more critical that the DPC continues to engage at an EU level to ensure data protection legislation in Ireland, including the Health Research Regulations enables researchers and other stakeholder organisations navigate and participate in important initiatives such as the European Health Data Space (EHDS) and the Data Governance Act, which aims to develops and promotes elements on the cross-border sharing of health data in secondary use. Ireland is a stakeholder in The Joint Action Towards the European Health Data Space (TEHDAS), which develops and promotes elements on the cross-border sharing of health data in secondary use. The major expected outcome of TEHDAS is a sustainable roadmap for the implementation of a European Health Data Space.

- Consideration should be given to development of codes of conduct and/or guidance in complex and sensitive areas of health research that involve processing of sensitive data such as genomic and genetic data.

24. The Law Society of Ireland

1 Introduction

1.1 The Law Society of Ireland ('the **Society'**) is pleased to respond to this consultation by the Data Protection Commission ('the **DPC'**) on its Draft Regulatory Strategy for 2021-2026 ('the **Strategy**').

1.2 The Society is the representative organisation for the solicitors' profession in the Republic of Ireland. Our members provide legal advice in respect of data protection law to data subjects, data controllers and data processors in Ireland. Our members represent clients in their dealings with the DPC, including data subjects who lodge complaints with the DPC and controllers/processors who are required to comply with the General Data Protection Regulation ('the **GDPR**') and related Irish laws, some of whom are under investigation by the DPC. As such, the Society provides a broad perspective in reflecting the experience of this diverse stakeholder group.

1.3 The Society recognises that the DPC performs a hugely important role both at a national and European level. The DPC has an onerous and expanding caseload and has to make decisions on how best to allocate resources in light of that challenge. The Society considers it essential that the Government continues to increase the level of funding made available to the DPC as a rapid expansion of regulatory capacity will be required in order for the DPC to deliver impactful regulation with the requisite levels of consistency, across the board.

1.4 The DPC needs to remain competitive in recruiting data protection lawyers and other experts and, where necessary, should receive sanction from Government in relation to salary thresholds to recruit appropriately. Investment in the structures, processes, people and systems used to support the DPC is incredibly important.

1.5 The Society supports the DPC's Draft Regulatory Strategy for 2021-2026 and believes that it represents a strong, ambitious and coherent vision for the future of data protection regulation in the State.

1.6 Building on that vision, the Society recommends six areas for consideration by the DPC in devising its strategy for the relevant period. They are:

1. Publishing more wide-ranging and comprehensive guidance and compliance supports in key areas;

2. Adapting the amicable resolution procedure;

3. Managing systemic and non-systemic complaints;

4. The proposed "collective approach" to investigating systemic issues;

5. The procedure for statutory inquiries; and

6. Participation at the European Data Protection Board (EDPB) and internationally.

2 Publishing more wide-ranging and comprehensive guidance and compliance supports in key areas

2.1 The GDPR is an example of principles-based legislation, meaning that controllers/processors must interpret and apply the principles set out in the GDPR to the circumstances of their processing operations. Large organisations have the resources and capabilities to perform this task, but many small to medium enterprises do not, and notwithstanding that the GDPR is now over three years in operation, these businesses continue to struggle to come to terms with the GDPR.

2.2 The Society acknowledges that the DPC has invested significant resources in developing and publishing guidance on the interpretation and application of different aspects of the GDPR since enactment. However, the Society believes that the DPC should increase the volume and detail of compliance supports which are offered on commonplace and timely issues faced by organisations, while taking into account that guidance on particular matters may instead be published by the EDPB. In addition to publishing guidance, compliance supports could also be offered through information portals, interactive training and the continued development of the DPO network.

