epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Comments of the
ELECTRONIC PRIVACY INFORMATION CENTER

INFORMATION COMMISSIONER'S OFFICE
Consultation on Data Protection Impact Assessments (DPIAs) Guidance
April 12, 2018

By notice published on March 22, 2018, the UK Information Commissioner's Office ("ICO") requests public comments on "ICO and Stakeholder Consultation on the Data Protection Impact Assessments ("DPIAs") Guidance."[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits the following comments on DPIA Guidance 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, DC in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has long worked to promote transparency and accountability for information technology. EPIC has filed numerous Freedom of Information Act lawsuits[3] to compel disclosure of privacy impact assessments by federal agencies.[4] EPIC has also urged the US Federal Trade Commission to investigate private firms that create secret, proprietary algorithms to assign scores to individuals,[5] and EPIC has opposed the scoring of individuals by government.[6] EPIC's new "Privacy Impact Assessment" initiative is a key component of the organization's long-running open government project and consumer protection work. EPIC broadly promotes "Algorithmic Transparency."[7]

---

[1] ICO and Stakeholder Consultations, *Data Protection Impact Assessments (DPIAs) Guidance*, https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/data-protection-impact-assessments-dpias-guidance/

[2] About EPIC, *EPIC*, https://epic.org/epic/about.html.

[3] 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/

[4] EPIC, *EPIC Open Government*, https://epic.org/open_gov/

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

[6] *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/.

[7] EPIC, *Algorithmic Transparency*, https://epic.org/algorithmic-transparency/.

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.[8]

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 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;

[8] 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")

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

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 ICO and consult the ICO 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 ICO.

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.[9] The ICO Guidance states that it is mandatory to conduct a DPIA if the proposed

[9] 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.

processing "uses systematic and extensive profiling with significant effects."[10] 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 ICO 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 ICO 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 ICO Guidance on the data controller's obligation to conduct a DPIA.

[10] Information Commissioner's Office, *Consultation: GDPR DPIA Guidance* (March 22, 2018), https://ico.org.uk/media/about-the-ico/consultations/2258459/dpia-guidance-v08-post-comms-review-20180208.pdf

b. DPIAs as Procedural Safeguards for Automated Processing

Automated processing plays a significant role in decisions that impact individual rights and opportunities.[11] Despite the pervasiveness of algorithmic decision-making in modern society, the process remains a "black box"[12] of unproven and unexplainable outcomes.

Professor Danielle Citron and Professor Frank Pasquale address the issue of a "scored society"[13] and urge for "technological due process"[14] 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.[15]

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 right at international institutions, including UNESCO and OECD.[16]

---

[11] 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.")

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

[13] 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

[14] 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

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

[16] 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*

We believe that the current ICO Guidance is unclear on the risks of automated decision-making that trigger a mandatory DPIA under GDPR Article 35(3)-(4). The ICO 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 ICO 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."[17] In addition, "the term 'extensive' implies that the processing also covers a large area, involves a wide range of data or affects a large number of individuals."[18] 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 proprietary 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.

- Specify that "systematic" processing includes profiling users in social networks for targeted advertisements and marketing purposes.

- Specify that "systematic" processing includes behavioral analyses of personal data that may have significant and negative effects on natural persons. This type of processing also requires a DPIA and ICO consultation under GDPR Article 35(4) as a "large-scale

OECD, EPIC Renews Call for Algorithmic Transparency, https://epic.org/2017/10/at-oecd-epic-renews-call-for-a.html

[17] Information Commissioner's Office, *Consultation: GDPR DPIA Guidance* (March 22, 2018), https://ico.org.uk/media/about-the-ico/consultations/2258459/dpia-guidance-v08-post-comms-review-20180208.pdf, at 20-21.

[18] *Id.*

profiling,"[19] which the ICO promulgated in the draft DPIA Guidance as "likely to be a high risk to individuals."

- 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).

b. Significant Effect

The ICO Guidance defines "significant effect" in Article 35(3)(a) as:

"A noticeable impact on an individual [that] can affect their circumstances, behaviour or choices in a significant way. A legal effect is something that affects a person's legal status or legal rights. A similarly significant effect might include something that affects a person's financial status, health, reputation, access to services or other economic or social opportunities."[20]

- The ICO 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.[21]

- 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

[19] *Id.* at 22
[20] *Id.* at 21
[21] 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

processing, the ICO Guidance should follow Article 29 Working Party report WP251[22] 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 ICO Guidance.

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

The ICO 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 freedoms[23] 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 ICO.

2. Clarification on Biometric Data Processing

[22] *Id.*
[23] *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)

- 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.[24]

3. Quasi-Identifiers May Pose High Risks to Individuals

- The ICO 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. ICO 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 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 2002[25] 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.[26] Notably, *EPIC v. Presidential Election Commission*[27] 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 lawsuits[28] to reveal where transparency is lacking and to highlight privacy-invasive programs that lack proper assessments of their impact on privacy.

The ICO Guidance does not require publication of DPIAs. Nor are the DPIA guidelines supported by a reporting mechanism to the ICO.[29] Leading DPIA scholars Paul de Hert and

---

[24] *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)
[25] Pub. L. 107-347, 116 Stat. 2899 (2002)
[26] EPIC, *EPIC Open Government*, https://epic.org/open_gov/
[27] *EPIC v. Presidential Election Commission*, https://epic.org/privacy/litigation/voter/epic-v-commission/
[28] 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
[29] 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

David Wright have noted the value of publishing the assessments to demonstrate accountability.[30]

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 ICO. 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.

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

The ICO Guidance notes that DPIAs are a vital part of data protection by design.[31] However, the guidelines do not aid analysis of 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 Article 35.

The ICO Guidance states that "it's important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise and you should see it as an ongoing process, and regularly review it."[32] This indicates a data protection by design approach, but the Guidance does not establish specific requirements. Instead, the ICO states that "DPIAs are designed to be a flexible and scalable tool."[33] 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.[34]

- 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 must incorporate Fair Information Practices.

- DPIAs should result in data minimization.

---

[30] David Wright & Paul de Hert, *Privacy Impact Assessment* (2012), Springer, Law, Governance and Technology Series, Vol. 6. at 27.
[31] Information Commissioner's Office, *Consultation: GDPR DPIA Guidance* (March 22, 2018), https://ico.org.uk/media/about-the-ico/consultations/2258459/dpia-guidance-v08-post-comms-review-20180208.pdf, at 10
[32] *Id.* at 8
[33] *Id.* at 9
[34] § 208 of the E-Government Act (2002), United States Federal Law.

- The ICO should provide further guidance on the "legitimate interests" of the purposes of processing.

- The ICO should routinely audit and monitor to enforce data controllers to stop and inform the ICO when the DPIA identifies likely high risks to individuals.

IV. More Focus on Individual Rights than Public Trust

The ICO Guidance states: "DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals."[35] A subsequent section highlights the financial incentives to conduct DPIAs: "There can also be financial benefits. Identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on."[36]

The 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.[37] The DPIA guidelines issued by an independent data protection authority must focus on the rights and responsibilities model of the GDPR, rather than the commercial incentives for data processing companies to adopt DPIAs as a reputational tool.

V. Conclusion

EPIC appreciates the opportunity to comment on the ICO 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 ICO 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

[35] *Id.*
[36] *Id.* at 10
[37] 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