Public consultation on the DPC's Regulatory Strategy 2020 - 2025

Consultation Round 1 of 2: Target Outcomes

December 2019
Data Protection Commission
21 Fitzwilliam Square, Dublin 2

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Contents

1. Introduction

The right to a private life, and the freedoms that this right should bring, is a long-standing one. The protection of personal data stems from that right but it is an area of the law that is still rapidly evolving.

At the Data Protection Commission (DPC), we are currently preparing our new Regulatory Strategy, to cover the period from 2020 to 2025. Even with that evolving backdrop, we want our new strategy to ensure that we **regulate with clear purpose** – clear to the people whose rights we safeguard, clear to the organisations that we regulate, and clear to ourselves and our fellow regulators.

In preparing the strategy, we are **consulting as widely as possible**.

- *We want to consider the views of our diverse stakeholders, especially the views of members of the public whose data protection rights we seek to uphold.*

The strategy will clearly set out the **DPC's regulatory priorities**.

- *We want to give insight and greater certainty to organisations and people on how the DPC intends to regulate to maximum effect.*

This strategy will become our guide in **how we deliver our obligations**.

- *We want to exercise our regulatory powers in a way that upholds the data protection rights for as many people as possible, for maximum impact over the long-term, within the resources that are available to us.*

This consultation document on our Target Outcomes is the first of two rounds of open public consultation, as part of the development of the new Regulatory Strategy. The written submissions received from this first round will be analysed carefully during the drafting of the Regulatory Strategy itself.[1]

In preparing our Regulatory Strategy, we will take full account of our obligations under Section 42 of the Human Rights and Equality Commission Act 2014.[2]

The draft Regulatory Strategy will be published in early 2020 and further written submissions on the draft will be invited as part of the second round of open public consultation.

[1] While the DPC will consider all submissions received, there should be no expectation by any party responding to the DPC on this consultation that every issue, position or view raised in its submission will be addressed specifically in the new DPC Regulatory Strategy.
[2] Section 42 of the Human Rights and Equality Commission Act 2014 is set out in the appendix of this document.

2. How to Respond to this Consultation

A summary of the DPC's work is set out in Section 3 of this document, along with some key terms related to data protection. We also explain our approach to developing our new Regulatory Strategy in that section.

Section 4 of this document outlines the **target outcomes that the DPC seeks to achieve** through our work. Specific questions are included throughout that section to which the DPC requests responses via written submissions. These questions are listed together in section 5.

- *Please send your submission with responses to any or all of the specific questions on which you would like to respond, by email to dpcstrategy@dataprotection.ie or by post to DPC Strategy, 21 Fitzwilliam Square, Dublin 2, Ireland.*
- *This first round of public consultation will be open for submissions until 24 January 2020.*

We especially welcome responses and submissions from members of the public and groups who do not generally comment on data protection matters. With that in mind, we have deliberately avoided technical and legal terminology as far as possible, so that this document is accessible to as many people as possible.

Of course, we also welcome submissions from advocacy groups in the area of data protection, from the organisations we regulate and their representative bodies, from academics in the field and other experts, from special interest groups, and from other commentators. We also welcome submissions both from within Ireland and beyond.

We expect, and welcome, diverse views as part of this consultation. We want to understand the perspectives of all our stakeholders and we will be transparent in how we come to our conclusions. All submissions will be reviewed and analysed carefully. A summary report of our analysis will be published on the DPC website in early 2020, as a separate document to the draft Regulatory Strategy which is also due to be published in early 2020.

The DPC also intends to publish the contents of all submissions received on the DPC website. The identity of the submitting party will also be published with each submission, unless that submitting party is an individual person and has expressly asked not to be identified.

3.The Work of the DPC

Explanation of key terms

What is personal data?

Personal data is any information that relates to you personally, when you are identified (or could potentially be identified) in connection with that information. In other words, it is any piece of information about you, such as your name, your date of birth, your email address, your phone number, your address, or a photo, that is linked to you or could be linked to you.

What is data protection?

Data protection law is about everyone's fundamental right to the protection of their personal data. When you give your personal data to an organisation, they have a duty to comply with certain rules which limit what they can do with your personal data.[3] Collectively, these rules, together with the rights that someone has to protect their personal data, are known as data protection. Organisations that decide on why and how to use your personal data are known in data protection law as 'data controllers', while people who give their personal data to organisations, or people whose data is obtained indirectly from another organisation, are called 'data subjects'.

What does 'processing' mean?

Data protection law sets out the rules that apply to the processing of personal data by organisations. Processing basically means using personal data and doing anything with it, from collecting to storing it, retrieving it, consulting it, sharing it with someone else, erasing it and destroying it.

What are data protection rights?

People have specific rights in relation to their personal data. These rights include, amongst others:

i. the right to be informed about who holds your personal data and why it is being processed (transparency),
ii. the right to access and be given a copy of your personal data (access),
iii. the right to rectify inaccurate or incomplete personal data (rectification), and
iv. the right to have your data erased (erasure).

What is the GDPR?

The General Data Protection Regulation[4] (GDPR) is an EU law which came into force on 25 May 2018. It is essentially a new set of data protection rules concerned with ensuring that each of us knows when personal data about us is collected and how it will be used, and giving us more control over the use of our personal data.

[3] The fundamental principles that must be adhered to when processing personal data are in the appendix.
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

The role of the DPC

The DPC is the **national independent authority** in Ireland responsible for upholding the fundamental right of individuals in the European Union (EU) to have their personal data protected. This means that the DPC is responsible for monitoring compliance with the GDPR and with several other legal frameworks that are listed in the appendix of this document.

By law, the DPC has always been an entirely independent body in how it delivers its regulatory tasks, including being independent of the Government. The GDPR also requires that the DPC has complete independence. The independence and objectivity of the DPC is reinforced by the fact that all of our funding is now directly voted by the Oireachtas, and none of our funding is from fees, levies or fines[5].

The GDPR defines the work of each supervisory authority in the EU, including the DPC.

- *Article 57 defines the main tasks of the DPC, and*
- *Article 58 defines the powers of the DPC.*

These tasks and powers are listed in the appendix of this document. The Data Protection Act 2018[6] also defines the statutory powers, duties and functions of the DPC.

[5] Under Article 57(4) of the GDPR, any supervisory authority may charge a reasonable fee where requests are manifestly unfounded or excessive.

[6] The Data Protection Act 2018 gave further effect to the GDPR and also gave effect to the EU Directive known as the Law Enforcement Directive or LED (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA).

Taking all of these tasks, powers and duties together means that, by law, the DPC must perform **many different functions every day**.

The scope of the DPC's work is very broad as we supervise every organisation that is processing personal data, whether public[7] or private, and regardless of industry or sector or size. This includes those organisations that fall under the scope of the Law Enforcement Directive (LED). However, despite that broad scope to supervise the processing of personal data, we do not have any regulatory scope in law that would directly cover other technology issues, such as 'fake news', online content moderation and online safety.

[7] With the sole exception of the Courts.

Changes over the past 5 years

As an organisation, the **DPC has changed radically** over the past 5 years, and so too has the work that we do.

- *The changes in the law mean that the DPC has taken on **extra responsibilities** and has gained **more powers** as a regulator, as summarised in the section just before.*
- *The DPC now has a **very central EU role** in safeguarding the data protection rights of many millions of people across the EU, as we supervise the technology, internet and social media companies that have their European headquarters in Ireland, on behalf of all EU individuals and not just those in Ireland. This is known as the **One Stop Shop** model under the GDPR.*[8]
- *The DPC now has particular responsibilities relating to the processing of **children's personal data**, under the GDPR and the Data Protection Act 2018.*
- *The DPC now has **five times the number of staff** that we did five years ago, due to the increase in our responsibilities and workload.*

The introduction of the GDPR, including the One Stop Shop model, has been a very significant change for the DPC. That change in itself will take several more years to fully bed down.

