

Comments of the
ELECTRONIC PRIVACY INFORMATION CENTER

DATA PROTECTION COMMISSION IRELAND
Consultation on Data Protection Impact Assessments (DPIAs) Guidance
July 3, 2018

By notice published on June 6, 2018,¹ the Data Protection Commission of Ireland (“DPC”) requests public comments on the Draft Data Protection Impact Assessment List (“DPIA Guidance”)² for submission to the European Data Protection Board for approval. Pursuant to this notice, the Electronic Privacy Information Center (“EPIC”) submits the following comments on DPIAs to (1) promote algorithmic transparency, (2) make clear the risks of automated processing of personal data, (3) increase accountability for automated processing, and (4) enforce privacy-enhancing techniques to minimize data collection.

EPIC is a public interest research center established in Washington D.C. in 1994 to focus public attention on emerging privacy and civil liberties issues.³ EPIC has long worked to promote transparency and accountability for information technology. EPIC has filed numerous Freedom of Information Act lawsuits⁴ to compel disclosure of privacy impact assessments by federal agencies.⁵ EPIC has also urged the US Federal Trade Commission to investigate private firms that create secret, proprietary algorithms to assign scores to individuals,⁶ and EPIC has opposed the scoring of individuals by the government.⁷ EPIC’s new “Privacy Impact

¹ Data Protection Commission Ireland, *Data Protection Commission issues draft Data Protection Impact Assessment list for public consultation* (June 6, 2018), <https://dataprotection.ie/docs/EN/06-06-2018-Data-Protection-Commission-issues-draft-Data-Protection-Impact-Assessment-list-for-public-consultation/m/1741.htm>

² Data Protection Commission Ireland, *Public Consultation: Draft List of Types of Data Processing Operations Which Require a Data Protection Impact Assessment* (June 2018), <https://dataprotection.ie/docimages/documents/DPIAConsultation.pdf>

³ About EPIC, *EPIC*, <https://epic.org/epic/about.html>.

⁴ EPIC, *EPIC v. FBI - Privacy Assessments*, <https://epic.org/foia/fbi/pia/>; *See also*, EPIC, *EPIC v. DEA - Privacy Impact Assessments*, <https://epic.org/foia/dea/pia/>; EPIC, *EPIC v. NSA - Cybersecurity Authority*, <https://epic.org/foia/nsa/nspd-54/default.html>; EPIC, *EPIC v. Presidential Election Commission*, <https://epic.org/privacy/litigation/voter/epic-v-commission/>

⁵ EPIC, *EPIC Open Government*, https://epic.org/open_gov/

⁶ EPIC, *Complaint In re Universal Tennis to the Federal Trade Commission* (May 17, 2017), <https://epic.org/algorithmic-transparency/EPIC-FTC-UTR-Complaint.pdf>

⁷ *See*, Letter from EPIC President Marc Rotenberg to the U.S. Senate Committee on Commerce, Science, and Transportation, EPIC (November 30, 2016), <https://epic.org/privacy/drones/EPIC-Sen-Commerce-Letter-re-AI.pdf>: “Algorithms are used for social control. China’s Communist Party is deploying a “social credit” system that assigns to each person government-determined favorability rating.”

See also, EPIC, *EPIC v. DOJ (Criminal Justice Algorithms)* <https://epic.org/foia/doj/criminal-justicealgorithms/>; EPIC, *Algorithms in the Criminal Justice System* <https://epic.org/algorithmictransparency/crim-justice/>.

