Submission to the Public Consultation on the DPC's Regulatory Strategy 2020-2025

ARTICLE EIGHT ADVOCACY

JANUARY 2020

TABLE OF CONTENTS

INTRODUCTION

Article Eight Advocacy is grateful to the Data Protection Commission for giving us this opportunity to provide submissions to this public consultation on the DPC's target regulatory outcomes.

We are a new advocacy group focussed on promoting and defending the fundamental right to data protection of individuals in Ireland, as set out in Article 8 of the Charter. We appreciate the vital work the DPC does in this hugely important area.

We have answered the questions posed by the DPC below, where appropriate. Our answers return regularly to some themes which are set out in this introduction.

For convenience citations are both inline and provided in a bibliography at the end of this document.

Never lose sight of the individual

"Do we focus on people with their dignity in all its many facets, or do we only see the customer, the data sources, the objects of surveillance?"[1]

- Data protection law exists to protect the rights and freedoms of individuals, preserve their dignity and extend the amount of control they have over the uses to which their personal data is put. **"The protection of natural persons in relation to the processing of personal data is a fundamental right."** (Recital 1, GDPR)
- The right of access and the right to information are pivotal to proper functioning of the European data protection regime. Without these all other rights are effectively unavailable to data subjects, thwarting the intent of the law.
- It appears that many data controllers are not providing data subjects with the mandated information about processing of their personal data and failing to fully comply with access requests.

Enforcement must be visible

- This raises awareness and appreciation among the general public of the DPC's role as the primary advocate for the rights of data subjects, and which powers the DPC can deploy in support of data subjects.
- This also raises awareness among data controllers of their obligations and the risks they are accepting in carrying out certain processing activities or failing to allow data subjects to exercise their full suite of rights.

[1]Angela Merkel, Harvard graduation address, May 2019
https://www.americanrhetoric.com/speeches/angelamerkelharvardcommencementenglish.htm

Timeliness matters and administrative roadblocks must be removed

- There is a risk of poor practices within data controllers becoming encoded as normal behaviour. This refers both to data processing activities and interaction with data subjects who attempt to exercise their rights.
- The longer there is little visible enforcement activity as we approach the second anniversary of the GDPR coming into force the greater this risk becomes.

In achieving any desired enforcement outcome, emphasis must be placed on the fundamental rights of individuals and achieving the goals of the GDPR.

One of these goals is to reduce harm to individuals by curbing the excesses of data controllers. This can only be done through effective supervision and where necessary adjudication on complaints involving the violation of fundamental rights.

The marked power imbalance between controllers and data subjects is indisputable. Another goal of the GDPR is to rebalance this relationship between data controllers and data subjects to give data subjects more control over their personal data.

Under the pre-GDPR regime the supervisory model was to a certain extent a discourse between regulators and data controllers, with data subjects deprioritised. The GDPR aims to elevate data subjects (and their representatives) to a rightful equal status in this conversation.

The first responsibility of the supervisory authority is as set out in Article 51 GDPR is **"monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing"**.

Therefore the swift handling of complaints from data subjects must be prioritised and more transparency around enforcement and supervision activities should be provided.

In a speech given recently at the Croatian Presidency of the EU Council Conference entitled 'Data Protection Day 2020: Facing New Challenges' European Data Protection Supervisor Wojciech Wiewiórowski said there is now "*a platform of jurisprudence for re-engineering digital society according to our fundamental rights and freedoms. We only need to rise to the challenge.*"[2]

[2] Wojciech Wiewiórowski and EDPS, 'Data Protection Day 2020: Facing New Challenges', https://edps.europa.eu/sites/edp/files/publication/20-01-16_speech_zagreb_en.pdf

RESPONSES TO CONSULTATION QUESTIONS

We have answered questions only where we feel we have something to contribute. There is obviously some overlap between the target outcomes and the questions posed by the DPC so we have endeavoured to keep repetition of the same points to a minimum,

Q1: Other outcomes

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?

None. The overall outcome of the DPC's activities in their entirety should be as set out in Article 1 of the GDPR: that **all fundamental rights and freedoms of individuals are protected** while ensuring the free movement of personal data within the Union.

Q2: Consistent regulation

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

→ This relates to target outcome 1: Data protection rights and obligations are regulated consistently.

All fourteen of the activities listed are of value and all will contribute to the desired outcome. It is not possible to rank these in terms of effectiveness as all of them are necessary.

More **detailed information about regulatory activity should be made generally available**.

The DPC should **publish clear explanations of its procedures and processes**. To those not familiar with the supervisory model of European data protection the process can be unintuitive.

The DPC should also **publish decisions on complaints**, enforcement notices and results of audits on a regular, as it happens basis. In the case of decisions the reasoning used to arrive at these should be provided. Publication of a selection of case studies once per annum in the annual report is insufficient to achieve the target outcome. From a promotional perspective this is a 'once and done' approach which generates a limited amount of media coverage over a very short period of time. Regular and ongoing publication of materials will keep the DPC's activities in the public eye.

From the perspective of data subjects, a lack of available information on actions which have been

taken by the DPC **prevents them from effectively scrutinising the data protection practices of data controllers and making informed decisions** about which entities to share their personal data with.

As stated above, the lack of visible enforcement activity creates a vacuum in which non-compliant data protection practices can flourish and become established as norms.

Media outreach and event participation is important as there is still widespread misunderstanding of the basics of data protection law. Data protection is frequently confused with privacy and / or information security. There is a lack of awareness that data protection and privacy are separate and distinct fundamental rights in the Charter.

