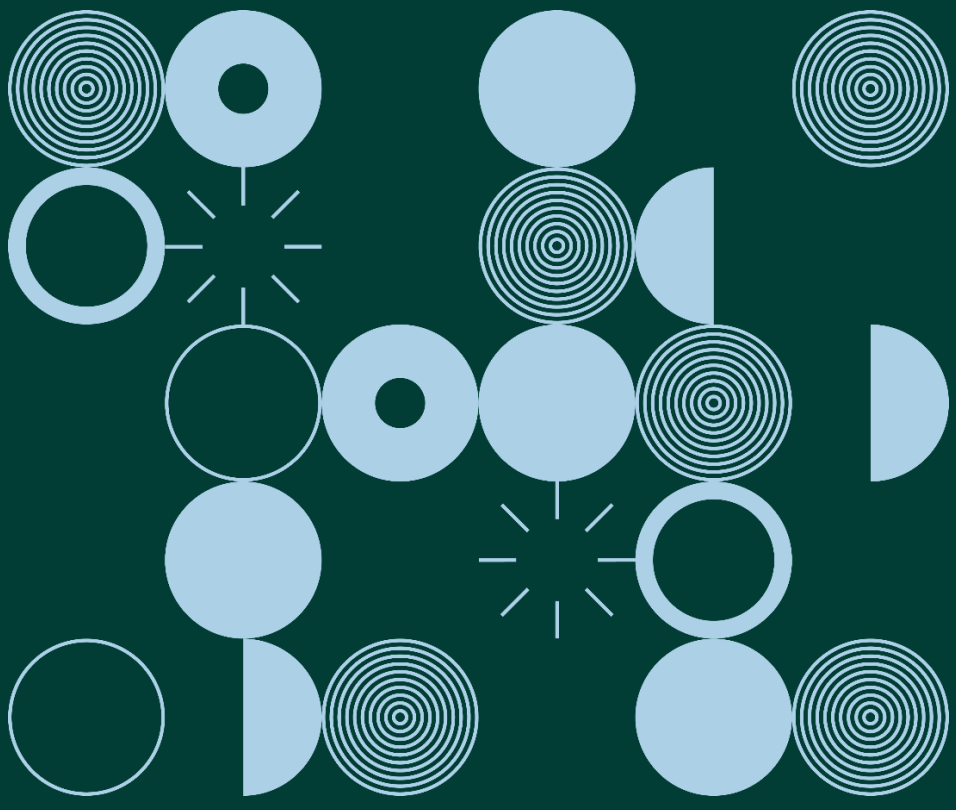
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Regulatory Strategy

CONSULTATION

April 2021



Contents

Glossary

CSA – Concerned Supervisory Authority

DPA – Data Protection Authorities

DPC – Data Protection Commission

DPO – Data Protection Officer

EDPB – European Data Protection Board

GDPR – General Data Protection Regulation

IMI – Internal Market Information System

LED – Law Enforcement Directive

LSA – Lead Supervisory Authority

OSS – One Stop Shop

Foreword

In its Strategy for 2021-2026, the Data Protection Commission sets out an ambitious vision for what we believe will be five crucial years in the evolution of data protection law, regulation and culture.

In developing this draft Strategy for stakeholder consultation, the DPC has been careful to give conscientious thought to the needs and insights of its stakeholders, the legislation under which it must regulate, the context in which it currently operates and the various future states for which it must prepare. It has also taken account of the academic theories that are emerging in respect of effective regulation and behavioural economics. This research has then been balanced against the recognition that the DPC's resources are finite and must be put where they can do the most good, which means that discerning regulatory choices must be made.

The breadth of the DPC's regulatory remit cuts across all areas of personal and public life; both at national and international level. In order to develop a Regulatory Strategy that will provide effective direction for such a vast operational remit, the DPC has been careful to take careful account of the wider context in which it regulates, the needs of its diverse stakeholders and the evolving nature of the fast-paced and non-traditional sectors it regulates.

It should also be acknowledged that this Strategy is being drafted in the very early years of radically reformed data protection legislation – in the form of the GDPR and ancillary Law Enforcement Directive – along with all the attendant interpretative challenges that such immense regulatory change usually produces. These challenges, against a backdrop of hugely increased public consciousness of data protection, has given rise to ambiguities of interpretation and application of the law that the DPC – along with its peer data protection authorities – must work to clarify.

No action or approach outlined in this draft – from the handling of complaints to the emphasis on strategic engagement – has arisen from a desire to do 'less' for stakeholders. The opposite is the case, and all strategic goals have been proposed as a means of doing more, *for more.* The DPC takes a pro-active and engaged approach to regulation and, by putting this document out for

consultation, the DPC wants to make sure it hears as many points of view as possible, before committing to a definite course of action.