Assessment” initiative is a key component of the organization’s long-running open government project and consumer protection work. EPIC broadly promotes “Algorithmic Transparency.”⁸ We recently advised the UK Information Commissioner’s Office to protect individual rights against algorithmic profiling and discrimination by requiring the systematic implementation and publication of DPIAs.⁹

I. Requirements for Mandatory DPIAs

1. DPIAs Should Promote Algorithmic Transparency

a. Overview of GDPR Articles 35 - 36 and Related Authorities

Articles 35 and 36 of the General Data Protection Regulation (“GDPR”) form the cornerstone legal authority for DPIAs. Article 35(1) and (2) establish the obligation of the data controller to conduct a DPIA before processing data that is likely to result in a high risk to individual rights and freedoms.¹⁰

Article 35(1):

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Article 35(2):

The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

Article 35(3) lists three types of data processing that automatically require a DPIA. These data processing techniques will always pose a high risk to individuals, and thus Article 35 mandates the data controller to conduct a DPIA and consult with the data protection authority to comply with the GDPR.

Article 35(3):

A data protection impact assessment referred to in paragraph 1 shall in particular be

⁸ EPIC, *Algorithmic Transparency*, <https://epic.org/algorithmic-transparency/>.

⁹ EPIC, *Comments to the UK Information Commissioner’s Office on Data Protection Impact Assessment Draft Guidance* (April 12, 2018), <https://epic.org/algorithmic-transparency/EPIC-ICO-Comment-GDPR-DPIA.pdf>

¹⁰ MARC ROTENBERG, *THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS* 692-93 (“Article 35: Data Protection Impact Assessment and Prior Consultation”)

required in the case of:

- a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- c) a systematic monitoring of a publicly accessible area on a large scale.

Article 35(4) empowers the DPC to publish a list of processing operations that are likely to cause a high risk and thus mandate a DPIA. The DPC Guidance must be specific and comprehensive, as it carries legal authority to enumerate obligations on data controllers to conduct DPIAs and consult the DPC.

Article 35(4):

The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

Article 35(6):

Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

Article 36 requires the data controller to immediately suspend processing when DPIAs point to a high risk for individuals. Article 36(1) mandates the data controller to submit DPIAs to the DPC and consult the DPC on whether the proposed processing is permissible under the law. The data controller is prohibited from proceeding without satisfying these safeguards under the supervision of the DPC.

Article 36(1):

The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Articles 35 – 36 of the GDPR, and Article 12 of the EU Data Protection Directive on which the provision is based, require “algorithmic transparency” for all processing of personal

data.¹¹ The DPC Guidance states that it is mandatory to conduct a DPIA if the proposed processing “uses systematic and extensive profiling with significant effects.”¹² Access to the “logic of the algorithm” is required to ensure accountability for the automated outcomes that adversely affect individuals’ rights and opportunities.

EU Data Protection Directive 95/46/EC, Article 12 (Right of Access):

Member States shall guarantee every data subject the right to obtain from the controller:

- (a) without constraint at reasonable intervals and without excessive delay or expense [...] knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1);

Setting clear rules for mandatory DPIAs prior to automated processing strengthens the authority of the DPC to enforce *ex post* liability for automated profiling that derogates individual rights under the GDPR. Data controllers should be auditable through their DPIAs on why and how they automatically processed personal data that had a significant effect on natural persons. If a data controller simply did not conduct a DPIA prior to automated processing, that would constitute an express violation of GDPR Article 35(3)(a) and the individual rights enshrined in GDPR Articles 15 and 22.

GDPR Article 15

- (1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: . . .
 - h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The GDPR empowers the DPC to protect individual rights against algorithmic profiling and discrimination caused by automated processing. GDPR Articles 13 (right to be informed of data processing), 15 (access rights of the data subject), and 22 (automated decision-making and profiling) establish baseline safeguards to automated decision-making and profiling. However, none of these related Articles and rights are referenced in the DPC Guidance on the data controller’s obligation to conduct a DPIA.

The DPC Guidance also does not incorporate the guidance of any relevant GDPR recitals

¹¹ European Parliament and Council, Article 12 of Directive 95/46/EC (24 October 1995), On the protection of individuals with regard to the processing of personal data and on the free movement of such data.