All the different mechanisms for **international cooperation and collaboration** are necessary in ensuring consistency in regulation across Europe, one of the key aims of the GDPR.

Q3: Legal clarity and certainty - gaps

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?

→ This relates to target outcome 2: There is clarity and certainty in how data protection law is applied

Clarity and certainty for organisations

Being based around principles and risk, data protection law is highly context dependent. It is therefore difficult to point to definite gaps in legal clarity which may be causing organisations compliance problems without discussing specific cases. However, it is our experience that the **levels of understanding of basics** such as access rights and exemptions to these, the provision of information to data subjects, and transparency and accountability are still **low in many controllers**.

How organisations behave on the ground is still being shaped after the introduction of the GDPR, and often in ways that are not helpful to data subjects. There is a widespread tendency to throw up bureaucratic blockages to make it more difficult for individuals to exercise their rights. In many situations risk still appears to be assessed as risks to the organisation rather than risks to the rights and freedoms of individuals.

> *"Having interpreted privacy law for their corporate employers and framed corporate privacy obligations in terms of risk rather than substantive privacy protections for users, compliance professionals create structures, services, and technologies to comply with their version of the law"*[3]

[3] Ari Ezra Waldman, 'Privacy Law's False Promise', SSRN Scholarly Paper (Rochester, NY: Social Science Research

Controllers must understand they have obligations to data subjects and that if they fail to meet these obligations there will be swift enforcement action from the regulator. That there is currently little evidence of visible enforcement action more than eighteen months after the GDPR came into force may lead controllers to believe this is how things are going to continue.

Many controllers are creating obstacles which hinder, frustrate and in some cases prevent the exercise of data subject rights entirely. Whether this is by design, through ignorance of obligations or poor advice is immaterial. The result is what Waldman calls *"the use of process to undermine substance"*.[4]

This must be addressed by the DPC through investigative powers, corrective powers and guidance.

Clarity and certainty for individuals

The European data protection supervisory model relies on individuals to do extensive background work on their own, seeking out information and exercising their right of access in order to assess whether processing activities are compliant. This places a **high burden on individuals** who in many cases will not be familiar with the workings of this system.

> *Data protection's supervisory model is quite unlike that for medical devices or financial services. Nobody expects a patient to check the reliability of a pacemaker before it is inserted into their heart or stress test a bank before they open a current account. And so the law does not provide patients and bank customers with tools that they would need to undertake such checks. Data protection is different: it expects that data subjects will do their own research and make their own decisions. The GDPR provides subjects with the tools to undertake those tasks. Subjects have the right to access their data, object to its processing, seek rectifications and corrections. These rights are not new. Similar rights were to be found in the GDPR's predecessors, the Strasbourg Convention and Directive 95/46. The difference is that the GDPR provides real supervisory and enforcement mechanisms to ensure that these rights can be successfully invoked.*[5]

The right of access is pivotal

If the right of access cannot be exercised **"easily"** (Recital 63, GDPR) then data subjects are frustrated before they can make any further inquiries about whether their data is being processed in a compliant manner, as shown below. This can understandably lead to **confusion, frustration and feelings of disempowerment**, which is especially disappointing for individuals when one of the promises of the GDPR was returning control over their personal data to individuals.

We note from the DPC's 'Response to the Public Accounts Committee, following appearance on

Network, 6 December 2019), page 31, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3499913

[4] Ari Ezra Waldman, 'Privacy Law's False Promise', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 6 December 2019), page 6, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3499913

[5] Denis Kelleher and Karen Murray, *EU Data Protection Law* (London: Bloomsbury Professional, 2018), para. 9.01.

26 September 2019'[6], submitted to the PAC on 18th October 2019 that the percentage of **complaints relating to the right of access** dwarf those relating to any other matter in 2018, **at 37.7% of the total**.

The IAPP survey 'What We Heard From Leading European Regulators'[7] says in reference to Ireland that "*2018's top complaint categories closely tracked those in prior years.*"

This indicates there are continuing significant problems with data subjects exercising their right of access, and that **data controllers are not complying with their obligations in this area**.

Issues around the right of access are not new, nor are they distinct to Ireland. Research from 2017 shows a general failure on the part of data controllers to satisfactorily handle access requests.

> *"During the first half of 2017, around sixty information society service providers were contacted with data subject access requests. Eventually, the study confirmed the general suspicion that access rights are by and large not adequately accommodated. The systematic approach did allow for a more granular identification of key issues and broader problematic trends. Notably, it uncovered an often-flagrant lack of awareness; organisation; motivation; and harmonisation."*[8]

Further research from 2019 - after the introduction of the GDPR - echoes this

> *The findings show that key objectives of EU law, to ensure businesses are transparent and clear about their use of peoples' data and that they meet and make it easy to exercise key rights, requires stronger oversight and enforcement of legal protections. Consumer and privacy organisations can help enforcement by continuing investigations and taking cases to court as necessary.*[9]

The diagram on the following page shows some common obstacles which data subjects encounter, the majority of them occurring before an access request can even be made.

The GDPR can only be as strong as its weakest link, and it appears that data subjects being unable to easily exercise the right of access is a particular pressure point within the system.