The Strategy is arranged according to fundamental goals, underpinned by the DPC's mission, vision and values, which collectively contribute to the delivery of its strategic priorities. The DPC recognises that it cannot achieve its ambitions alone – new partnerships and new ways of engaging will be necessary as we look towards a future of closer convergence. Nonetheless, the DPC builds from a position of confidence: we are a Regulatory office with ambition, a clear sense of purpose, a history of achievement, and a future of considerable promise.

We look forward to hearing the views and insights that this draft Regulatory Strategy generates. While we cannot guarantee that it will be possible to ultimately reconcile all of the disparate views in the final document – we will consider and take account of them all.

How to respond to this consultation

The DPC is aware that this consultation will likely prompt responses with different emphases and perspectives from many quarters, and it is important that the DPC gathers as many points of view as possible before committing to a definite course of action.

We therefore invite stakeholders to share their views with us, in writing, to

dpcstrategy@dataprotection.ie

OR

Regulatory Strategy Consultation

Data Protection Commission

21 Fitzwilliam Square South

D02 RD28

Dublin 2

The length of submission is at the discretion of the respondent and submissions are welcome on whichever point(s) the respondent feels most strongly about.

Closing date for submissions is June 30th 2021

IT SHOULD BE NOTED THAT THE DPC INTENDS TO PUBLISH ON ITS WEBSITE THE CONTENT OF ALL RESPONSES RECEIVED TO THIS CONSULTATION. THE IDENTITY OF EACH PARTY RESPONDING WILL LIKEWISE BE PUBLISHED UNLESS THAT PARTY IS AN INDIVIDUAL WHO HAS EXPRESSLY REQUESTED NOT TO BE PUBLICLY IDENTIFIED.

Mission, Vision and Values

Mission: Upholding the consistent application of data protection law through engagement, supervision and enforcement, and driving compliance with data protection legislation.

The Data Protection Commission safeguards the data protection rights of individuals and provides clarity for the organisations it regulates by:

- *educating stakeholders on their rights and responsibilities;*
- *taking a fair and balanced approach to complaint handling;*
- *communicating extensively and transparently with stakeholders;*
- *participating actively at European Data Protection Board level to achieve consistency;*
- *cultivating technological foresight, in anticipation of future regulatory developments;*
- *sanctioning proportionately and judiciously; and*
- *retaining and amalgamating the expert capacities of its staff to ensure operational effectiveness.*

Vision: The Data Protection Commission is committed to being an independent, internationally influential and publicly dependable regulator of EU data protection law; regulating with clear purpose, trusted by the public, respected by our peers and effective in our regulation. The DPC will play a leadership role in bringing legal clarity to the early years of the General Data Protection Regulation. The DPC will apply a risk-based regulatory approach to its work, so that its resources are always prioritised on the basis of delivering the greatest benefit to the maximum number of people. The DPC will also be a rewarding and challenging place to work, with a focus on retaining, attracting and allocating the most appropriate people to deliver on its mandate, recognising the value and capacities of its staff as its most critical asset.

Values: The Data Protection Commission is an autonomous regulator, with responsibility for regulating both private and public sector organisations, as well as safeguarding the data protection rights of individuals. In the conduct of these duties, the DPC is committed to act always in a way that is:

- ✓ Fair
- ✓ Expert
- ✓ Consistent
- ✓ Transparent
- ✓ Accountable
- ✓ Forward Looking
- ✓ Engaged
- ✓ Independent

Mandate

The Data Protection Commission is afforded a broad-ranging mandate for the purpose of monitoring and enforcing the General Data Protection Regulation, which provides individuals with enhanced rights to data protection and increased obligations for organisations who process personal data. The GDPR also greatly strengthens the powers of Data Protection Authorities, and the DPC's given powers and assigned tasks allow it to handle complaints from individuals, in addition to conducting its own investigations into more systemic areas of risk. The DPC regulates in accordance with the General Data Protection Regulation, the Data Protection Act 2018, the E-Privacy Directive and the Law Enforcement Directive.

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**

1. Regulate consistently and effectively

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

The GPDR introduced harmonised legislation across Europe with the intention of providing legal certainty to both individuals and organisations as to how the personal data of EU persons could be processed which, to a large extent, it has done.

Crucially, the GDPR is based on principles rather than specifics, which allows it to expand and accommodate future developments in the uses of personal data. However, this does mean that the legislation must undergo critical evaluation every time it is applied to specific contexts or technologies.