2.3 An example of where guidance is needed as a priority is the handling of employee subject access requests. Many employers regularly receive subject access requests from employees or former employees. Whilst the DPC has published general guidance on subject access requests, considerable uncertainty remains among organisations, data subjects and their legal advisers about matters such as: (i) what records constitute the personal data of employees; (ii) the extent of searches that a controller/employer is obliged to conduct; (iii) how the exceptions to subject access requests apply in an employment context; and (iv) the circumstances where a request may reasonably be

regarded as “manifestly unfounded or excessive”. Clear and comprehensive guidance on these issues would benefit data subjects and controllers alike. The employment relationship is the subject of a number of significant treatments in the Data Protection Act 2018 and, as such, regulatory guidance is appropriate.

2.4 In this regard, the Society commends the DPC's timely publication of guidance on data protection issues arising during the course of the Covid-19 pandemic.

2.5 New data protection issues and challenges constantly arise in modern society in respect of which organisations would gladly receive guidance from the DPC to assist them in meeting their compliance obligations. As part of its policy focus, we believe that the DPC should engage and consult with those involved in new developments (in areas such as processing, technology and markets). To achieve that end, investment in forensic and technological knowledge must continue to be a focus.

2.6 We are also of the view that the Strategy should deal with both the compliance supports which are required to be put in place and adequate communication of the availability of same. The Society agrees that vulnerable groups or those who may have less economic power (such as children and the general public) should continue to be the focus of specific policy activities over the coming five year period. 3

3 Adapting the amicable resolution procedure

3.1 The "amicable resolution" procedure, which existed under the Data Protection Acts 1988 and 2003, has been applied to GDPR complaints handling under Section 109(2) of the Data Protection Act 2018. Section 109(2) permits the DPC to "*take steps as it considers appropriate to arrange or facilitate*" the amicable resolution of a complaint which has been lodged with the DPC, where the DPC deems that to be appropriate.

3.2 The Society recognises that the DPC invests substantial resources in the amicable resolution procedure which often leads to a successful regulatory outcome i.e. where both the data subject and controller reach an accommodation without the need for further regulatory action. In some cases, a controller can address a data subject's concerns by providing additional information and/or a clear explanation and in others, a controller will change its decision to refuse a data subject's request as a result of instigation (by the DPC) of the amicable resolution procedure.

3.3 However, it appears that the amicable resolution procedure could be operated without drawing quite so heavily on the DPC's regulatory resources. For example, the DPC could follow the approach of other data protection authorities by directing a

controller/processor to respond directly to a data subject's complaint before the DPC will intervene in the complaint. Only where the data subject remains dissatisfied with the controller's/processor's response would the DPC need to intervene, either by mediating the complaint or taking regulatory action if the DPC determined that there was no reasonable prospect of an amicable resolution.

4 Managing systemic and non-systemic complaints

4.1 The Society supports the DPC's proposal to prioritise the allocation of its resources to the "*cases that are likely to have the greatest systemic impact for the widest number of people over the longer term*."

4.2 This is a sensible approach which best protects the rights of data subjects as a whole. The DPC is an independent expert body which sits within the wider EU data protection regulatory framework. It is well-positioned to identify which issues are of the greatest concern and significance to data subjects. The criteria used to select cases to prioritise should be transparent and a mechanism which would allow organisations/data subjects to apply to have cases prioritised would also be helpful.

4.3 Of course, the prioritisation of resources for systemic cases ought not to lead to any neglect of non-systemic complaints, which are nonetheless important to the individual data subjects concerned. These should also be dealt with in a timely manner.

4.4 All data subjects have a right to lodge a complaint and to have it handled in accordance with the provisions of the Data Protection Act 2018 and the GDPR. However, for non-systemic cases, the DPC has powers under Section 109(5) of the Data Protection Act 2018 to take action without undertaking an extensive investigation. Where the DPC examines the facts and finds an infringement (or not as the case may be), it should use these summary statutory powers as it deems appropriate.

5 Proposed "collective approach" to investigating systemic issues

5.1 The Society notes, with interest, the DPC's proposal to take a "collective approach" to investigating systemic issues. The DPC has not, however, outlined the proposed procedure for a collective approach nor has it identified the relevant statutory basis for such an approach.