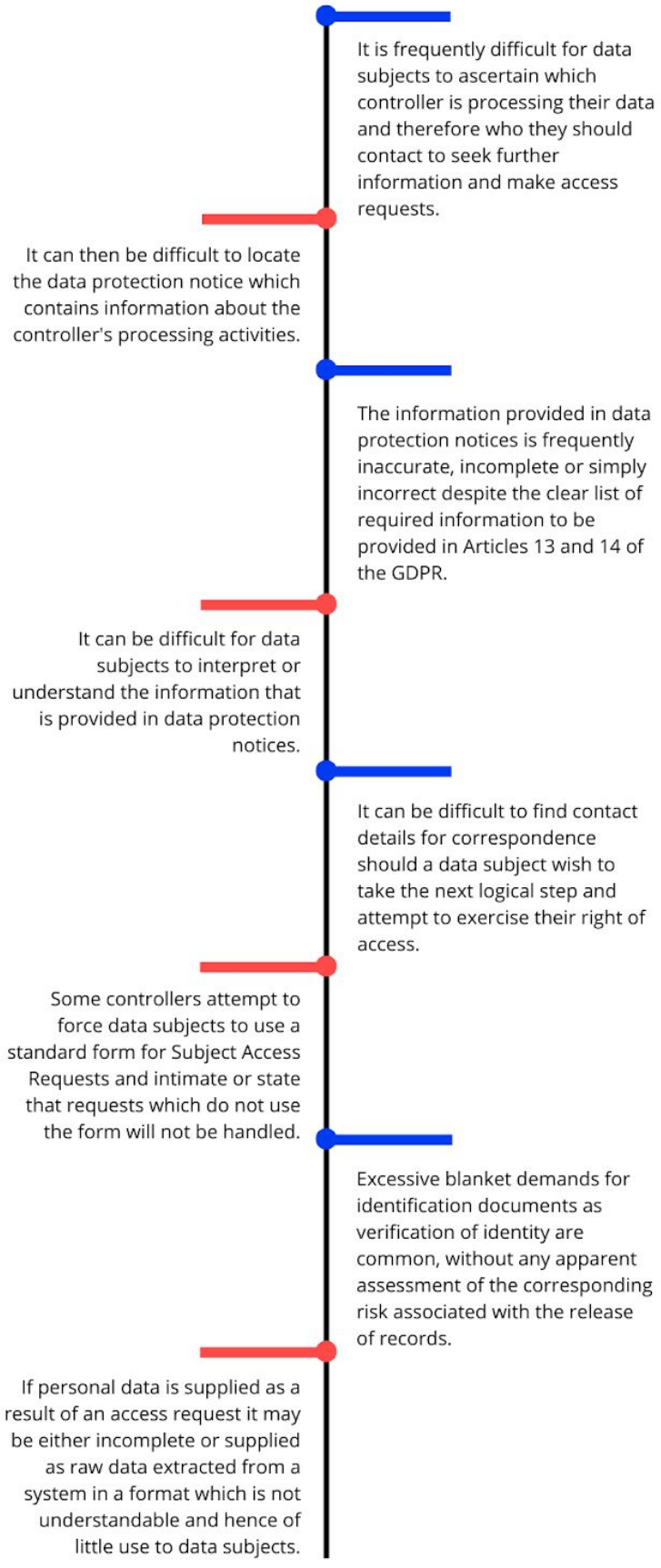
---

[6] Data Protection Commission of Ireland, 'Response to the Public Accounts Committee following appearance on 26 September 2019', https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/committee_of_public_accounts/submissions/2019/2019-12-31_correspondence-graham-doyle-head-of-communications-data-protection-commission-32r002486-pac_en.pdf

[7] Caitlin Fennessy, 'GDPR at One Year: What We Heard from Leading European Regulators', May 2019, https://iapp.org/media/pdf/resource_center/GDPR_at_One_IAPPWhitePaper.pd

[8] Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors. Data Subject Access Rights in Practice', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 20 January 2018), page 3, https://papers.ssrn.com/abstract=3106632

[9] Pat Walshe, Heinrich-Böll-Stiftung, and Transatlantic Consumer Dialogue, 'Privacy in the EU and US: Consumer Experiences across Three Global Platforms | Heinrich Böll Stiftung | Brussels Office - European Union', Heinrich-Böll-Stiftung, accessed 11 January 2020, page 8, https://eu.boell.org/sites/default/files/2019-12/TACD-HBS-report-Final.pdf


It is frequently difficult for data subjects to ascertain which controller is processing their data and therefore who they should contact to seek further information and make access requests.
It can then be difficult to locate the data protection notice which contains information about the controller's processing activities.
The information provided in data protection notices is frequently inaccurate, incomplete or simply incorrect despite the clear list of required information to be provided in Articles 13 and 14 of the GDPR.
It can be difficult for data subjects to interpret or understand the information that is provided in data protection notices.
It can be difficult to find contact details for correspondence should a data subject wish to take the next logical step and attempt to exercise their right of access.
Some controllers attempt to force data subjects to use a standard form for Subject Access Requests and intimate or state that requests which do not use the form will not be handled.
Excessive blanket demands for identification documents as verification of identity are common, without any apparent assessment of the corresponding risk associated with the release of records.
If personal data is supplied as a result of an access request it may be either incomplete or supplied as raw data extracted from a system in a format which is not understandable and hence of little use to data subjects.

Q4: Legal clarity and certainty - activities

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

→ This relates to target outcome 2: There is clarity and certainty in how data protection law is applied

All thirteen of these activities contribute to achieving the target outcome.

As stated above, we feel that **publication of a greater amount of more detailed material** relating to decisions made, investigations and other activities of the DPC will deliver a growing reference resource which can be consulted by data subjects and their representatives, data controllers, data protection officers and practitioners. This will be a valuable tool in achieving legal clarity and certainty over the time period concerned.