Given the pace at which technology and society continue to evolve, there is a distinct need to increase certainty and stability in how data protection law is applied. 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.

Stakeholder feedback, both from individuals and others, shows that there is a real desire for greater transparency about how the DPC carries out its regulatory functions and for such information to be made available in a comprehensible and audience-appropriate manner. Clear, consistent and transparent regulation of data protection law supports compliance and empowers individuals.

The DPC will engage iteratively with the Government regarding the expanding resources necessary to ensure the operational effectiveness of the DPC, now and into the future. In addition, the DPC will also retain concurrent focus on building the organisation as a rewarding and challenging place to work, promoting self-development and learning for its employees, recognising that its staff are its most critical asset.

In order to achieve this outcome, the DPC proposes:

- Clarifying the limits of legislation and setting expectations for stakeholders, including how and when corrective measures are imposed.
- Improving guidance to individuals, including vulnerable groups, in an appropriate format, promoting deeper understanding of data protection law and increased control over personal information.
- Standardising and publishing the procedures for complaint handling and inquiries.
- Increasing transparency and provision of information on the DPC's outreach activities and engagement with stakeholders;
- More frequent publication of case studies illustrating how data protection law is applied, how non-compliance is identified and how corrective measures are imposed.
- Cooperation and communication with peer data protection authorities on emerging issues.
- Seeking clarification and consistency on procedures under the One-Stop-Shop mechanism and international cooperation.
- Working closely with the European Data Protection Board to develop legal certainty for international transfers of personal data.
- Petitioning government for the provision of adequate budget allocation to ensure that the strategic priorities the DPC has identified are deliverable.
- Seeking sanction from government to conduct specialist recruitment campaigns to increase skills and capacity in necessary areas.
- Prioritising training appropriate opportunities for current staff to ensure that skills are kept up-to-date.
- Engaging with both the Department of Public Expenditure and Reform and the Office of Public Works to secure essential central office space.
- Upholding our Public Sector Duty and ensuring we comply with Standards in Public Office.

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.

Understanding and controlling the use of our personal information is key to having control over our own lives. Data protection law recognises this and the EU Charter of Fundamental Rights defines the right to have one's personal data protected as a fundamental human right and, as a result, the bar is set very high in terms of the levels of transparency and accountability that EU persons expect when their data is processed by an organisation.

The DPC has a specific mandate to uphold the rights of individuals to access personal information that relates to them, and to ensure that the information is processed fairly. Transparency in how individuals' personal information is handled is essential, as is trust in the organisations that use it. Feedback from all stakeholders has called for an increase in levels of transparency on what constitutes a 'good' or 'bad' actor in processing terms. The DPC will continue its 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.

The DPC wants to achieve as much as possible for as many people as possible. This includes not only the many thousands of individuals who contact us directly, but also the many millions of people who do not, but whose rights may have been infringed by circumstance. In order to do this effectively and efficiently, the DPC needs to 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 addition to the work the DPC undertakes to support organisations in understanding their compliance and accountability requirements, the DPC must also focus on increasing individuals' awareness and understanding of data protection law, so that they can make more informed data protection choices and exercise their own authority under the GDPR.

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.[1] The 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. The DPC 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.

Stakeholder feedback from individuals indicates that what they really seek is greater understanding of their rights and entitlements, so that they can empower themselves, identify reputable actors and conduct their transactions with confidence. By allocating DPC resources to the systemic areas where they can do most good, the DPC can positively impact levels of awareness and compliance, and move away from a complaint-heavy system which is neither expedient nor beneficial for the majority.

It is important to note that the DPC is not looking for ways to dismiss complaints – it is however trying to find a more efficacious way of handling the extremely high volumes of complaints it receives annually, and to do so in a way that benefits the greatest majority of people. The DPC's proposition is that there is more than one way to uphold the data protection rights of individuals, including allocating resources to high-risk issues where they can do most good.

In order to achieve this outcome, the DPC proposes:

- Raising public awareness of their data protection rights and how they can control the use of their personal data.
- Taking account of how data protection impacts vulnerable groups and engaging with advocacy groups to communicate this appropriately.
- Identifying trends and themes within individual complaints so that we can achieve strong collective outcomes.
- Engage with civil society bodies on areas of concern for individuals.

[1] DPC Ireland 2018-2020 Regulatory Activity Under GDPR

- Prioritising the allocation of DPC resources to cases that have higher systemic impact on large numbers of people.
- Promoting a cultural shift towards compliance by extensive engagement with stakeholders, so that data protection rights are upheld as a behavioural default by society.
- Regularly communicating with organisations on investigation procedures and final outcomes.
- Engaging fairly with organisations to promote openness, trust and compliance culture.
- Actively promoting the development of codes of conduct and certifications to enable sectoral best-practice and demonstrable compliance in processing activities.
- Working with peer DPAs to introduce consolidated and consistent enforcement across Europe, which would harmonise enforcement approaches and agree the criteria for regulatory success.