But changes are not just limited to the introduction of the GDPR itself. The work of the DPC is also impacted by other continuing changes in our wider environment, at an Irish, EU and international level. Those impacts will continue over the next 5 years.

Data protection is becoming ever more prominent.

- *In the past, there was a distinction drawn between the digital economy and the economy, and between digital society and society. Today, that distinction no longer exists and our personal data is used to decide how we are offered particular services, products, news and choices - and sometimes information about us is used in certain ways that mean that some of us are not offered particular services, products, news and choices, or in ways that mean we are not clear on how or by whom our personal data is being used. Our understanding and control of how our personal data is used is central to our control of our own lives.*
- *Data protection rights are more widely discussed now than ever before, in homes, schools, workplaces, and in traditional and social media. However, the impact of this discussion is unclear, in terms of how it influences organisations in their approach to personal data processing and in how it influences people to exercise their data protection rights.*
- *Given that rapid conversion to a digital society and digital economy, it seems that what is considered reasonable and fair in the processing of personal data is also still evolving.*
- *This evolving interpretation and prominence of data protection partly explain why the types of complaints we receive at the DPC are changing in their nature. We are*

[8] The One Stop Shop model is explained in the appendix of this document.

receiving an increasing number of complex complaints that touch on several aspects of data protection law. We are also receiving more and more complaints relating to data protection rights that stem from situations that centre on completely different laws, for example, situations where receivers have been appointed or where legal proceedings are underway.

Technology is rapidly changing.

- *The GDPR is based on principles and is technology-neutral. The application of the GDPR to new technologies and to new types of personal data processing must be interpreted – by organisations and by the DPC. This includes still rapidly-developing technologies, such as facial recognition, artificial intelligence, blockchain and advertising technology (adtech).*
- *In recent years, some apparent advances in technology have proceeded without regard to the protection of personal data, and indeed without real regard for whether those advances are serving any purpose or solving any actual problems.*

The legal environment is still evolving.

- *The work of the DPC must take account of the growing body of case law in the area of data protection, especially judgments of the Court of Justice of the EU. We must also have regard for case law on good administration and procedural fairness, given the scale of our powers.*
- *Although the text of the EU's draft ePrivacy Regulation has not yet been agreed and the date for its introduction has not yet been set, we know that its introduction will impact the DPC's functions and responsibilities.*
- *Many countries outside the EU have already enacted or plan to enact new data protection laws. The DPC is monitoring these changes to understand the potential impact to the practices of the multinational organisations that we supervise on behalf of the EU.*

The European political environment is changing.

- *Any Brexit scenario would impact how organisations that operate into or out of the UK, and who therefore will engage in cross-border processing[9] in the future, remain compliant with data protection law. This impact would be particularly sharp in a Brexit no-deal scenario.*
- *Any Brexit scenario would also impact the work of the DPC, particularly in approving and authorising personal data transfers between Ireland and the UK.*

[9] As defined by Article 4(23) of the GDPR.

Developing the DPC Regulatory Strategy

The work of the DPC could be summarised very simply.

> ***We perform our tasks and functions as set out in law. We produce outputs (for example, issuing guidance for individuals and organisations). We take regulatory actions by exercising our statutory powers (for example, by using our corrective powers).***

We most definitely **must and will** continue to perform our tasks and functions in law, and our new Regulatory Strategy must take account of this.

However, we are now in our second year of GDPR implementation. We now have clarity on the budget available to us for 2020 at least, and it is not unlimited.

- *Our new Regulatory Strategy is an opportunity to re-examine how our work could have the **biggest impact possible within the resources we have available to us**, taking account of the greatest risks to people's rights.*
- *Our new Regulatory Strategy must consider how we can best set ourselves up to deliver that impact over the next 5 years even **while our regulatory environment continues to change**, from the point of view of changes in society, technology, law and the EU.*

For those reasons, our analysis is starting with what we want to achieve as a regulator, rather than starting with what is demanded of us.

1. First, we're focusing on **WHY** we do **WHAT** we do – *what are the target outcomes to which we aspire and what are our activities that achieve those outcomes?*
2. Second, we'll analyse **HOW** we deliver those activities to achieve the outcomes we seek – *what is our Regulatory Strategy for the next five years?*

We are inviting submissions on the first question *1* above via this document. We want to be open-minded, consultative and transparent in how we examine these fundamental questions.

The submissions we receive from this first round of consultation and our own analysis will inform our new draft Regulatory Strategy for the period 2020 to 2025, to answer question *2*. The Strategy will address **how** we will achieve our target outcomes.

- *It will set out our mission and vision for the lifetime of the new Strategy.*
- *It will define our priorities and balance of activities within the resources we have available to us, to ensure we have maximum impact to achieve our target outcomes.*
- *It will include our enforcement priorities and explain how we will execute our powers and tasks.*
- *It will set out the building blocks that are needed to deliver the strategic priorities, for example, organisation development and partnerships.*

The draft Regulatory Strategy will be the subject of the second round of open public consultation in early 2020.

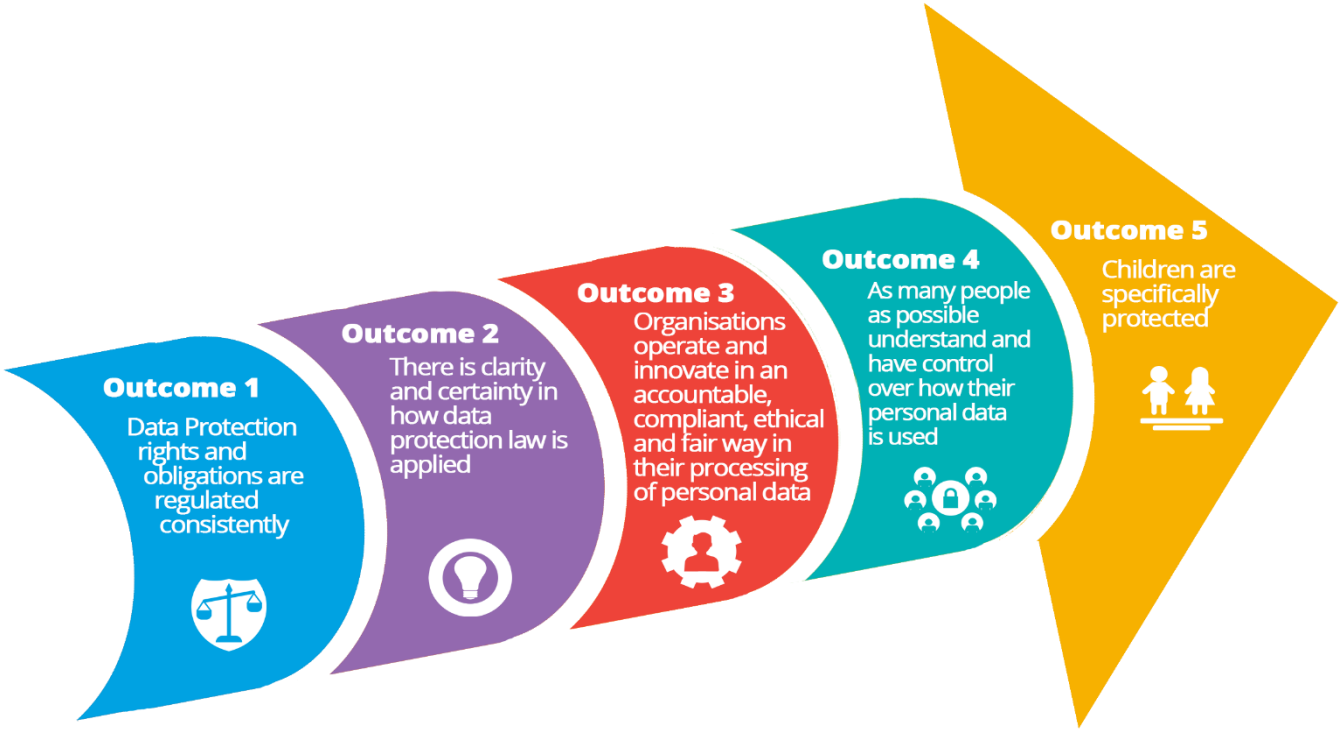
4. Target Outcomes

Our first focus is on **WHY** we deliver the work of the DPC.