Additional **guidance for data subjects** as set out in the list of activities is extremely useful. In many cases the bureaucratic obstacles which have been constructed by data controllers discourage data subjects from exercising their rights or require them to seek legal or other representation to pursue relatively simple requests. This is not how the system was intended to function. Data subjects **should not require legal literacy** and/or legal assistance for the majority of their interactions with data controllers.

Debunking of common misinterpretations of data protection law is also of value since there is still widespread misunderstanding of the scope and aims of data protection law. Data protection is frequently confused with and conflated with privacy and information security by individuals, organisations and in the media.

Guidance for data controllers is of course valuable. Areas in which we see recurring misunderstandings include

- Basic obligations to data subjects, particularly concerning transparency, provision of information and the right to access, as discussed throughout this document.
- The principles of necessity and proportionality and how they apply to European data protection law.[10]
- The use of legitimate interests as a lawful basis. Controllers often cite legitimate interests without describing these legitimate interests or providing any evidence that the required balancing test has been carried out. Per Article 13.1(d) and Article 14.2(b) GDPR the legitimate interest being pursued by the data controller must be described and best practice requires some elements of the balancing test to be included.
- Misunderstanding of lawful bases in general.
- The scope of the accountability principle, discussed in more detail below.

[10] "Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.": CJEU joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, 9 November 2010, paragraph 50

Q5: Accountability, compliance, ethical and fair processing

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?

→ This relates to target outcome 3: Organisations operate and innovate in an accountable, compliant, ethical and fair way in their processing of personal data

In response to target outcome 3, there is **no binary choice between compliance and innovation**. This is a frequently-deployed industry canard. Compliance is not a hindrance to innovation. Organisations can innovate while being compliant.

> *A January 2019 survey from Cisco found numerous competitive advantages to entities that invested in privacy under the GDPR. That study also found that the two biggest challenges for companies under the GDPR were data security requirements and employee training. Data security requirements and employee training are basic and foundational privacy practices; the fact that these requirements have proven challenging is, itself, evidence of how cavalier companies have been with respect to data privacy.*[11]

Impact on organisations' accountability and compliance

Accountability is part of compliance, an overarching principle set out in **Article 5.2** and expanded on in **Article 24** of the GDPR. Without accountability a data controller cannot be compliant. Data *"controllers must be able to demonstrate compliance with data protection provisions to data subjects, the general public and supervisory authorities at any time."*[12]

This broad reach of the accountability principle does not seem to be fully understood by many data controllers.

> *According to the Article 29 Working Party's opinion*[13]*, the essence of accountability is the controller's obligation to*

[11] Joseph Jerome, 'The GDPR's Impact on Innovation Should Not Be Overstated', Center for Democracy and Technology (blog), 1 April 2019, https://cdt.org/insights/the-gdprs-impact-on-innovation-should-not-be-overstated/

[12] Europäische Union and Europarat, eds., *Handbook on European Data Protection Law*, 2018 edition, Handbook / FRA, European Union Agency for Fundamental Rights (Luxembourg: Publications Office of the European Union, 2018), page 137.

[13] Article 29 Working Party, 'Opinion on the Principle of Accountability', 2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

- *put in place measures which would - under normal circumstances - guarantee that data protection rules are adhered to in the context of processing operations; and*
- *have documentation ready which demonstrates to data subjects and to supervisory authorities the measures that have been taken to achieve compliance with the data protection rules.*

> *The principle of accountability thus requires controllers to actively demonstrate compliance and not merely wait for data subjects or supervisory authorities to point out shortcomings.*[14]

Further **guidance for controllers on accountability** would be welcome. Information campaigns targeted at controllers and explaining the broad reach of the accountability principle could be of use, as well as corrective powers applied for any failure to be able to demonstrate compliance as required by the Regulation.

Guidance for controllers on **the relevance of judgements of the Courts of Justice of the European Union** to their data protection practices would also be useful, as it is unclear whether this is well understood on the ground. From relatively recent rulings such as Planet49 in October of last year to judgements of several years ago such as Rynes (2014), Bara (2015) and Nowak (2017) it seems many controllers are unaware of how their processing operations should have changed in the light of these.

How can the DPC influence organisations towards ethical and fair processing?

Fair processing is a compliance matter enshrined in the first principle of data protection in the GDPR (Article 5.1) and its predecessor Directive 95/46. Clear and visible **supervision and enforcement** via the investigative and corrective powers of the DPC will influence organisations towards fair processing.

While we note that the Information Commissioner's Office in the UK has recently appointed a data ethics adviser[15], we feel it is potentially distracting for a supervisory authority to become involved in a debate around ethics and technology which typically generates more heat than light and can serve as a useful distraction behind which data controllers can continue with non-compliant processing practices, or even shift some of the blame for unethical uses of personal data away from themselves.

> *Other companies by contrast saw opportunities to equate ethics with flexibility and vagueness – a chance to dilute the irresponsibilities towards individuals and society.*
> [16]

[14] Europäische Union and Europarat, *Handbook on European Data Protection Law*, 137

[15] ICO, 'Blog: Data Ethics and the Digital Economy', 18 November 2019, https://ico.org.uk/about-the-ico/news-and-events/blog-data-ethics-and-the-digital-economy/.

[16] Giovanni Buttarelli, Opening Speech, 40th ICDPPC https://edpl.lexxion.eu/data/article/13557/pdf/edpl_2018_04-026.pdf

It is two years since Microsoft published its ethical principles for AI[17], Facebook followed with something similar in May 2018[18], Google published its responsible practices for AI[19] in June 2018.