¹² Data Protection Commission Ireland, *Public Consultation: Draft List of Types of Data Processing Operations Which Require a Data Protection Impact Assessment* (June 2018), <https://dataprotection.ie/docimages/documents/DPIAConsultation.pdf>, at 3.

which directly address profiling (Rec. 71), risk assessments (Rec. 74-77, 84, 89-92), and responsibility to consult with a supervisory authority (Rec. 94). EPIC advises the Commission to reference these recitals in the DPIA list to provide a more comprehensive and authoritative guide on the factors of “high risk,” “significant effect,” “large scale processing,” and “systematic and extensive processing.”

b. DPIAs as Procedural Safeguards for Automated Processing

Automated processing plays a significant role in decisions that impact individual rights and opportunities.¹³ Despite the pervasiveness of algorithmic decision-making in modern society, the process remains a “black box”¹⁴ of unproven and unexplainable outcomes.

Professor Danielle Citron and Professor Frank Pasquale address the issue of a “scored society”¹⁵ and urge for “technological due process”¹⁶ by a public audit and assessment of automated processing systems.

Procedural regularity is essential given the importance of predictive algorithms to people’s life opportunities—to borrow money, work, travel, obtain housing, get into college, and far more. Scores can become self-fulfilling prophecies, creating the financial distress they claim merely to indicate. The act of designating someone as a likely credit risk (or bad hire, or reckless driver) raises the cost of future financing (or work, or insurance rates), increasing the likelihood of eventual insolvency or un-employability. When scoring systems have the potential to take a life of their own, contributing to or creating the situation they claim merely to predict, it becomes a normative matter, requiring moral justification and rationale.¹⁷

DPIAs can safeguard individual rights in algorithmic decision-making by establishing procedural regularity to assess risks and to restrain from processing when risks are identified. EPIC has long campaigned for algorithmic transparency to be regarded as a fundamental human

¹³ The Aspen Institute, *Artificial Intelligence: The Great Disruptor* (April 2, 2018), <https://www.aspeninstitute.org/publications/artificial-intelligence-great-disruptor/>. (“In 2017, artificially intelligent (AI) technologies surged into the popular discourse for its advancements — such as autonomous vehicles and predictive analytics — to critiques of potential biases, inequity and need for transparency.”)

¹⁴ Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, at 218 (Harvard University Press 2015)

¹⁵ Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process For Automated Predictions*, 89 *Washington Law Review* 1 (2014), http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2435&context=fac_pubs

¹⁶ Danielle Keats Citron, *Technological Due Process*. U of Maryland Legal Studies Research Paper No. 2007-26; *Washington University Law Review*, Vol. 85, pp. 1249-1313, (2007). <https://ssrn.com/abstract=1012360>

¹⁷ Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process For Automated Predictions*, 89 *Washington Law Review* 1 (2014), at 18

right at international institutions, including UNESCO and OECD.¹⁸

We believe that the current DPC Guidance is unclear on the risks of automated decision-making that trigger a mandatory DPIA under GDPR Article 35(3)-(4). The DPC derives legal authority from Article 35(4) to create binding guidance on the types of processing that require DPIAs. Thus, it is critical to clarify these definitions and requirements to ensure that DPIAs can promote algorithmic transparency and protect individual rights implicated in automated profiling.

2. Clarification on the Risks of Automated Decision-Making

a. Systematic and Extensive Profiling

The DPC Guidance briefly defines “systematic and extensive” as a processing that “occurs according to a system; is pre-arranged, organised or methodical; takes place as part of a general plan for data collection; or is carried out as part of a strategy.”¹⁹ In addition, “the term ‘extensive’ implies that the processing covers a large area or involves a large range of data or data subjects.”²⁰ These definitions are broad and hard to understand without practical examples. EPIC makes the following suggestions and proposals to strengthen the mandatory DPIA requirement under GDPR Article 35(3)(a):

- Specify that algorithmic decision-making is a “systematic” processing that mandates a DPIA.
- DPIAs should evaluate the logic of algorithms that profile individuals, and the envisaged consequences of such automated processing on individual rights and freedoms.
- Specify that “systematic and extensive” processing includes indirect profiling of a natural person based on their association with a specific group.
 - I.e. Providing more favorable loan offers for members of certain groups based on age, profession, gender, and other personal or demographic segments.
- Algorithms that rank and index search results must also require a thorough DPIA because