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.

In the DPC's original consultation on the draft target outcomes, we identified the specific protection of children's data as a desirable strategic outcome. However, a key finding from the DPC's iterative engagement with stakeholders - from across all sectors - has been their expansion of this category to include vulnerable groups in general, identifying the elderly, non-native speakers and those from at-risk demographics such as the homeless as being in need of specific supports to ensure their data protection rights are upheld.

Stakeholders felt that children and vulnerable groups shared a common risk factor: a frequent dependency on others to advocate on their behalf. Respondents to our consultation on target outcomes specifically identified the risks posed to children and other vulnerable groups when those persons advocating for them were themselves unclear on the provisions of data protection legislation, most particularly when it came to sharing data with third parties. Respondents cited instances where the confusion around data sharing – and particularly around consent – had resulted in both children and vulnerable adults enduring prolonged exposure to adverse situations, due to what had become an incapacitating perplexity around how, what and when to share data.

In the specific case of children, stakeholders further felt that the potential for uninformed choices around data sharing to have direct consequences in later life posed sufficient risk to warrant targeted and age appropriate education for minors, so that they can grow up aware of their rights and appreciate the importance controlling their own personal information. Education of minors is also deeply linked to the debate around the age of autonomy for children to exercise their rights on their own behalf and the veracity of consent and 'age

gates' as measures of accountability for data controllers whose services are directed at, intended for, or likely to be accessed by children – particularly online.

The GDPR is intended to safeguard the EU fundamental right to data protection and thereby improve conditions for EU persons, not diminish them. The DPC has a further duty under Section 42 of the Irish Human Rights and Equality Act to promote equality, prevent discrimination and protect the human rights of all who will be impacted by its policies and plans. Both of these principles underpin the work of the DPC and are reinforced by its drive to engage and educate, so that the provisions of data protection law are enjoyed equally by all, including those who require extra support to uphold their rights.

In order to achieve this outcome, the DPC proposes:

- Defining the specific protections required to safeguard the rights of children in the protection of their personal data, and providing guidance for individuals and organisations.
- Providing ready-to-use education materials and raising awareness of children's data protection rights, aimed at children, their teachers, their parents and guardians.
- Actively promoting the development of codes of conduct on the processing of children's personal data.
- Conducting detailed research on how data protection law applies to children, both internally and through research partnerships, for example on the use of age verification mechanisms and methods for obtaining parental consent for online services.
- 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.
- Continuing DPC efforts to bring clarity and consistency to the application of data protection law, so that controllers can operate effectively and without undue anxiety.

- 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.
- Assessing annually the DPC's efforts in response to its Public Sector Duty and providing a public account of same in our annual report.

4. Bring 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.

The GDPR obliges data protection authorities to fulfil a number of distinct functions as regulators and affords authorities significant powers of investigation and sanction where they find that the law has been infringed. This suite of necessary and effective powers includes, but is not limited to, the ability to fine transgressing organisations. While corrective powers have been enumerated in the GDPR, their consistent application is not, in order to allow for the different requirements of member state law.

The DPC has finite resources available to fulfil its extensive mandate and therefore needs to give real consideration as to how best to apply them, to ensure that complaints of less systemic importance do not disproportionately occupy the resources of the regulator when those same resources could be applied to systemic cases, improving data protection outcomes for multiple individuals. The goal is 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.

The GDPR advocates a risk-based approach to data protection, in order to deliver improved results for data subjects in a timelier manner. On this basis the DPC may, in the future, adopt a collective approach to investigating systemic issues, rather than run multiple investigations into individual complaints about the same matter. Running multiple parallel investigations is costly in terms of time and resources and does not deliver improvements for individuals beyond those to whom the particular case relates. If individual rights can be vindicated by a collective approach, the DPC believes it is more prudent and expeditious to do so. 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.

Feedback from focus group consultations with individuals reported a sense of frustration or undue burden amongst individuals who felt 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.

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. However, in parallel to its supports for organisations and where necessary, the DPC will also punish those entities who infringe data protection law, and will do so in a way that is effective, proportionate and dissuasive. By a balanced combination of these harder and softer regulatory approaches, the DPC will further reinforce the fundamental importance of accountability for data controllers under the GDPR.