In April 2019 the European Commission's High-Level Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence[20], the same month that Google abandoned its Advanced Technology External Advisory Council[21].

Doteveryone's crowdsourced directory of Ethical Tech initiatives is 26 pages long[22].

As of the beginning of 2020, popular website creator Squarespace features a template with dummy text which reads *"I'm a Designer and Speaker who is interested in the ethics of AI"*[23], which simultaneously points to the popularity, commodification and lack of seriousness around much of this debate.

In short, there is an abundance of competing initiatives, frameworks, guidance documents, policies and discussion documents. There is no consensus on which of these to apply.

The DPC currently has no statutory power whereby it can make judgments on how ethical any particular processing activity is. However, there is an ethical dimension to the principle of fairness, which has been present in data protection law for several decades.

[17] 'AI principles & Approach from Microsoft', Microsoft, n.d., https://www.microsoft.com/en-us/AI/our-approach-to-ai

[18] Jordan Novet, 'Facebook forms a special ethics team to prevent bias in its A.I. software', CNBC, 3 May 2019, https://www.cnbc.com/2018/05/03/facebook-ethics-team-prevents-bias-in-ai-software.html

[19] Sundar Pichai, 'AI at Google: our principles', Google blog post, 7 June 2018, https://www.blog.google/technology/ai/ai-principles/

[20] European Commission, 'Ethics guidelines for trustworthy AI', 8 April 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[21] Kent Walker, 'An external advisory council to help advance the responsible development of AI', Google blog post, updated 4 April 2019, https://www.blog.google/technology/ai/external-advisory-council-help-advance-responsible-development-ai/

[22] Doteveryone Ethical Tech Directory (created 2017, updated by everyone)

[23] Frederike Kaltheuner on Twitter, 2 January 2020, https://twitter.com/F_Kaltheuner/status/1212781342322233344

Q6: Corrective powers and deterrent effect

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

→ This relates to target outcome 3: Organisations operate and innovate in an accountable, compliant, ethical and fair way in their processing of personal data

We have worked on the assumption that the deterrent effect mentioned in this question is a broad one whereby a corrective power applied to one controller influences the behaviour of other controllers. Hopefully a sanction applied to an individual controller will in most cases provide a sufficient deterrent to prevent repeated cases of the same infringement by the same controller. If there are repeat infringements by the same controller then the model used to apply sanctions should naturally take account of this.

Corrective powers can and should have a **wide influence**. Ireland is a small country and news travels rapidly. Sanctions employed against one or two controllers can have a much broader effect across an industry sector. However, the DPC should not rely only on word of mouth within particular industry circles to ensure sanctions have the desired deterrent effect.

Infringements on the data protection rights of individuals and non-compliance by controllers are not distinct to particular industry sectors, so the deterrent effect of the application of corrective powers will not be limited to just one industry sector if publicised sufficiently. **Publicity around sanctions of all types** is important in reassuring the public that the DPC is an active regulator which is prepared to act swiftly and decisively. In January 2020 this is not apparent.

Potential reputational damage associated with the publicity of a sanction can have a significant deterrent effect in certain sectors. If sanctions are applied but not publicised, or are solely publicised through publication in the DPC's annual report then the deterrent effect is significantly diluted.

Assessing which of the corrective powers in Article 58 will prove the greatest deterrent is dependent on context. It is difficult to do in the absence of information about the application of corrective powers and evidence of any effects on the entities to which these powers were applied or more broadly.

It is not yet possible to assess the potential **deterrent effect of administrative fines** in Ireland as, to the best of our knowledge, none have as yet been imposed. Even when fines have been imposed it will be difficult to assess their impact since any change in behaviour by controllers not directly sanctioned may be attributable to any number of other factors in addition to the sanction.

A **ban on or limitation of processing** can be more effective than administrative fines as in certain cases financial penalties have obviously been priced in as a cost of doing business. For example, on an earnings call on 24th April 2019, Facebook indicated it had priced in a fine of between $3 and $5 billion from the Federal Trade Commission[24]. When the fine was confirmed as $5 billion on

[24] Mike Isaac and Cecilia Kang, 'Facebook Expects to Be Fined Up to $5 Billion by F.T.C. Over Privacy Issues', New York

12th July 2019 Facebook's stock price went up.[25]

Since many businesses cannot function properly without the ability to process personal data, orders to stop processing or the threat of same can have a significant deterrent effect.

> *We need to slow things down, to give our institutions, individuals, and processes the time they need to find new and better solutions. The only way we will buy this time is if companies learn to say, "no" to some of the privacy-invading innovations they're pursuing. Executives should require those who work for them to justify new invasions of privacy against a heavy burden, weighing them against not only the financial upside, but also against the potential costs to individuals, society, and the firm's reputation.*[26]

Orders to controllers to comply with data subjects' rights requests will influence behaviour and are a crucial mechanism in keeping the entire supervisory model working smoothly. Currently we are encountering situations in which complaints to the DPC about failures to comply with rights requests are absorbed into the DPC's complaints process and remain unresolved for long periods of time. These should be resolved in a more timely manner through the use of orders by the DPC, bearing in mind always that there is a significant power imbalance between data subjects and data controllers and that the right of access is mentioned specifically in the Charter and key to giving individuals control over their personal data.