¹⁸ EPIC, *At UNESCO, Rotenberg Argues for Algorithmic Transparency* (Dec. 8, 2015), <https://epic.org/2015/12/at-unesco-epics-rotenberg-argu.html>; UNESCO, Privacy Expert Argues “Algorithmic Transparency” Is Crucial for Online Freedoms at UNESCO Knowledge Café, <https://en.unesco.org/news/privacy-expert-argues-algorithmic-transparency-crucial-onlinefreedoms-unesco-knowledge-cafe>; See, Jaap-Henk Hoepman, Summary of the CPDP Panel on Algorithmic Transparency (January 26, 2017) remarks of Marc Rotenberg, <https://blog.xot.nl/2017/01/26/summary-of-the-cpdp-panel-on-algorithmic-transparency/>; EPIC, *At OECD, EPIC Renews Call for Algorithmic Transparency*, <https://epic.org/2017/10/at-oecd-epic-renews-call-for-a.html>

¹⁹ Data Protection Commission Ireland, *Public Consultation: Draft List of Types of Data Processing Operations Which Require a Data Protection Impact Assessment* (June 2018), <https://dataprotection.ie/docimages/documents/DPIAConsultation.pdf> at 8.

²⁰ *Id.*

they can distort web users' access to information with limited transparency and accountability. Virtually every search engine, social media company, and web operator develops its own unique algorithm to curate content for individual users to control how information is fetched and displayed from search queries.²¹ The DPC Guidance should explain these implications in the definition of "large-scale" processing by search engines that process data for these purposes.²²

- Specify that "systematic" processing includes behavioral targeting that creates a risk to the rights and freedoms of natural persons through disinformation and social engineering. This type of processing also mandates a DPIA and DPC consultation under GDPR Article 35(4) as a "large-scale profiling,"²³ which the DPC promulgated in the draft DPIA Guidance as "likely to be a high risk to individuals"²⁴ and thus triggers a DPIA.
 - I.e. Profiling individuals based on their personal data uploaded to social media as a strategy for social engineering (the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes).
 - Algorithmic transparency is necessary whenever there is processing of personal data that generates targeted political advertising. Algorithms now enable targeted ads with unprecedented granularity. This technology surpasses the reach of traditional media and necessitates greater scrutiny with DPIAs, as algorithms can be misused for disinformation that affect the rights and freedoms of natural persons.
 - Online advertisers should always conduct a DPIA and consult with the DPC on what techniques it deployed to create a target audience for an advertisement, including what data it collected about the user that caused the user to be placed within that target audience.

b. Significant Effect

The DPC Guidance defines "significant effect" in Article 35(3)(a) as an outcome that has a "detrimental or discriminatory effect on an individual or that cause a change in behaviour, decision making, circumstances or ability to avail of their rights or entitlements."²⁵ The examples provided by the Guidance treat "significant effect" as a "legal effect," causing a limitation of legal rights or affecting a person's legal status. We believe that this is a restrictive definition that does not address a broader range of privacy harms that affect a person's opportunities and

²¹ See, Jaap-Henk Hoepman, *Summary of the CPDP Panel on Algorithmic Transparency* (January 26, 2017)(remarks of Marc Rotenberg, <https://blog.xot.nl/2017/01/26/summary-of-the-cpdp-panel-on-algorithmic-transparency/>).

²² Data Protection Commission Ireland, *Public Consultation: Draft List of Types of Data Processing Operations Which Require a Data Protection Impact Assessment* (June 2018), <https://dataprotection.ie/docimages/documents/DPIAConsultation.pdf> at 7.

²³ *Id.* at 4.

²⁴ *Id.*

²⁵ *Id.* at 5.

autonomy.