All of our work has its origins in the law as it stands now, and in how the law has evolved over time, in terms of the fundamental right that every person has to the protection of his or her personal data. We deliver our work within the legal framework[10] and within our statutory remit. However, we do not approach our work as merely our fulfilment of our legal obligations and functions – our overriding purpose is that our work delivers concrete and long-lasting change.

We see **five** target outcomes that drive us in completing our tasks, functions and duties in law. They each build on each other and we seek to make progress on **all five at the same time**. These five target outcomes are the core reasons for why we do the work that we do.

We may never reach a point in time when any of these five target outcomes is complete and fully achieved. We also recognise that other events, influences and organisations have positive impacts on these five outcomes, and future improvements will not be just due to the work of the DPC. Nonetheless, these are the five target outcomes that we strive towards at the DPC.



Consultation Question 1

Is there any other distinct outcome that the DPC should include and why? How would that additional outcome fit with the existing five target outcomes?

[10] The full legal framework for the DPC's work is set out in the appendix of this document.

Outcome 1

Data protection rights and obligations are regulated consistently.

We consider that this is a target outcome in its own right, and is not just a means to ensure our other target outcomes are achieved. Being consistent is a key component of being fair.

We see three different aspects to consistent regulation.

- **Within the DPC,** we aim to be consistent in how we handle complaints, inquiries and other matters, taking account of the different contexts for those cases. We expect that this aspect of the target outcome is achievable in the near term. Since the GDPR took effect, we have been applying this consistency so that people and organisations know what to expect from us procedurally, even if certainty and clarity on the substantive legal aspects is still developing (target outcome 2).
- **Within the European Economic Area (EEA)[11],** we supervise and enforce the GDPR in a way that is consistent with other EEA data protection supervisory authorities, who are all members of the European Data Protection Board (EDPB).[12]
- **Internationally**, we would like to see that the same high standards of protection that are available to people in the EEA will continue to become available to those in other countries around the world, and are regulated accordingly. This global convergence of data protection law, to the EU standard, would also simplify operations for organisations that operate in multiple countries.

These are the activities that the DPC undertakes to achieve this target outcome.

- Reinforcing the right to notice, the right to be heard and the right to be given reasons within our own procedures and practices, where applicable;
- Examining all relevant judgments of the Courts on administrative and procedural matters, and taking full account of those judgments in our own procedures and decision-making;
- Standardising our procedures for handling queries, complaints, inquiries and other regulatory tasks where possible, and publishing explanations of those procedures to people and organisations;
- Setting the expectations of complainants and organisations, at the outset of every case, on the procedures that will be followed by the DPC, including how and when we use our corrective powers;

[11] The European Economic Area includes all European Union (EU) member states and Iceland, Liechtenstein, and Norway.

[12] The tasks of the European Data Protection Board (EDPB), in ensuring the consistent application of the GDPR, are set out in Article 70 of the GDPR. As well as the supervisory authorities of the EEA countries, the European Data Protection Supervisor (EDPS) is also a member of the EDPB, with the EU Commission also participating in its activities and meetings.

- Cooperating with other EDPB supervisory authorities on cases that fall under the One Stop Shop[13] model, including delivering our obligations as a lead supervisory authority to consult with other EDPB supervisory authorities on our draft decisions and to take due account of their views;
- Encouraging other EDPB supervisory authorities to take part in joint operations on DPC-led investigative work, particularly to make best use of their specialist knowledge and also as a way to understand each other's regulatory approaches in practice;
- Communicating proactively with other EDPB supervisory authorities on emerging issues that could impact a relatively high number of people in the EEA;
- Exercising our powers and reaching decisions in a fair, impartial and transparent manner;
- Clarifying the Irish legal environment for other EDPB supervisory authorities, so that a distinction can be made between consistent regulation of data protection law and valid differences in procedures and administration at a national level;
- Engaging with data protection authorities from outside the EEA, directly, within established international fora and at conferences, to understand the differences in data protection laws, and how those differences impact people and organisations;
- Collaborating with other EDPB supervisory authorities and the EU Commission on international cooperation with data protection authorities outside the EEA;[14]
- Participating in and speaking at conferences and other events in Ireland and abroad, so that our regulatory approach is understood, and so that we can understand the differences in regulatory approach in other countries, including in how this affects people and organisations;
- Responding to requests for information and interviews from international media outlets, so that the DPC's regulatory approach can be understood by the widest international audience possible, including those people outside Ireland who are affected by the DPC's regulation;
- Providing a comprehensive account of our regulatory activity in our annual report that is published as soon as possible after the end of each year.

Consultation Question 2

Which of the DPC's activities have the greatest effect on achieving the target outcome on consistent regulation?

[13] The One Stop Shop model is explained in the appendix of this document.
[14] The specific steps on international cooperation are set out in Article 50 of the GDPR.

Outcome 2

There is clarity and certainty in how data protection law is applied.

One of the reasons for developing the GDPR as a new EU-wide regulation was to provide legal certainty[15]. And the GDPR in itself has achieved that to a great extent.

However, **the GDPR is based on principles**. It does not set out legal requirements for specific contexts or technologies. Therefore, the GDPR must be interpreted carefully every time it is applied to those specific contexts or technologies. Many of the rights and obligations in the GDPR are not new to data protection law. However, as technology and society continue to change, data protection law must be interpreted and applied.

That is why we have identified that achieving clarity and certainty in how data protection law is applied is a target outcome in itself. This ideal future state would provide stability for organisations and people. **Compliance is much likelier when the application of the law is clear and understood.** We especially want to help those organisations that want to be compliant and accountable but are not sure how to go about it.

The DPC is only one of many organisations and bodies working towards this target outcome. The Courts, and especially the Court of Justice of the EU, and the EDPB are key players in working towards legal clarity and certainty in how data protection law is applied. However, even though we are just one player amongst many, we want to do as much as possible to accelerate this clarity and certainty being achieved.

These are the activities that the DPC undertakes to achieve this target outcome.

- Providing guidance to people so they are clear on how the law supports them in controlling the use of their personal data, so they are clear in how to exercise their data protection rights;
- Using a mix of formats and tools to deliver information, and prioritising the information that is needed by the most people, or that could have the biggest impact, or that could assist the most vulnerable;
- Providing guidance and case studies aimed at organisations on how data protection law should be applied both in general and in specific contexts, and prioritising the information we provide according to areas of non-compliance that we identify, or that could have the greatest impact in improving protections while still enabling innovation, service delivery and commercial gain;
- Responding to common or specific misunderstandings of how data protection law is applied via guidance, blogs and the media;
- Contributing to the development of EDPB guidelines and opinions, in support of consistent interpretation and application of the GDPR;

[15] Recital 13 of the GDPR.