> *"We're seeing a social shift in the long term effects of privacy…. As billions more in venture investing targets our personal data for resale in a multitude of ways, people are starting to more deeply question their growing lack of data privacy and control."*[27]

Times, 24 April 2019, https://www.nytimes.com/2019/04/24/technology/facebook-ftc-fine-privacy.html

[25] Nilay Patel, 'Facebook's $5 billion FTC fine is an embarrassing joke', The Verge, 12 July 2019, https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke

[26] Paul Ohm, 'Don't Build a Database of Ruin', Harvard Business Review, 23 August 2012, https://hbr.org/2012/08/dont-build-a-database-of-ruin

[27] Andrew Hawn, quoted in 'Data Privacy Will Be The Most Important Issue In The Next Decade', Forbes, 26 November 2019, https://www.forbes.com/sites/marymeehan/2019/11/26/data-privacy-will-be-the-most-important-issue-in-the-next-decade/#67a4caa41882

Q7: Fines and other corrective powers

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?

→ This relates to target outcome 3: **Organisations operate and innovate in an accountable, compliant, ethical and fair way in their processing of personal data**

Despite the media interest in the size of fines available to the DPC, fines in isolation may not always have the greatest impact. For public sector controllers the level of administrative fine which can be applied is capped and other corrective powers will frequently be more useful in bringing processing activities into compliance.

A recent blog post by venture capitalist Fred Wilson shows that the business model of what can broadly be referred to as technology companies remains strongly focussed on data acquisition (emphasis ours) -

> *"Machine learning finally came of age in the 2010s and is now table stakes for every tech company, large and small.* ***Accumulating a data asset around your product and service*** *and using sophisticated machine learning models to personalize and improve your product is not a nice to have. It is a must have."*[28]

If it is a commercial imperative for startup and early stage companies to acquire large volumes of personal data then this brings up a potential issue with fines as a sanction: if fines are based on turnover / revenue , then **early stage companies** which are not generating significant volumes of revenue but at the same time process large volumes of personal data **may not see much exposure to fines based on this model**.

Instagram is frequently cited as an historical example of this. When Instagram was acquired by Facebook in 2012 it had around 30 million subscribers but only 13 employees[29] and no discernible revenue, being described at the time as "a startup that has lots of buzz but no business model."[30]

Fines and other corrective powers are most effective when there is a clear business argument to be made internally for compliance i.e. failure to comply will have a commercial impact on data controllers. Appeals to the higher nature of data controllers often fall on deaf ears at decision-making levels unless there is a commercial imperative. With this in mind **the DPC could**

[28] Fred Wilson, 'What Happened In The 2010s', 31 December 2019, https://avc.com/2019/12/what-happened-in-the-2010s/

[29] Thomas Houston, 'Facebook to buy Instagram for $1 billion', The Verge, 9 April 2012, https://www.theverge.com/2012/4/9/2936375/facebook-buys-instagram

[30] Laurie Segall, 'Facebook acquires Instagram for $1 billion', CNN, 09 April 2012, https://money.cnn.com/2012/04/09/technology/facebook_acquires_instagram/

publish an indicative model of how fines will be calculated, similar to those published by the Autoriteit Persoonsgegevens (AP) in March 2019 and the Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in October 2019. This would provide DPOs and those responsible for data protection within controllers with stronger arguments for investment in data protection.

Fines in combination with other corrective powers will likely have the most the most desirable effect in many situations.

Since the DPC was unable to impose administrative fines under the old acts, and no fines have as yet been imposed under the GDPR, controllers may not be aware that

> *[t]he concept of "equivalence" is central in determining the extent of the obligations of the supervisory authorities to ensure consistency in their use of corrective powers according to article 58 (2) in general, and the application of administrative fines in particular.*[31]

This concept of equivalence dictates that administrative fines should be consistent across Member States in order to ensure the level of protection is equivalent in all Member States.

At the time of writing CMS's Enforcement Tracker[32] has records of over 180 fines imposed or proposed by national supervisory authorities since 25th May 2018. Not all of these have been finalised and some are at various stages in appeals processes. Fines from Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Malta, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, the Netherlands and the United Kingdom are listed.

The European Data Supervisor has also been active, issuing two reprimands to the EUropean Parliament, the latter for a lack of transparency.

> *"The investigation into the European Parliament's use of NationBuilder resulted in the first ever EDPS reprimand issued to an EU institution: a contravention by the Parliament of Article 29 of Regulation (EU) 2018/1725, involving the selection and approval of sub-processors used by NationBuilder. A second reprimand was subsequently issued by the EDPS, after the Parliament failed to publish a compliant Privacy Policy for the thistimeimvoting website within the deadline set by the EDPS. In both instances, the European Parliament acted in line with EDPS recommendations."* [33]

The guidelines on the application and setting of administrative fines go on to say

> *The supervisory authorities are encouraged to use a considered and balanced approach in*

[31] Article 29 Working Party, 'Guidelines on the Application and Setting of Administrative Fines', March 2017, page 5, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[32] https://enforcementtracker.com/

[33] Wojciech Wiewiórowski, 'EDPS Investigates European Parliament's 2019 Election Activities and Takes Enforcement Actions', 28 November 2019, Press release, https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-european-parliaments-2019_en

> *their use of corrective measures, in order to achieve both an effective and dissuasive as well as a proportionate reaction to the breach. The point is to not qualify the fines as last resort, nor to shy away from issuing fines, but on the other hand not to use them in such a way which would devalue their effectiveness as a tool.*[34]

Sanctions large and small have been applied across Europe for a wide range of non-compliant processing activities. The DPC should not shy away from doing the same.

[34] Article 29 Working Party, 'Guidelines on the Application and Setting of Administrative Fines', March 2017, page 7, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

Q8: Balance between individual complaints and other work

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?