- The DPC should clarify that individuals may still suffer a significant effect from a decision that is not “solely” based on automated processing. This would estop data controllers from avoiding the mandatory DPIA requirement with *de minimis* human intervention on automated processing whilst producing de facto automated decisions.
- Emphasize that a “significant” effect need not necessarily be a “legal” effect on an individual’s legal status and rights.
- Emphasize that the Article 29 Working Party has adopted Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251) which states:

Even if a decision-making process does not have an effect on people’s legal rights it could still fall within the scope of Article 22 if it produces an effect that is equivalent or similarly significant in its impact. In other words, even where no legal (statutory or contractual) rights or obligations are specifically affected, the data subjects could still be impacted sufficiently to require the protections under this provision.²⁶

- Clarify that the processing may produce a “significant effect” even if the data subject is unaware of how they have been profiled. If the affected individual is unaware of the processing, the DPC Guidance should follow Article 29 Working Party report WP251²⁷ to consider:
 - the intrusiveness of the profiling process;
 - the expectations and wishes of the individuals concerned;
 - the way the advert is delivered; or
 - the particular vulnerabilities of the data subjects targeted
- Emphasize that processing that might have little impact on individuals personally may in fact have a significant net effect on certain groups of society, thereby mandating the DPIA requirement.
- Incorporate more explanations from the Article 29 Working Party Guidelines to set clear and comprehensive requirements. Authoritative practice guidelines should pre-empt data controllers from limiting their DPIA obligations with prohibitive interpretations of the

²⁶ Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251)* (October 3, 2017), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

²⁷ *Id.*

DPC Guidance.

II. **Guidance on GDPR Article 35(4): DPC List of Mandatory DPIAs**

The DPC is required by Article 35(4) of the GDPR to publish a list of types of processing that are likely to be high risk and so require a DPIA. EPIC makes the following suggestions and proposals:

1. **Clarification on Large-Scale Profiling**

- Explicitly address data processing for behavioral targeting and advertising as “likely to be a high risk to individuals.”
- Explicitly prohibit any data processing for social engineering as an infringement of individual rights and freedoms²⁸ protected in the European Union, notwithstanding the controller’s DPIA results.
- Add “data processing that disseminates large-scale personal data of social media users to third parties” as a high risk to individuals requiring a comprehensive DPIA and consultation with the DPC.

2. **Clarification on Biometric Data Processing**

- Further define biometric data. Include “facial templates” as sensitive biometric data that requires a DPIA.
- Clarify that numerical scoring of facial templates that result from scanning image identity still constitutes “biometric data” that poses a likelihood of high risk to individuals.²⁹

3. **Quasi-Identifiers May Pose High Risks to Individuals**

- The DPC Guidance consistently refers to “personal data” in defining the instances of processing that are likely to be a high risk to individuals. However, particularly in the categories of data matching, invisible processing, and tracking, even data that is not directly attributable to a personal aspect of a natural person, such as a phone’s unique identifier, may pose a high risk to individual rights and freedoms.

4. **DPC Guidance Should Require Publication of DPIAs**

Privacy assessments are a critical part of assessing the level of intrusiveness new technologies could have on individual rights and freedoms. EPIC believes in the publication of

²⁸ See, EPIC, *EPIC, Consumer Groups Urge FTC To Investigate Facebook*, <https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf> (discussing the privacy right infringements of social engineering)

²⁹ See, EPIC, *In re Facebook and Facial Recognition (2018)*, <https://www.epic.org/privacy/ftc/facebook/facial-recognition2018/> (FTC complaint filed by EPIC on the lack of privacy safeguards on biometric data processing by Facebook)

DPIAs to provide transparency to the public and increase accountability for both commercial and governmental processing of personal data.