- Publishing research on how data protection law applies to rapidly-changing technologies, on questions of wider legal impacts, and on changing business models, including through research partnerships;

- Taking full account of all relevant judgments of the Courts, including the Court of Justice of the EU, on how data protection law should be applied in our guidance, information, complaint handling, investigations and decision-making;

- Assessing how an inquiry into a potential infringement might clarify how specific obligations apply to a particular context, when preparing for the scoping and commencement of that inquiry;

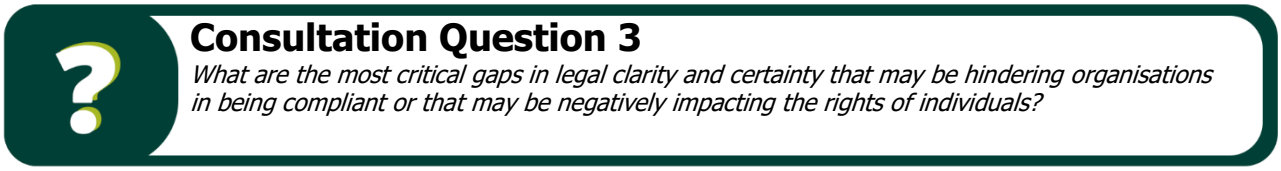
- Publishing summary and detailed information about our decisions where it is appropriate, useful and in the public interest, and taking advantage of opportunities to explain those decisions via the media, so that the application of the law can be understood by people and organisations;

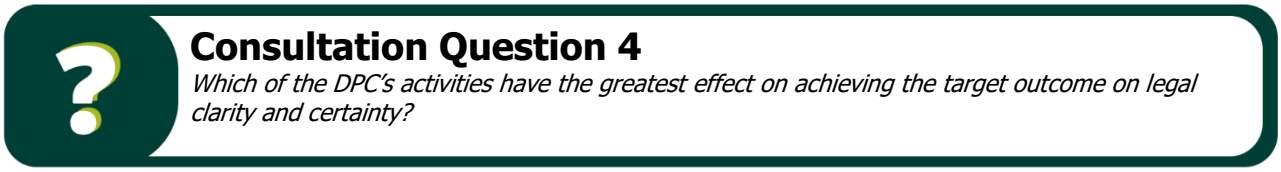
- Initiating litigation when we are obliged to do so, for example, on interpretation of EU law or when decisions of the European Data Protection Board arising from disputes on our own decisions could provide a lack of certainty in our view;

- Participating in discussion on issues that do not fall directly under data protection law but that are closely linked or intersect with data protection, particularly where there may be gaps in the law, in protections or in regulation, and collaborating with regulators in those linked areas, for example, digital safety, competition and consumer protection;

- Responding to requests for information and interviews from media outlets, so that the application of the law is understood by the widest audience possible, especially those who are affected by the DPC's regulation;

- Assessing potential changes to data protection law and providing well-balanced and thorough submissions to legislators when invited to do so, for example on the impact of the new draft EU Regulation on ePrivacy.





Outcome 3

Organisations operate and innovate in an accountable, compliant, ethical and fair way in their processing of personal data.

Data protection law and its regulation most definitely do not stand in the way of technology progress.[16] There is no binary choice that needs to be made between protecting personal data and using technology - for example, to enhance our lives, to enable breakthroughs in healthcare, to respond to humanitarian crises and even just to socialise.

Furthermore, data protection law and its regulation in the EU do not seek to undermine the freedom to conduct a business.[17] Neither do data protection law and its regulation have as their primary purpose the curtailing of public services that people and society need. However, in delivering products and services, organisations must take accountability for how they process personal data. They can do this by following the fundamental principles for personal data protection under the GDPR, which are set out in the appendix.

The DPC supervises how organisations take accountability for meeting these principles. Our legal framework, and the fact that data protection is a fundamental right, means that we have a different regulatory approach to many other regulators, for example, regulators that supervise economic activity and from whom organisations must seek pre-approval. We have a multi-pronged approach to our supervision – ranging from raising awareness to influencing to advising to authorising to monitoring to investigating to enforcing to prosecuting.

These are the activities that the DPC undertakes to achieve this target outcome.

- Providing guidance aimed at organisations on how data protection law should be applied both in general and in specific contexts, and prioritising the information we provide according to areas of non-compliance that we identify, or that could have the greatest impact in improving protections while still enabling innovation, service delivery and commercial gain, for example, guidance aimed at start-ups;
- Refining our methods for planning, developing and publishing guidance and tools, and measuring the concrete impact of our guidance in terms of how it increases understanding and compliance;
- Publishing detailed case studies of our decisions in a format that helps organisations to understand how the decisions apply to their own processing of personal data, and so reinforce their accountability and improve their compliance;
- Prioritising the development of guidance for micro, small and medium sized enterprises, ensuring that the guidance is as practical and clear as possible, with the aim that organisations generally don't require external advice on their compliance and accountability once they follow our guidelines;

[16] Recitals 4 to 7 of the GDPR explain that technological and societal developments need to be supported by a strong, coherent data protection framework.
[17] Article 16 of the EU Charter of Fundamental Rights.

- Prioritising the development of guidance and materials for designated Data Protection Officers[18], providing ways for DPOs to network and share information with each other, and engaging with DPOs directly in recognition of their critical role in organisations' accountability;

- Participating in and speaking at conferences and other events, in Ireland and abroad, so that we can directly explain to and influence as many organisations as possible how they can be compliant with data protection law, and process personal data fairly and ethically;

- Conducting detailed research on how data protection law applies to rapidly-changing technologies, on questions of legal analysis, and on changing business models, both internally and through research partnerships, and publishing the findings of that research in formats that help organisations to be compliant and to manage risks;

- Implementing the building blocks for organisations to demonstrate their compliance voluntarily through codes of conduct, by publishing the relevant criteria as quickly as possible and in line with EDPB guidelines, by engaging in discussions on proposed codes of conduct, and by reviewing draft codes of conduct as quickly and thoroughly as possible so that they can be applied by organisations;

- Implementing the building blocks for organisations to demonstrate their compliance voluntarily through certification schemes, by working closely with the Irish National Accreditation Board (INAB)[19] on accreditation criteria, by promoting the development of certification schemes, and by engaging directly with certification bodies as needed, so that certification schemes are available to organisations as soon as possible;

- Bearing a significant regulatory load on behalf of people across the EEA, by supervising, investigating and enforcing against the technology, internet and social media companies that have their European headquarters in Ireland;

- Assigning expert resources to help organisations understand their accountabilities when transferring personal data outside the EEA through guidance and direct advice, reviewing draft applications for Binding Corporate Rules as quickly and as thoroughly as possible, authorising personal data transfers via specific mechanisms, and seeking clarity on how transfers potentially affect individuals;

- Responding to requests from Government departments for consultation with the DPC on potential changes to legislation that relates to the processing of personal data;

- Responding to requests from organisations that have completed data protection impact assessments (DPIAs) and have not been able to mitigate all high risks to the processing of personal data, within the response timelines set out in the GDPR;

- Engaging with organisations directly on their approach to data protection compliance, particularly with those organisations that process the personal data of a

[18] Certain organisations are required to appoint a Data Protection Officer, under Article 37 of the GDPR, and the tasks of the Data Protection Officer are set out in Article 39 of the GDPR.
[19] The Irish National Accreditation Board is the accreditation body for certification schemes in Ireland, under the Data Protection Act 2018.

significant number of people, as a way to understand their business models and proactively identify potential issues before they happen, and measuring the concrete impact of our engagement efforts;

- Acting quickly when we become aware of a potential new product and service being introduced by an organisation, that could have a negative effect on a large number of people, and ensuring that the product or service is changed before it is even introduced, either through discussions with the organisation or through formal enforcement action such as a warning;

- Responding swiftly and in the most appropriate way to notifications we receive from individuals as protected disclosures;[20]

- Reviewing every notification and complaint of a personal data breach that we receive, examining the risks to people's rights and freedoms that could result from the breach, identifying trends and systemic issues, and pursuing formal investigations of specific breaches or groups of breaches depending on their nature and gravity;

- Confirming and regularly communicating our short to medium term enforcement priorities, according to the key areas of risks that we identify;

- Pursuing investigations into potential infringements that we identify could have a relatively significant effect on a large number of people, both in Ireland and in the EEA, and publicly confirming the existence of those investigations when we identify that this confirmation can be a deterrent to non-compliance by other organisations;

- Conducting our investigative and decision-making processes in a way that complies with the principles of natural justice and fair procedures, and making determinations and decisions in a rational, reasoned and transparent manner;

- Using all of our investigative powers to maximum effect and applying every power that is necessary for a given investigation, so that we can confirm the full set of facts as efficiently and quickly as possible, both during a formal inquiry and also in non-inquiry contexts;

