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

EUROPEAN DATA PROTECTION BOARD

Consultation on Guidelines 1/2018
Certification Criteria in Articles 42 and 43 of the General Data Protection Regulation

July 12, 2018

By notice published on May 30, 2018,[1] the European Data Protection Board ("EDPB" or "the Board") requests public comments on EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the General Data Protection Regulation ("GDPR").[2] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits the following comments to identify the risks of market-developed certification mechanisms and assessments on GDPR compliance made by third party certification bodies.

EPIC urges the Board to establish strict procedural and substantive safeguards for the certification processes in GDPR Articles 42-43 to uphold the rights of individuals and the rule of law. In order for data protection certification mechanisms to serve as a successful accountability tool for the GDPR, they must be implemented in conformity with the fundamental principles and rights of the GDPR. Therefore, the EDPB should pursue a harmonized approach to GDPR certification by (1) working with the European Commission and national data protection authorities ("DPAs") to ensure accountability and consistency in the certification standards; and (2) enforcing algorithmic transparency, privacy-enhancing techniques, and data minimization in the certification criteria.

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.[4] In response to the Cambridge Analytica data breach in March 2018, EPIC filed a Freedom of Information Act

---

[1] European Data Protection Board, *Call for Comment: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679* (May 30, 2018), https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-12018-certification-and-identifying_en

[2] European Data Protection Board, *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679* (Adopted on May 25, 2018), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_1_2018_certification_en.pdf (hereafter "EDPB Guidelines")

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

[4] EPIC, *EPIC FOIA Cases*, https://epic.org/foia/

lawsuit[5] to compel disclosure of Facebook's audits that were required by the Federal Trade Commission's 2011 Consent Order.[6] These disclosures revealed[7] that a third party auditor had wrongly certified Facebook to be in compliance with the Consent Order, thus highlighting the need for active regulatory supervision over certification schemes.

EPIC also campaigns for "Algorithmic Transparency."[8] We recently advised the UK Information Commissioner's Office and the Irish Data Protection Commissioner to protect individual rights against algorithmic profiling and discrimination by requiring the systematic implementation and publication of data protection impact assessments.[9]

I. National Data Protection Authorities Should Develop and Enforce Certification Schemes

Under GDPR Article 64(1)(c), the EDPB has a mandate to review proposals for the certification criteria to be imposed on data controllers and processors in Article 42(5), as well as the conditions for accreditation of a certification body pursuant to Article 43(3). GDPR Article 70 further enumerates the various powers of the EDPB in establishing data protection certification mechanisms, such as coordinating with the European Commission to ensure adequate safeguards in the certification criteria to reflect the values and policy goals of the GDPR. This authority is rooted in Article 63 (Consistency Mechanism), which ensures the consistent application of the GDPR throughout the European Union by tasking supervisory authorities to cooperate with each other and the Commission to set harmonized standards on the enforcement of rights and responsibilities in the GDPR.

Therefore, though it is not mandatory in Article 42 for the national DPAs to directly issue their own certification schemes,[10] doing so at a national level would be critical for consistency, accountability, and legal certainty for the wider aims of the GDPR as a harmonizing data protection law across the EU. The EDPB Guidelines should emphasize the important role of national DPAs in setting the certification criteria in their capacity as a supervisory authority with

---

[5] EPIC, *EPIC v. FTC – Facebook Privacy Assessments* (April 20, 2018), https://epic.org/foia/ftc/facebook/EPIC-v-FTC-Complaint.pdf

[6] Consent Order, *In the Matter of Facebook, Inc.*, Docket No. C-4365 (Federal Trade Commission July 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; EPIC, *In re Facebook – Cambridge Analytica*, https://epic.org/privacy/facebook/cambridge-analytica/

[7] Nicholas Confessore, *Audit Approved of Facebook Policies, Even After Cambridge Analytica Leak* (April 19, 2018), The New York Times, https://www.nytimes.com/2018/04/19/technology/facebook-audit-cambridge-analytica.html

[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; EPIC, *Comments to Irish Data Protection Commissioner on Data Protection Impact Assessment Draft Guidance* (July 3, 2018), https://epic.org/algorithmic-transparency/EPIC-Irish-DPC-Comment-DPIA.pdf

[10] *EDPB Guidelines* at 6; Article 42(5) of the General Data Protection Regulation: "A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63."

the competence to assess compliance and exercise corrective powers under Article 58.