In the United States, the E-Government Act of 2002³⁰ obliges the publication of PIAs. EPIC has long worked to bring transparency and accountability to the efforts of governmental agencies to use new surveillance and information technology that collects and stores personal information about citizens.³¹ Notably, *EPIC v. Presidential Election Commission*³² challenged the unlawful collection of personal voter data without the publication of a legally required PIA by the now defunct Presidential Advisory Commission. EPIC continues to engage in numerous Freedom of Information Act lawsuits³³ to reveal where transparency is lacking and to highlight privacy-invasive programs that lack proper assessments of their impact on privacy.

a. Publication as a Reporting Mechanism to DPC

The DPC Guidance does not require publication of DPIAs. Nor are the DPIA guidelines supported by a reporting mechanism to the DPC.³⁴ Leading DPIA scholars Paul de Hert and David Wright have noted the value of publishing the assessments to demonstrate accountability.³⁵

EPIC believes that mandatory publication is necessary. Under the current Guidance, it is virtually impossible to oversee whether the data controllers engaged in high risk processing are complying with GDPR Articles 35 – 36, or the best practice guidelines promulgated by the DPC. Publication of DPIAs would certify that data controllers have met the requirements of the GDPR by conducting a critical privacy analysis, and ensuring compliance to the legal, regulatory, and policy requirements of individual privacy rights.

5. Require Transparent and Systematic DPIAs to Prevent Lax Self-Evaluations

Pursuant to GDPR Article 35(5), the DPC Guidance provides a list of processing where a DPIA is not required. The DPC provides a DPIA exemption for processing that was “previously found not to be at risk by a DPIA.”³⁶ EPIC believes that this is a lax standard which could diminish accountability for data processing that affect the rights and freedoms of natural persons.

³⁰ Pub. L. 107-347, 116 Stat. 2899 (2002)

³¹ EPIC, *EPIC Open Government*, https://epic.org/open_gov/

³² *EPIC v. Presidential Election Commission*, <https://epic.org/privacy/litigation/voter/epic-v-commission/>

³³ EPIC, *EPIC v. FBI - Privacy Assessments*, <https://epic.org/foia/fbi/pia/>; *See also*, EPIC, *EPIC v. DEA - Privacy Impact Assessments*, <https://epic.org/foia/dea/pia/>; EPIC, *EPIC v. NSA - Cybersecurity Authority*, <https://epic.org/foia/nsa/nspd-54/default.html>

³⁴ David Wright, Paul de Hert, Kush Wadhwa & Dariusz Kloza, *A Privacy Impact Assessment Framework for Data Protection and Privacy Rights* (September 21, 2011), Prepared for the European Commission Directorate General Justice, JLS/2009-2010/DAP/AG, <http://www.vub.ac.be/LSTS/pub/Dehert/507.pdf>

³⁵ David Wright & Paul de Hert, *Privacy Impact Assessment* (2012), Springer, Law, Governance and Technology Series, Vol. 6. at 27.

³⁶ Data Protection Commission Ireland, *Public Consultation: Draft List of Types of Data Processing Operations Which Require a Data Protection Impact Assessment* (June 2018), <https://dataprotection.ie/docimages/documents/DPIAConsultation.pdf> at 8.

Allowing organizations to rely on this exemption would lead to incomplete information and lack of transparency in DPIAs. The DPC would also have no audit trail to assess whether the new processing that did not conduct a DPIA actually exceeded the purposes and scope of the processing that a previous DPIA determined was low-risk.

For example, an organization may conduct a DPIA and self-assess that there is no “high risk to individuals” that requires a consultation with the DPC under GDPR Article 36(1). However, without publication of the DPIA that led to this conclusion, there is no way for the supervisory authority or the public to scrutinize the elements of DPIA and whether the assessment on the necessity, proportionality, and risks of processing adequately considered the data subject’s intrinsic rights and freedoms.

Furthermore, conducting a DPIA is not a one-step process that stops at a single evaluation of the proposed processing. It requires a conscious and systematic effort³⁷ by the data controller at each step of the processing operation, who must review each factor that could impact the consequences of implementation. In particular, a slight variance in the processing technology or the types of data points processed can pose significantly different risks to individuals. Therefore, organizations should not rely on a past DPIA to affirm that the future processing will not need an updated DPIA, as this is in no way guaranteed. Instead, the DPC should require the publication of DPIAs and make data controllers accountable for systematically identifying privacy risks caused by specific processes or applications—especially in the development of new technologies or the collection of granular data.