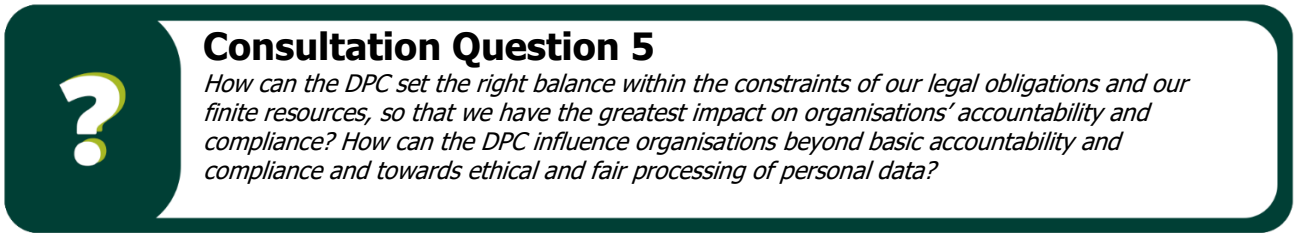
- Taking account of the deterrent effect that our corrective powers can have when we are determining the most appropriate corrective power, including fines, for each decision that finds an infringement;

- Assessing what is a proportionate corrective power for every specific infringement, based on the facts of that case and the findings in our decision, while still maintaining the consistency of our regulatory approach;

- Taking account of the deterrent effect that our corrective powers can have, in terms of impact on other organisations, when we are determining the most appropriate corrective power, including fines, for each decision that finds an infringement;

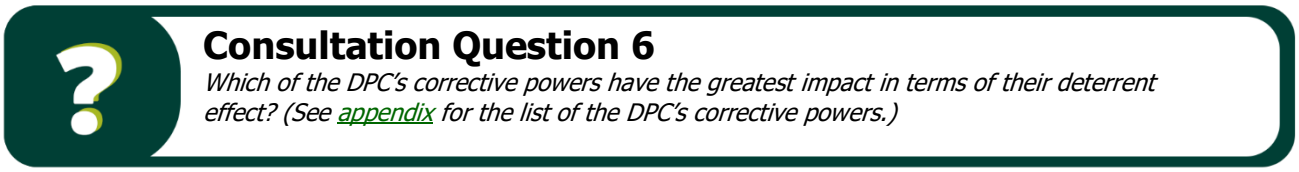
[20] The DPC is included under Section 7 of the Protected Disclosures Act and Statutory Instrument 339 of 2014. This means that employees may make protected disclosures to the DPC relating to compliance with data protection law.

- Exercising our prosecution powers when we find infringements relating to electronic communications under ePrivacy Regulations or offences under the Data Protection Act 2018, in a fair and transparent manner;
- Defending our decisions robustly in the Courts.



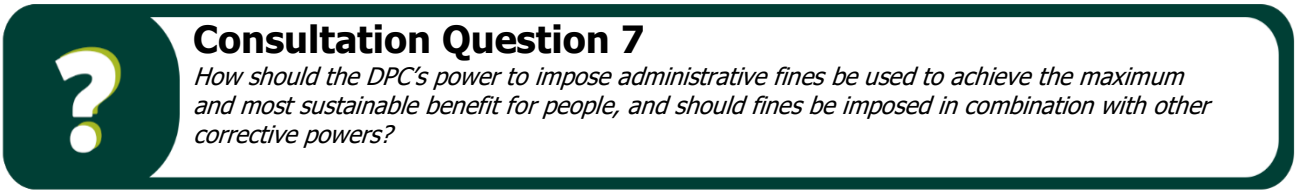
Consultation Question 5

How can the DPC set the right balance within the constraints of our legal obligations and our finite resources, so that we have the greatest impact on organisations' accountability and compliance? How can the DPC influence organisations beyond basic accountability and compliance and towards ethical and fair processing of personal data?



Consultation Question 6

Which of the DPC's corrective powers have the greatest impact in terms of their deterrent effect? (See appendix for the list of the DPC's corrective powers.)



Consultation Question 7

How should the DPC's power to impose administrative fines be used to achieve the maximum and most sustainable benefit for people, and should fines be imposed in combination with other corrective powers?

Outcome 4

As many people as possible understand and have control over how their personal data is used.

For each of us, our understanding and control of how our personal data is used is central to our control of our own lives. This is why our data protection rights are so important. Transparency in how our information is used and in the choices we have is critical. Transparency is not just about building trust. Our right to be able to access the information stored about us, and our rights to have that information corrected or erased, provide us with some further control. This is why organisations must be transparent in how they use our personal data, under the GDPR.

Every day at the DPC, **we are motivated and energised by our core purpose of safeguarding these rights that each of us has** - protection of personal data is a fundamental right. We want every person who has a concern or an issue or a complaint to be supported in their rights being upheld and in getting a satisfactory resolution.

- We want to provide as many people as possible with useful information on their rights.
- For people who contact us directly with questions, we provide support with our immediate advice – receiving advice and getting a better understanding of rights and obligations can be a stepping stone towards getting control over personal data.
- In other cases, we may contact an organisation directly when someone has raised an issue with us. Often, just one contact from us can resolve the original issue for the person.
- For some other cases, we do more extensive work in handling a complaint and reach a more formal conclusion on that complaint.

Many thousands of people contact us every year with questions, concerns and complaints about their own individual circumstances, and we sincerely want to get a satisfactory resolution for every one of those people. But we also want to improve the protections for the millions of people who have not contacted us but whose rights may have been infringed by different organisations on a large scale. For some complaints, we identify that the alleged interference in rights does not justify further extensive effort by us, given our limited resources. Regardless of how much work we do on an individual complaint, we always explain our reasons for concluding the case, once we identify that our work on that case is complete.

At the DPC, we want to achieve as much as possible for as many people as possible. This is why we need to constantly make sure that our work on individual complaints is balanced with our work on issues that can affect millions of people.

These are the activities that the DPC undertakes to achieve this target outcome.

- Raising the awareness of the public on how they can control the use of their personal data and on their data protection rights, through advertising campaigns, public information sessions, and via representative groups;

- Responding to requests for information and interviews from media outlets, so that awareness is raised on data protection rights, obligations and misconceptions, especially amongst people who may not have sought this out themselves;

- Providing useful guidance to people, as a practical way to support them in controlling the use of their personal data, in managing risks to their personal data, and in exercising their data protection rights, using a mix of formats and tools to deliver the information, and prioritising the information that is needed by the most people, so that they do not need to contact us directly;

- Responding as quickly as possible with directly relevant information to people who do need to contact us with questions on their own specific circumstances;

- Advising people of other avenues that they could use to get information and potentially get a better outcome for their case, including via regulators working in other areas of the law;

- Taking account of how data protection impacts vulnerable people, monitoring how organisations meet their data protection obligations in a way that considers the circumstances of vulnerable people, and seeking input from special interest groups that represent vulnerable people to assist with our own understanding;

- Completing sufficient assessment of each individual complaint received by us, to identify the most appropriate and fastest way to handle and conclude that case, and communicating the basis for our approach to the complainant, in a way that can be easily understood;

- Concluding as many complaints as possible by amicable means[21], for example, by seeking that the organisation involved fulfil the complainant's rights without the need for enforcement action to achieve that specific fulfilment, while still potentially pursuing the issue with the organisation if there are potential systemic problems identified;

- Acting quickly when we become aware of a potential new product and service being introduced by an organisation, that could have a negative effect on a large number of people, and ensuring that the product or service is changed before it is even introduced, either through discussions with the organisation or through formal enforcement action such as a warning;

- Identifying trends and themes across groups of individual complaints, and pursuing investigations that cover the main issues in those groups of complaints, so that we can achieve strong collective outcomes as efficiently as possible within our finite resources;

- Pursuing investigations into potential infringements that we identify could have a relatively significant effect on a large number of people, both in Ireland and in the EEA, even when we have not received many or any complaints about the issue.