To best ensure public accountability and the consistent application of the GDPR, national DPAs should issue the certification criteria in consultation with the EDPB and the European Commission, and directly administer the scheme without delegating the assessment to independent third parties or market actors that have no responsibility to the public.

We draw this recommendation from two practical examples that illustrate the lack of competence and reliability of market-based certification bodies.

(1) Deceptive TRUSTe Certification Program

In 2014, the Federal Trade Commission ("FTC") settled charges that TRUSTe, a company that provides privacy certifications for online businesses including children's privacy and the (now repealed) US-EU Safe Harbor program, deceived consumers through its privacy seal program.[11]

TRUSTe had offered a variety of assessments and certifications, monitoring tools, and compliance controls to companies. It issued seals of approval which represented to consumers, competing businesses, and regulators, as demonstrating compliance with the best privacy practices and rigorous assessments for re-certification. However, TRUSTe failed in its role as a certification body to verify the privacy practices of companies that collected and disclosed consumer data. TRUSTe also misrepresented its status as a for-profit entity to the public that relied on its certification decisions to put their trust on the services of particular companies.

The FTC charged TRUSTe with failure to conduct re-certifications for companies that displayed privacy seals.[12] TRUSTe had materially misrepresented the level of privacy safeguards implemented by the certified companies, and failed to hold companies accountable for their privacy representations.

(2) Facebook Audits by PricewaterhouseCoopers ("PWC")

The FTC's 2011 Consent Order with Facebook "required, within 180 days [of the entry of the Consent Decree], and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected."[13]

On March 16, 2018, Facebook admitted to the unlawful transfer of 87 million user

[11] Federal Trade Commission, Press Release, *TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program; Company Failed to Conduct Annual Recertifications, Facilitated Misrepresentation as Non-Profit* (November 17, 2014), https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its

[12] Consent Order, *In the Matter of TRUSTe, Inc*., (Federal Trade Commission, November 17, 2014), https://www.ftc.gov/system/files/documents/cases/141117trusteagree.pdf

[13] *Id.*

profiles to the data mining firm Cambridge Analytica.[14] In April 2018, EPIC filed a Freedom of Information Act ("FOIA") lawsuit[15] to obtain the release of the unredacted Facebook Assessments and all records concerning the third party auditor approved by the FTC.

Records obtained by EPIC revealed that Facebook's third party auditor, PWC, had approved Facebook's privacy practices as being in compliance with the FTC Consent Order even after Facebook became aware of the misuse of millions of user profiles by Cambridge Analytica. PWC represented: "In our opinion, Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information."[16] Due to the unaccountable and incompetent review by a third party auditor, Facebook continued its practices without reporting the breach to the FTC. Facebook discovered this violation in 2015 but did not inform the public until this year.[17]

The consequences of an incorrect third party assessment of Facebook's data practices were immense, and imperiled both user privacy and the integrity of democratic institutions. Relying on the data provided by Facebook, a Cambridge University researcher collected the private information of approximately 270,000 users and their extensive friend networks under false pretenses as a research-driven application.[18] The data from 87 million profiles was subsequently transferred to Cambridge Analytica, a political consulting firm hired by President Trump's 2016 election campaign that offered services that could identify personalities of voters and their voting behavior.[19] Cambridge Analytica engaged in the illicit collection of Facebook user data from 2014 to 2016,[20] encompassed by the reporting periods of the mandatory audits.

This significant example illustrates why regulatory authorities must take an active role in determining the certification criteria and assessing compliance with data protection laws. It would derogate public trust in the GDPR if national DPAs were to delegate this important function to market-driven certification bodies and third party auditors.

(3) European Harmonization of Data Protection Laws

A 2017 report prepared for the European Commission's Directorate-General for Justice

---

[14] Press Release, Facebook, *Suspending Cambridge Analytica and SCL Group from Facebook* (Mar. 16, 2018), https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/ [hereinafter "Facebook Press Release"].