III. Cross-Guidance on GDPR Article 25: DPIA as Privacy by Design

DPIAs are vital to achieving data minimization, but the DPC Guidance does not address this. The guidelines also fail to address GDPR Article 25 which governs privacy by design. EPIC believes that the DPIA Guidance should cross-reference GDPR Article 25 on privacy by design and default, to incorporate the highest standard of processes and technologies that further data protection principles and demonstrate full compliance of Articles 35 - 36.

The DPC does not emphasize the importance of embedding DPIAs into organizational processes to ensure that the evaluations guide decision-making on data collection. Although the Guidance states that “[c]ontrols and measures can be organisational or technical and may be fully effective in mitigating risk, or partial,” it does not promote the adoption of privacy-enhancing techniques which are critical to protecting individual rights against preventable risks. We also find it problematic that the Guidance does not urge organizations to view DPIAs as an ongoing obligation that requires regular review and consultations with the DPC.

DPIAs should be a scalable tool with core requirements that aim to minimize the

³⁷ Rolf H. Weber, *Privacy Impact Assessment – A Privacy Protection Improvement Model?* (August 2011), 25th IVR World Congress LAW SCIENCE AND TECHNOLOGY Frankfurt am Main No. 039 / 2012 Series B.

collection of sensitive data and eliminate secondary uses of data that pose additional risks.

EPIC makes the following suggestions and proposals:

- DPIAs must be commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information.³⁸
- DPIAs should comprehensively address and explain the complexities of the underlying data collection and processing systems.
- Privacy assessments should continue even after the deployment of certain processing.
- DPIAs should be mandatory for new technologies that collect more granular data on individuals or possess the capacity to collect larger quantities of data. DPIAs should assess whether the collection of this data is necessary or proportionate. The DPC should prohibit the excessive collection of data that pose a risk to individual rights.
- DPIAs should result in data minimization.
- DPIAs should eliminate unspecified and unlimited data collection.
- DPIAs should eliminate data collections exceeding their purpose.
- DPIAs should give data subjects greater access and control of their data. The DPC should require organizations to implement technical and operational measures to allow individuals to scrutinize DPIAs and exercise their rights accordingly.
- The DPC should prohibit secret data collection.
- Whenever there is automated processing of data, the DPC should require algorithmic transparency through DPIAs on the logic of the processing and how it can affect individual rights.
- The DPC should routinely audit and monitor data controllers to ensure they stop and inform the DPC when the DPIA identifies likely high risks to individuals.

IV. Conclusion

DPIAs are crucial to ensuring oversight and accountability of personal data collection, use, and disclosure by private and public actors. Privacy assessments must protect individual rights and freedoms from extensive and intrusive data processing.³⁹ The DPIA guidelines issued by an independent data protection authority must focus on the rights and responsibilities model

³⁸ § 208 of the E-Government Act (2002), United States Federal Law.

³⁹ Paul de Hert, *A Human Rights Perspective on Privacy and Data Protection Impact Assessments* (September 16, 2011), Springer, Law, Governance and Technology Series 6, <http://www.vub.ac.be/LSTS/pub/Dehert/517.pdf>

of the GDPR.

EPIC appreciates the opportunity to comment on the DPC consultation for the DPIA Guidance. The enforcement of DPIAs, pursuant to Article 35 of the GDPR, should strengthen transparency and accountability and help ensure fairness in the processing of personal data. We urge the DPC to promulgate strong standards to ensure that DPIAs protect individuals' rights and freedoms.

Respectfully Submitted,

/s/ Marc Rotenberg

Marc Rotenberg
EPIC President

/s/ Sunny Seon Kang

Sunny Seon Kang
EPIC International Consumer Counsel

/s/ Eleni Kyriakides

Eleni Kyriakides
EPIC International Counsel

/s/ John Davisson

John Davisson
EPIC Counsel