Consultation Question 8

How can we set the right balance between our work on individual complaints and our work on issues that can affect millions of people, so that we have the greatest impact for as many people as possible?

[21] As set out in Section 109(2) of the Data Protection Act 2018.

Outcome 5

Children are specifically protected.

At the DPC, we are driven by our core purpose of safeguarding the data protection rights that each of us has. We are especially passionate about safeguarding the rights of vulnerable people and most particularly the rights of children.

The GDPR is very clear that children need specific protection when it comes to personal data as they may be less aware than adults of the risks and consequences[22]. Not only are children vulnerable when it comes to their data protection rights, if a child's data protection rights have not been met, the negative impact could have a long-term effect into adulthood.

These are the activities that the DPC undertakes to achieve this target outcome.

- Defining the specific protections required to safeguard the rights of children in the protection of their personal data, and providing guidance for people and organisations;
- Providing ready-to-use education materials and raising awareness on children's data protection, aimed at children, their teachers and their parents;
- Conducting detailed research on how data protection law applies to children, both internally and through research partnerships, for example, on how age verification methods could be deployed safely and on how parental consent can be obtained for online services;
- Collaborating with and drawing from the advice and experiences of advocates and experts in the field of protection and promotion of children's rights, including other regulators and statutory bodies;
- Initiating and actively promoting the development of codes of conduct on the processing of children's personal data;
- Pursuing formal investigations, decision-making and applying corrective powers related to potential infringements that could impact children's data protection rights as a critical priority for DPC enforcement.

Consultation Question 9

Which of these activities are likely to have the greatest effect on achieving the target outcome of ensuring that children are specifically protected? Is there an order in which these activities should be prioritised?

Consultation Question 10

Are there any other actions that the DPC should be undertaking that will help us to achieve our target outcome of ensuring that children are specifically protected?

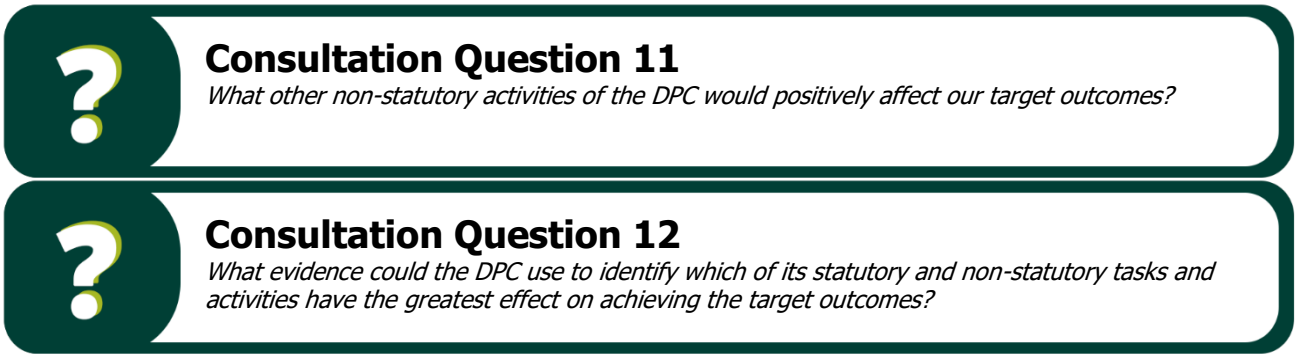
[22] Recital 38 of the GDPR.

Conclusions

Our target outcomes are ambitious, especially considering that we do not have unlimited resources. At the same time, we have an extensive set of tasks, activities and functions that we must perform by law.

We want to be as deliberate as possible in examining how we can use our resources to best effect to address the greatest risks for the most people. As we develop our new Regulatory Strategy for the period 2020 to 2025, we will be examining and testing the concrete connections between our activities and the outcomes that we want to achieve. As far as possible, we want to use evidence to make the hard choices we face on our regulatory priorities, while still delivering our legal obligations.

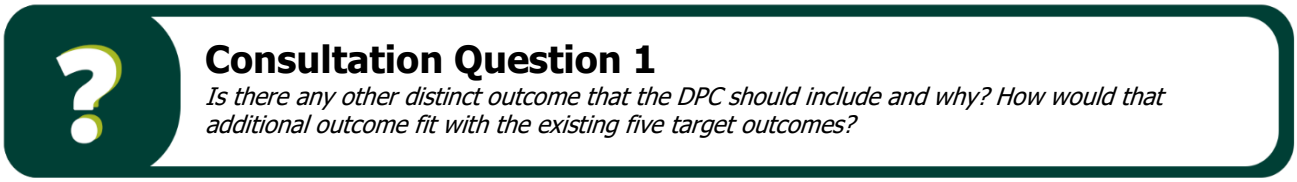
We will be assessing what other activities we could undertake to help achieve those outcomes and we will also be examining how our different activities affect each other. The submissions we receive during this first round of open public consultation are important to our full assessment.



5. All Consultation Questions

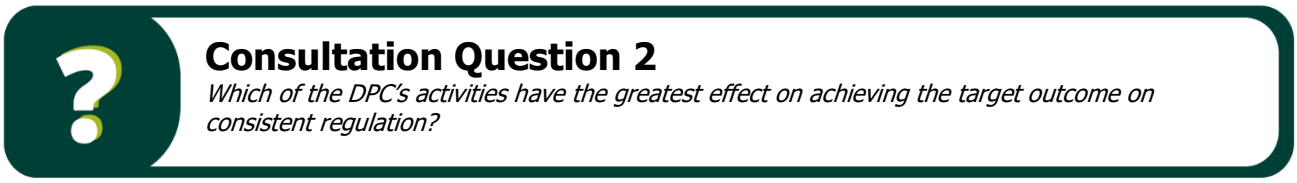
The questions to which responses are requested, via written submissions to the DPC, are set out throughout Section 4 of this document. All of those questions are listed again together here.

Responses are invited to one, many or all of these questions. Submissions can be emailed to dpcstrategy@dataprotection.ie or posted to DPC Strategy, 21 Fitzwilliam Square, Dublin 2, before 24 January 2020.



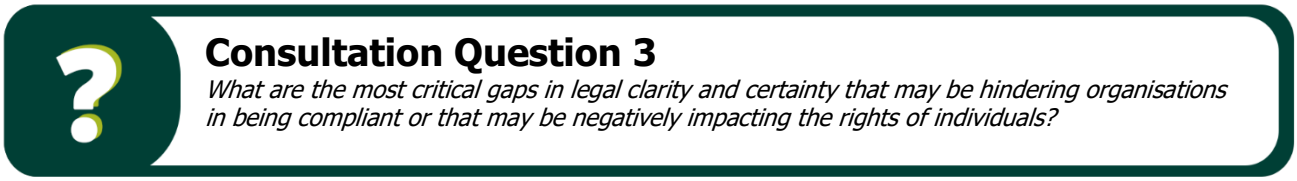
Consultation Question 1

Is there any other distinct outcome that the DPC should include and why? How would that additional outcome fit with the existing five target outcomes?



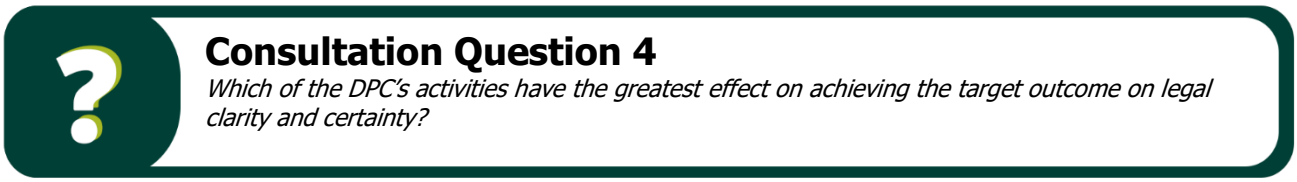
Consultation Question 2

Which of the DPC's activities have the greatest effect on achieving the target outcome on consistent regulation?