5.2 If a collective approach to investigations is to be taken by the DPC, the Society encourages publication of a draft outline of the proposed procedure for further consultation.

5.3 Whilst the lack of information in respect of the proposed procedure limits what can be said at this juncture, the Society would make the general observation that the right of a data subject to seek the vindication of his/her rights is a cornerstone of both the GDPR and Irish law. Accordingly, any collective procedure will have to take account of the rights of individual data subjects and access to an enforcement procedure. Similarly, controllers and processors have individual rights to fair procedures as well as rights to expect that the DPC will follow the processes prescribed by applicable laws. Confidentiality will also have to be respected in any collective procedure.

6 Procedure for statutory inquiries

6.1 At the end of 2020, the DPC had 83 open statutory inquiries, 27 of which related to cross-border processing where the DPC was acting as lead supervisory authority under the GDPR (per the DPC's 2020 Annual Report). These inquiries are often highly complex in nature and the Society recognises that the DPC cannot simply dispose of same through a speedy process.

6.2 The Society believes that the DPC should be commended for resisting public pressure to simply expedite matters – it is far more important that decisions are reached after all relevant facts are gathered and examined, that the parties are heard and that matters arising are thoroughly assessed. It is only through a deliberative process that a real and lasting vindication of a data subject's rights will be attained.

6.3 Nonetheless, the Society proposes the following in order to improve the efficiency of statutory inquiries conducted by the DPC under the GDPR's one-stop-shop mechanism:

6.3.1 The DPC should consult with the controller, concerned EU data protection authorities and any other relevant third party (e.g. processor or data subject complainant) before framing the terms of reference of a statutory inquiry under Section 110 of the Data Protection Act 2018. An initial framing of the issues, before the investigation has commenced, may lead to more targeted terms of reference and ultimately, a more focused inquiry.

6.3.2 The DPC's standard process for statutory inquiries is to issue Requests for Information (RFI) and to invite responses from the controller/processor. This can be a labour intensive, iterative and long drawn-out procedure. An alternative (and perhaps more efficient) approach would be to invite the controller/processor which is being investigated to make preliminary submissions based on the terms of reference of the inquiry. Upon receipt of this preliminary submission, the DPC could then probe the controller / processor to seek further information/documentation as may be required. A similar opportunity to make preliminary submissions could be extended to a

complainant in the case of a complaints-based inquiry under Section 110 of the Data Protection Act 2018, with a right of reply for the controller.

6.3.3 The DPC's standard process for statutory inquiries is entirely paper-based. Undoubtedly, this form of written exchange is a necessary feature of any statutory inquiry. However, the DPC should also be open to in-person meetings/examinations in which controllers/processors who are being investigated are invited, on a voluntary basis, to make an oral, technical demonstration or visual presentation and to be subjected to examination by the authorised officer. It can be incredibly difficult to convey complex technical information without the benefit of visual aids and an examination procedure. Given that Section 12(8) of the Data Protection Act 2018 grants the DPC the discretion to determine its own procedures, the Society believes that it should be possible for the DPC to receive oral/visual presentations as it conducts statutory inquiries (otherwise than by way of a formal oral hearing under Section 138/Schedule 3 of the Data Protection Act 2018).

7 Participation at EDPB and Internationally

The Society supports the DPC's proposal to actively participate at EDPB level.

The Society also appreciates the role played by the DPC when participating in dialogue outside Europe. The DPC plays a leading role in supervising and enforcing the GDPR in the interests of data subjects across the EU.

Commensurate with the significance of the DPC's role, the Society believes that the DPC should be a strong voice at the EDPB, and on the international stage, advocating for the rights of data subjects, being a thought leader on issues such as children's data, and defending the GDPR's one-stop-shop mechanism.

8 Conclusion

The Society hopes that the DPC finds this commentary and our recommendations to be useful and will be glad to engage further on any of the matters raised.

An Coimisiún um Chosaint Sonraí
Data Protection Commission