In order to achieve this outcome, the DPC proposes:

- Prioritising the allocation of DPC resources to cases that have higher systemic impact on large numbers of people.
- Regulating in a fair, impartial and transparent manner.
- Applying corrective powers proportionately – including fines, where appropriate – to produce changed behaviours and an improved culture of data protection compliance.
- 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.
- Working with the EDPB to develop consistent procedures for the IMI system and improving the metrics it generates.

- Regularly communicating with organisations on investigation procedures and final outcomes.
- Engaging fairly with organisations to promote openness, trust and compliance culture.
- Working with our peer DPAs to introduce consolidated and consistent enforcement across Europe, which would harmonise enforcement approaches and agree the criteria for regulatory success.

5. Support organisations and drive compliance

Desired outcome: 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.

The GDPR was developed, in part, to ensure legal certainty and consistency for organisations whose work involves – wholly or partially – the processing of personal data. This certainty around obligations was intended, in turn, to facilitate future commercial endeavours which would be compliant, accountable and in accordance with harmonised data protection standards.

However, the introduction of harmonised data protection law without a harmonised enforcement framework has produced some inconsistencies of understanding as to what impactful regulation means. There is sometimes a tendency to conflate fining with regulatory success and to use the imposition of fines as a means to measure effectiveness. In the responses received from stakeholders, this was one of the areas where opinion diverged. Individuals favoured large fines for breaches of data protection law (some respondents drew a distinction between first and repeat offenders, having no tolerance for the latter) while respondents from industry called for a more risk-based approach, so that instances of wilful negligence or deliberate infractions would be punished more severely.

The so-called 'hard enforcement' options and sanctions are tools at the disposal of the regulator, but they are not the limit of the regulatory role. That extends beyond the application of penalties to include changing cultural approaches to data protection for the benefit of society as a whole. This is done by extensive engagement - which is not indicative of an unwillingness to regulate, but rather a recognition that investing time and effort into developing a culture of compliance will ultimately drive data protection efficacy. The DPC is committed to using the full range of its regulatory tools – including fines – to bring that culture of compliance about.

This is also true in cases where the DPC acts as the Lead Supervisory Authority for cross-border inquiries, where it must determine the parameters of its investigations are set in such a way as to ensure that a result is ultimately

deliverable within the stipulations of the law. We recognise that the geographical and operational spread of some of our regulated entities makes the outcomes of our multinational inquiries of direct relevance to peer DPAs, as is the case with all cross-border operations. The DPC will continue to conduct its inquiries, fairly and transparently, according to the independence specified to it by the terms of the GDPR, and in accordance with its obligations under the law. It will also work with its peers at EDPB level to improve communication around the scope of DPC inquiries and, more particularly, to achieve clarity so that Article 60 operations can proceed smoothly and deliver outcomes for all concerned parties in a timelier manner.

Guidance and engagement with organisations will be crucial to drive accountability and promote the culture of data protection compliance more generally. They are regulatory tools in their own right, and should not be undervalued because they deemed to be 'softer' than straight penalties. Driving compliance – rather than retrospectively and unilaterally penalising non-compliance – can ultimately produce better results for all stakeholders. The GDPR is a risk-based regulation and, as per the responses to our consultations, a risk-based approach to sanctions is also the preferred method of applying these powers. The DPC will prioritise prosecution, sanction and/or fining those infractions that result from wilful, negligent or criminal intent.

In order to achieve this outcome, the DPC proposes:

- Pursuing effective regulatory actions which makes use of the full suite of corrective measures, appropriately applied, to regulate effectively in a rapidly evolving sector.
- Regulating in a fair, impartial and transparent manner.
- Applying corrective powers proportionately to produce changed behaviours and an improved culture of data protection compliance.
- Promoting a cultural shift towards compliance by extensive engagement with stakeholders, so that data protection rights are upheld as a matter of normal business practice.
- 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.

- Actively pursuing codes of conduct and certifications to enable sectoral best-practice and demonstrable compliance in processing activities.
- Producing indicative guidance on scope-setting for large-scale and multinational inquiries.
- Communicating proactively with other EDPB supervisory authorities on emerging issues.
- Engaging with data protection authorities from outside the EEA to understand the differences in data protection laws and their implications.
- Collaborating with peers on international cooperation endeavours.
- Participating at conferences and other events so that our regulatory approach is widely communicated and understood.
- 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.
- Working with DPOs to increase the knowledge and impact of their role.
- Engaging consistently and iteratively with businesses and representative bodies to build trust and increase compliance.
- Regularly reviewing and communicating our supervision and enforcement priorities.

An Coimisiún um Chosaint Sonraí
Data Protection Commission