→ This relates to target outcome 4: As many people as possible understand and have control over how their personal data is used

Many issues that can affect millions of people start with an individual complaint. A data subject attempting to exercise their right of access, for example, should be able to do so knowing that the supervisory authority is present in the background, willing to assist them if they should encounter difficulties. A public record of swift and effective enforcement actions should be made available and publicised to reassure data subjects that this is the case.

Attempts to secure amicable resolutions can understandably lead to delays. This is unavoidable since it has been legislated for in the Data Protection Act 2018 but efforts should be made by the DPC to

- explain at the outset that this is the approach which is taken and the extended time frames involved for data subjects
- allow data subjects to specify early in the process that they are not seeking an amicable resolution.

At the same time the DPC is uniquely positioned among European supervisory authorities to make changes to the data processing activities of many global platform companies which are located in Ireland.

> *"States and regulators will never address these broad problems unless they address the core business model of the platforms: micro-targeted advertisements based on data gathering at massive scale. As long as this model is allowed, driving in turn the prioritising of clickbait material that fuels engagements, and allowing ads and posts to be hidden from a larger audience that might refute their claims, the platforms (and we) will remain ripe for exploitation. Micro-targeting offers only minute benefits to the regular platform user — a more timely shoe or holiday ad. Set against this, pro-democracy activists are exposed to serious threats and violence, and all of society pays the price of the inevitable destruction of the norms of democracy."*[35]

A recently-published report from Amnesty International reiterates this. Business models

[35] Karlin Lillington, 'Opening Statement by Karlin Lillington, Irish Times Journalist to the Grand International Committee on Disinformation and Oireachtas Joint Committee on Communications, Climate Action and Environment', https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/joint_committee_on_communications_climate_action_and_environment/submissions/2019/2019-11-08_opening-statement-karlin-lillington-columnist-the-irish-times_en.pdf

predicated on excessive collection of personal data cause harm for individuals in the real world.

> *"The companies' surveillance-based business model forces people to make a Faustian bargain, whereby they are only able to enjoy their human rights online by submitting to a system predicated on human rights abuse. Firstly, an assault on the right to privacy on an unprecedented scale, and then a series of knock-on effects that pose a serious risk to a range of other rights, from freedom of expression and opinion, to freedom of thought and the right to non-discrimination."* [36]

Both these elements of the DPC's work are vital to the protection of the rights and freedoms of individuals and where possible neither should be prioritised to the detriment of the other.

Q9: 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?

→ This relates to target outcome 5: **Children are specifically protected.**

As with our other responses to some of the preceding questions, it is not possible to set out a definitive ranking of these activities in terms of efficacy.

Formal investigations, decision-making and applying corrective powers are obviously of great importance. Due to the increased risk of reputational damage to controllers should they be found to be in breach of the regulation with respect to the personal data of children, the application of these tools should be highly effective.

Collaborating with children's rights experts is valuable and considerable research has been done in this area.

Codes of conduct will no doubt prove useful to controllers in this area and others. Since there have been no codes of conduct approved as yet that we are aware of it is difficult to assess the usefulness of them in achieving this outcome.

Regarding **production of education materials**, the Article 29 Working Party Guidelines on Transparency states the following:

> *"WP29's position is that transparency is a free-standing right which applies as much to*

[36] Amnesty, 'Facebook and Google's Pervasive Surveillance of Billions of People Is a Systemic Threat to Human Rights', accessed 11 January 2020, https://www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/

> *children as it does to adults. WP29 emphasises in particular that children do not lose their rights as data subjects to transparency simply because consent has been given/ authorised by the holder of parental responsibility in a situation to which Article 8 of the GDPR applies. While such consent will, in many cases, be given or authorised on a once-off basis by the holder of parental responsibility, a child (like any other data subject) has an ongoing right to transparency throughout the continuum of their engagement with a data controller."*[37]

This places an onus on controllers to provide age appropriate information to children. This should be a relatively straightforward activity to pursue in conjunction with the development of education materials.

Q10: Other actions relating to the protection of children

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?

→ This relates to target outcome 5: **Children are specifically protected.**

We don't have any additional activities to add with regard to this target outcome.

Q11: Other non-statutory activities

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

There are a very large number of activities listed in the consultation document. All of them are worthwhile and will contribute to achieving the target outcomes. We don't have any other activities to add.

[37] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679', April 2018, para. 15, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025

Q12: Evidence of success

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

All the activities listed in the consultation document are of value and will contribute to the desired outcomes, and many of them are interlinked, overlap and will have an enhancing effect on each other.

It is impossible to assess at this point which may prove to be the most effective.

About Article Eight Advocacy

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

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

Web: article8.ie | **Email:** info@article8.ie

8/10 Coke Lane, Smithfield,

Dublin 7, D07 EN2Y

Ireland

CRO #663077

Bibliography

1. Angela Merkel, Harvard graduation address, May 2019 https://www.americanrhetoric.com/speeches/angelamerkelharvardcommencementenglish.htm

2. Wojciech Wiewiórowski and EDPS, 'Data Protection Day 2020: Facing New Challenges', https://edps.europa.eu/sites/edp/files/publication/20-01-16_speech_zagreb_en.pdf

3. Ari Ezra Waldman, 'Privacy Law's False Promise', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 6 December 2019), page 31, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3499913

4. Ari Ezra Waldman, 'Privacy Law's False Promise', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 6 December 2019), page 6, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3499913

5. Denis Kelleher and Karen Murray, EU Data Protection Law (London: Bloomsbury Professional, 2018), para. 9.01.

6. Data Protection Commission of Ireland, 'Response to the Public Accounts Committee following appearance on 26 September 2019', https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/committee_of_public_accounts/submissions/2019/2019-12-31_correspondence-graham-doyle-head-of-communications-data-protection-commission-32r002486-pac_en.pdf