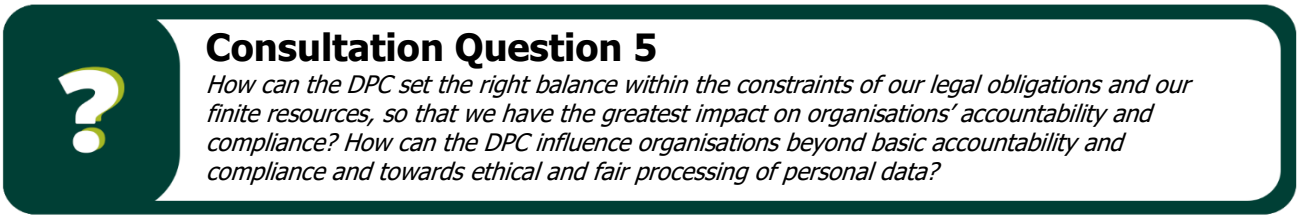
Consultation Question 3

What are the most critical gaps in legal clarity and certainty that may be hindering organisations in being compliant or that may be negatively impacting the rights of individuals?



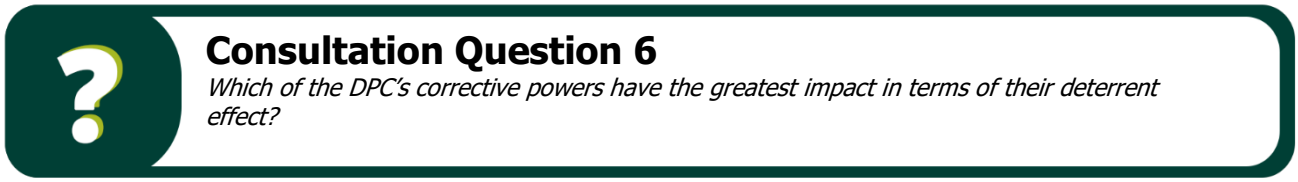
Consultation Question 4

Which of the DPC's activities have the greatest effect on achieving the target outcome on legal clarity and certainty?



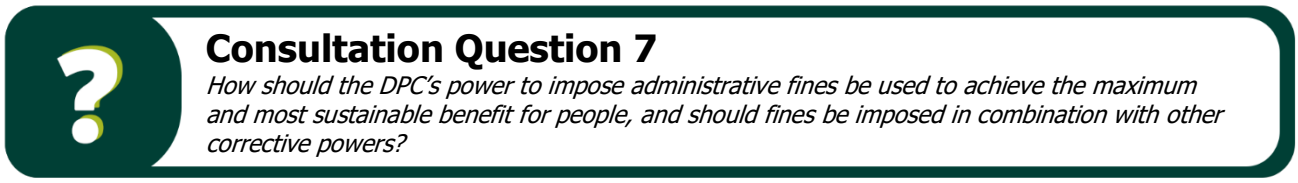
Consultation Question 5

How can the DPC set the right balance within the constraints of our legal obligations and our finite resources, so that we have the greatest impact on organisations' accountability and compliance? How can the DPC influence organisations beyond basic accountability and compliance and towards ethical and fair processing of personal data?



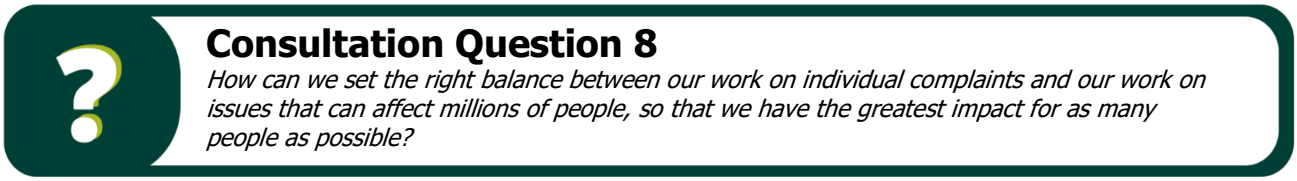
Consultation Question 6

Which of the DPC's corrective powers have the greatest impact in terms of their deterrent effect?



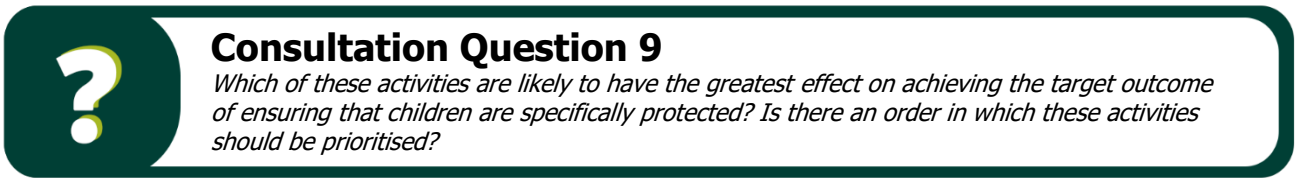
Consultation Question 7

How should the DPC's power to impose administrative fines be used to achieve the maximum and most sustainable benefit for people, and should fines be imposed in combination with other corrective powers?



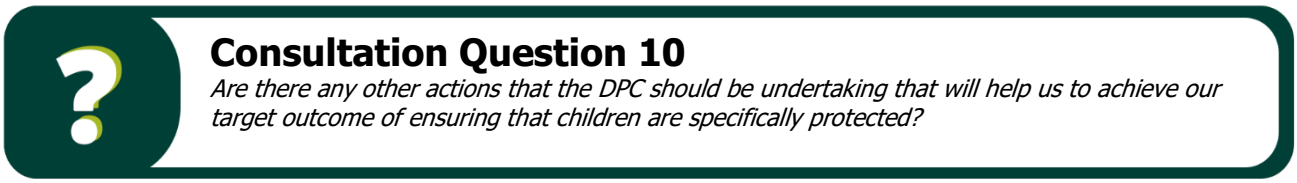
Consultation Question 8

How can we set the right balance between our work on individual complaints and our work on issues that can affect millions of people, so that we have the greatest impact for as many people as possible?



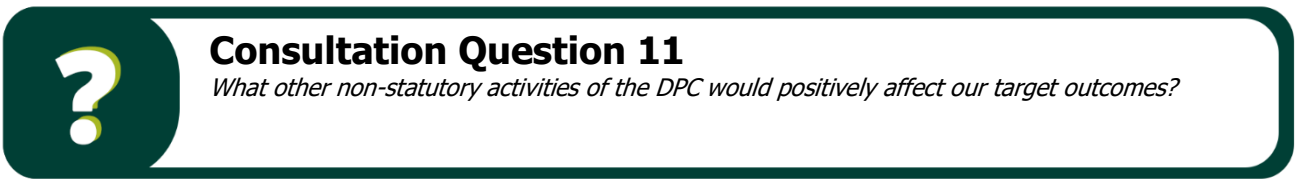
Consultation Question 9

Which of these activities are likely to have the greatest effect on achieving the target outcome of ensuring that children are specifically protected? Is there an order in which these activities should be prioritised?



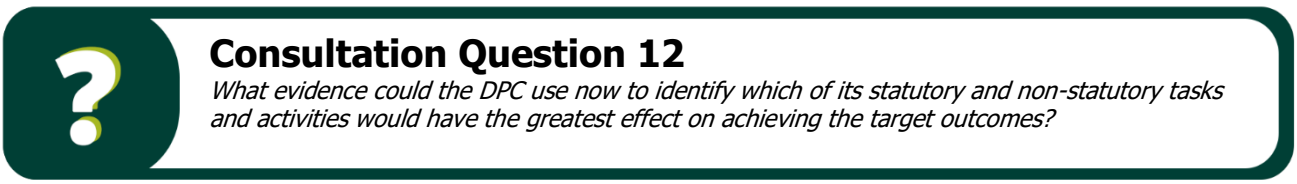
Consultation Question 10

Are there any other actions that the DPC should be undertaking that will help us to achieve our target outcome of ensuring that children are specifically protected?