7. Caitlin Fennessy, 'GDPR at One Year: What We Heard from Leading European Regulators', May 2019, https://iapp.org/media/pdf/resource_center/GDPR_at_One_IAPPWhitePaper.pdf

8. Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors. Data Subject Access Rights in Practice', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 20 January 2018), page 3, https://papers.ssrn.com/abstract=3106632

9. Pat Walshe, Heinrich-Böll-Stiftung, and Transatlantic Consumer Dialogue, 'Privacy in the EU and US: Consumer Experiences across Three Global Platforms | Heinrich Böll Stiftung | Brussels Office - European Union', Heinrich-Böll-Stiftung, accessed 11 January 2020, page 8, https://eu.boell.org/sites/default/files/2019-12/TACD-HBS-report-Final.pdf

10. "Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.": CJEU joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 9 November 2010, paragraph 50

11. Joseph Jerome, 'The GDPR's Impact on Innovation Should Not Be Overstated', Center for Democracy and Technology (blog), 1 April 2019, https://cdt.org/insights/the-gdprs-impact-on-innovation-should-not-be-overstated/

12. Europäische Union and Europarat, eds., Handbook on European Data Protection Law, 2018

edition, Handbook / FRA, European Union Agency for Fundamental Rights (Luxembourg: Publications Office of the European Union, 2018), page 137.

13. Article 29 Working Party, 'Opinion on the Principle of Accountability', 2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

14. Europäische Union and Europarat, Handbook on European Data Protection Law, page 137

15. ICO, 'Blog: Data Ethics and the Digital Economy', 18 November 2019, https://ico.org.uk/about-the-ico/news-and-events/blog-data-ethics-and-the-digital-economy/

16. Giovanni Buttarelli, Opening Speech, 40th ICDPPC https://edpl.lexxion.eu/data/article/13557/pdf/edpl_2018_04-026.pdf

17. 'AI principles & Approach from Microsoft', Microsoft, n.d., https://www.microsoft.com/en-us/AI/our-approach-to-ai

18. Jordan Novet, 'Facebook forms a special ethics team to prevent bias in its A.I. software', CNBC, 3 May 2019, https://www.cnbc.com/2018/05/03/facebook-ethics-team-prevents-bias-in-ai-software.html

19. Sundar Pichai, 'AI at Google: our principles', Google blog post, 7 June 2018, https://www.blog.google/technology/ai/ai-principles/

20. European Commission, 'Ethics guidelines for trustworthy AI', 8 April 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

21. Kent Walker, 'An external advisory council to help advance the responsible development of AI', Google blog post, updated 4 April 2019, https://www.blog.google/technology/ai/external-advisory-council-help-advance-responsible-development-ai/

22. Doteveryone Ethical Tech Directory (created 2017, updated by everyone)

23. Frederike Kaltheuner on Twitter, 2 January 2020, https://twitter.com/F_Kaltheuner/status/1212781342322233344

24. Mike Isaac and Cecilia Kang, 'Facebook Expects to Be Fined Up to $5 Billion by F.T.C. Over Privacy Issues', New York Times, 24 April 2019, https://www.nytimes.com/2019/04/24/technology/facebook-ftc-fine-privacy.html

25. Nilay Patel, 'Facebook's $5 billion FTC fine is an embarrassing joke', The Verge, 12 July 2019, https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke

26. Paul Ohm, 'Don't Build a Database of Ruin', Harvard Business Review, 23 August 2012, https://hbr.org/2012/08/dont-build-a-database-of-ruin

27. Andrew Hawn, quoted in 'Data Privacy Will Be The Most Important Issue In The Next Decade' , Forbes, 26 November 2019, https://www.forbes.com/sites/marymeehan/2019/11/26/data-privacy-will-be-the-most-import

ant-issue-in-the-next-decade/#67a4caa41882

28. Fred Wilson, 'What Happened In The 2010s', 31 December 2019, https://avc.com/2019/12/what-happened-in-the-2010s/

29. Thomas Houston, 'Facebook to buy Instagram for $1 billion', The Verge, 9 April 2012, https://www.theverge.com/2012/4/9/2936375/facebook-buys-instagram

30. Laurie Segall, 'Facebook acquires Instagram for $1 billion', CNN, 09 April 2012, https://money.cnn.com/2012/04/09/technology/facebook_acquires_instagram/

31. Article 29 Working Party, 'Guidelines on the Application and Setting of Administrative Fines', March 2017, page 5, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

32. https://enforcementtracker.com/

33. Wojciech Wiewiórowski, 'EDPS Investigates European Parliament's 2019 Election Activities and Takes Enforcement Actions', 28 November 2019, Press release, https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-european-parliaments-2019_en

34. Article 29 Working Party, 'Guidelines on the Application and Setting of Administrative Fines', March 2017, page 7, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

35. Karlin Lillington, 'Opening Statement by Karlin Lillington, Irish Times Journalist to the Grand International Committee on Disinformation and Oireachtas Joint Committee on Communications, Climate Action and Environment', https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/joint_committee_on_communications_climate_action_and_environment/submissions/2019/2019-11-08_opening-statement-karlin-lillington-columnist-the-irish-times_en.pdf

36. Amnesty, 'Facebook and Google's Pervasive Surveillance of Billions of People Is a Systemic Threat to Human Rights', accessed 11 January 2020, https://www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/

37. Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679', April 2018, para. 15, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025