Consultation Question 11

What other non-statutory activities of the DPC would positively affect our target outcomes?



Consultation Question 12

What evidence could the DPC use now to identify which of its statutory and non-statutory tasks and activities would have the greatest effect on achieving the target outcomes?

6. Further Information

Planned publication sequence

We are planning three main sets of publication, in the course of developing our new Regulatory Strategy.

Set A
- Target Outcomes (this document)
  - *There will be open public consultation on this document*

Set B
- *Draft* DPC Regulatory Strategy 2020-2025
  - *There will be open public consultation on this document*
- Summary analysis report from the first round of public consultation

Set C
- *Final* DPC Regulatory Strategy 2020-2025
- Strategy Implementation and Measurement Plan
- Summary analysis report from the second round of public consultation
- Review of DPC Statement of Strategy for 2019

The Strategy Implementation and Measurement Plan will set out how the strategic priorities will be implemented, including through key projects and initiatives. The Plan will also set out how the impact to our target outcomes will be measured. This measurement approach will need to take account of other events, influences and organisations that also have positive impacts on the target outcomes of the DPC.

During the coming months, while the DPC's Regulatory Strategy is being developed, we will also publish a guide for organisations and individuals on the DPC's regulatory procedures.

Other consultation

The DPC has already held some focus groups with members of the public. We ran these focus groups to try to understand the views of the public on:
- *Data protection rights;*
- *How compliance with data protection law should be encouraged, facilitated and maximised and how non-compliance should be regulated;*
- *The role of the DPC.*

The understanding we gained from those focus groups has been taken into account in our five target outcomes. We may run further focus groups, depending on the submissions we receive to this first round of public consultation.

As well as seeking submissions via the two planned rounds of public consultation, we also plan to seek further direct input as we prepare our draft Regulatory Strategy. For example, we will be engaging informally with the organisations and people we interact with anyway in the course of our work, on the draft Regulatory Strategy. We may also consult specifically with representative bodies, advocacy groups and other organisations, based on the submissions we receive from this first round of public consultation. We will also engage with other data protection authorities and regulators in other spheres.

Principles of data protection

At a minimum, the GDPR provides for certain overarching obligations which must be met by organisations that 'process' (or in other words, use or handle) personal data in all its forms. The fundamental principles which must be met when processing personal data are set out in Article 5 of the GDPR as follows.

- *Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;*
- *Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;*
- *Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;*
- *Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;*
- *Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;*
- *Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and*
- *Finally, the controller is responsible for, and must be able to demonstrate, their compliance with all of the principles above of data protection - accountability.*

Relevant legislation

Legislation that sets out the DPC's tasks, powers and regulatory obligations is as follows.

i. General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
ii. Data Protection Act 2018
iii. Data Protection Acts 1988 to 2003
iv. ePrivacy Regulations (Statutory Instrument No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011)
v. The "Law Enforcement Directive" (Directive (EU) 2016/680) transposed into Irish law by way of the Data Protection Act 2018

There are several other pieces of primary legislation which are not principally concerned with data protection functions but where a function or responsibility is attributed to the DPC.

Tasks and powers of the DPC

Article 57(1) of the GDPR sets out the **tasks** of each supervisory authority in the EU, including the DPC. These are as follows.

(a) monitor and enforce the application of this Regulation;
(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;
(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
(d) promote the awareness of controllers and processors of their obligations under this Regulation;
(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;
(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;
(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);
(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);
(l) give advice on the processing operations referred to in Article 36(2);
(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
(p) draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(r) authorise contractual clauses and provisions referred to in Article 46(3);
(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;
(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
(v) fulfil any other tasks related to the protection of personal data.

Article 58 of the GDPR sets out the **powers** of each supervisory authority in the EU, including the DPC. These are as follows.

(1) Investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
(b) to carry out investigations in the form of data protection audits;
(c) to carry out a review on certifications issued pursuant to Article 42(7);
(d) to notify the controller or the processor of an alleged infringement of this Regulation;
(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

(2) Corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
(e) to order the controller to communicate a personal data breach to the data subject;
(f) to impose a temporary or definitive limitation including a ban on processing;
(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

(3)<u>Authorisation and advisory powers:</u>

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;
(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;
(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);
(e) to accredit certification bodies pursuant to Article 43;
(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);
(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
(h) to authorise contractual clauses referred to in point (a) of Article 46(3);
(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);
(j) to approve binding corporate rules pursuant to Article 47.

One Stop Shop Model under the GDPR

The objective of the One Stop Shop (OSS) model is to streamline how organisations that do business or carry out their activities in more than one EU member state deal with data protection authorities (DPAs), called 'supervisory authorities' in the GDPR. The OSS means that organisations with multiple bases across different member states of the EU are overseen by just one DPA when it comes to supervision of the organisation's 'cross-border processing'. This is the DPA where the organisation has its 'main establishment' in the EU. The main establishment of an organisation will generally be its place of central administration (e.g. its headquarters).

Under the GDPR, cross-border processing involves one of two scenarios. The first is where an organisation has bases or establishments in more than one member state and processing takes place in the context of the activities of more than one such establishment. The second scenario is when an organisation is based or established in just one member state but the processing substantially affects, or is likely to substantially affect, people in more than one member state. In either of those scenarios, the concept of the 'lead supervisory authority' under the GDPR will apply to determine the DPA that has primary responsibility for oversight of that organisation, for example, in dealing with a complaint on its cross-border processing.

Under the rules of the GDPR, the organisation is only subject to the regulatory actions of the DPA who is its lead supervisory authority rather than multiple actions by different data protection authorities of different member states, in the event of an infringement.

The role of the DPA who is the lead supervisory authority includes investigating a complaint or alleged infringement of the GDPR relating to cross-border processing and preparing a draft decision on the matter. It then must coordinate, where possible, a consensus decision with other EU data protection authorities who are deemed to be 'concerned supervisory authorities'.

This means that the lead supervisory authority must not only take 'utmost account' of the views of the DPA which received the complaint when preparing a draft decision, but also then share its draft decision with all concerned supervisory authorities and consult with, and consider their views, in finalising the decision. Where this is not possible, the GDPR provides for a dispute-resolution mechanism to be triggered that will ultimately result in the members of the EDPB making a majority decision on the disputed issues in the draft decision.

Under the OSS mechanism, the DPC is the lead supervisory authority for a broad range of multinationals, including many large technology and social media companies, whose main establishment is located in Ireland. As a lead supervisory authority, the DPC now handles complaints originally lodged with other EU data protection authorities, in addition to handling complaints that people lodge directly with the DPC.

Irish Human Rights and Equality Commission Act 2014

The DPC's obligations under Section 42 of the Irish Human Rights and Equality Commission Act 2014 are summarised as follows.

(1) A public body shall, in the performance of its functions, have regard to the need to—
- (a) eliminate discrimination,
- (b) promote equality of opportunity and treatment of its staff and the persons to whom it provides services, and
- (c) protect the human rights of its members, staff and the persons to whom it provides services.

(2) For the purposes of giving effect to subsection (1), a public body shall, having regard to the functions and purpose of the body and to its size and the resources available to it—
- (a) set out in a manner that is accessible to the public in its strategic plan (howsoever described) an assessment of the human rights and equality issues it believes to be relevant to the functions and purpose of the body and the policies, plans and actions in place or proposed to be put in place to address those issues, and
- (b) report in a manner that is accessible to the public on developments and achievements in that regard in its annual report (howsoever described).

An Coimisiún um Chosaint Sonraí
Data Protection Commission

An Coimisiún um Chosaint Sonraí
21 Cearnóg Mhic Liam, BÁC 2,
DO2 RD28, Éire

Data Protection Commission
21 Fitzwilliam Square, Dublin 2,
D02 RD28, Ireland