[15] EPIC, *EPIC v. FTC – Facebook Privacy Assessments* (April 20, 2018), https://epic.org/foia/ftc/facebook/EPIC-v-FTC-Complaint.pdf

[16] Previously available on Federal Trade Commission website: https://www.ftc.gov/system/files/documents/foia_requests/3_2017-00270.pdf. Reported on Nicholas Confessore, *Audit Approved of Facebook Policies, Even After Cambridge Analytica Leak* (April 19, 2018), The New York Times, https://www.nytimes.com/2018/04/19/technology/facebook-audit-cambridge-analytica.html

[17] Facebook Press Release

[18] EPIC, *In re Facebook – Cambridge Analytica*, https://epic.org/privacy/facebook/cambridge-analytica/

[19] Matthew Rosenberg, Nicholas Confessore, & Carole Cadwalldr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[20] *Id.*

and Consumers entitled 'Recommendations for Improving Practical Cooperation between European Data Protection Authorities'[21] supported a harmonized approach to ensure consistent and trustworthy certification mechanisms across member states:

> Certification raises a particular challenge in that some DPAs have already very established certification schemes, whilst others have embryonic schemes, and the majority do not engage in certification at all.[22]
>
> Therefore a harmonised position will be challenging to reach, but offers great benefits in terms of communication and awareness of certification schemes as well as in relation to certifications that easily and smoothly cross borders.

EPIC believes that any certification and audit process for the GDPR must engage the collective cooperation of European supervisory authorities to (1) ensure consistent criteria that reflect the substantive rights and responsibilities of the GDPR, (2) facilitate effective communication and feedback between the DPAs to mutually assist in enforcing compliance, and (3) implement certification mechanisms with the highest standard of data protection and privacy.

II. Certification Criteria Should Uphold Substantive GDPR Rights and Responsibilities

The EDPB Guidance states in 'The Development of Certification Criteria'[23]:

> The GDPR established the framework for the development of certification criteria. Whereas fundamental requirements concerning the procedure of certification are addressed in Articles 42 and 43 while also providing essential criteria for certification procedures, the basis for certification criteria must be derived from the GDPR principles and rules and help to provide assurance that they are fulfilled.
>
> The development of certification criteria should not only consider market demand, but for successful approval, also verifiability, significance, and suitability of certification criteria to demonstrate compliance with the Regulation must be taken into account.

Certification criteria approved by a supervisory authority pursuant to Article 42(5) must protect individual rights and freedoms from extensive and intrusive data processing. Certification guidelines issued by the EDPB must focus entirely on the rights and responsibilities of the

---

[21] David Barnard-Wills, Vagelis Papakonstantinou, Cristina Pauner & José Díaz Lafuente, *Recommendations for improving practical cooperation between European Data Protection Authorities* (January 2017), http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA2_D41_final_20170114.pdf

[22] Rodrigues, Rowena, David Barnard-Wills & Vagelis Papakonstantinou, *The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR,* International Review of Law, Computers & Technology, Vol.30, No. 3, 2016, pp. 246-270.

[23] *EDPB Guidelines* at 10

GDPR, rather than the market demand to use certification as a reputational tool.

EPIC recommends the EDPB to provide substantive guidelines on developing certification criteria that require algorithmic transparency, privacy-enhancing techniques, and data minimization.

(1) Algorithmic Transparency in Certification Criteria

Automated processing plays a significant role in decisions that impact individual rights and opportunities.[24] Despite the pervasiveness of algorithmic decision-making in modern society, the process remains a "black box"[25] of unproven and unexplainable outcomes. We must know the basis of decisions, whether right or wrong. But as decisions are automated, and organizations increasingly delegate decision-making to techniques they do not fully understand, processes become more opaque and less accountable.

Professor Danielle Citron and Professor Frank Pasquale address the issue of a "scored society"[26] and urge for "technological due process"[27] 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.[28]

The GDPR empowers supervisory authorities 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

---

[24] 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.")

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

[26] 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

[27] 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

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

(automated decision-making and profiling) establish baseline safeguards to automated decision-making and profiling. Furthermore, the EDPB is empowered by Article 70(1)(f) to "issue guidelines, recommendations and best practices […] further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2)."

To achieve a consistent application of the GDPR and a harmonized approach to certification that upholds algorithmic transparency, the EDPB should develop certification criteria that require data controllers and processors to disclose the logic of the processing of algorithms, and to stop processing when profiling risks are identified. For this purpose, the EDPB should collaborate with national DPAs to formulate guidance on the level of transparency required to provide "meaningful information" to data subjects, and the extent to which data controllers must explain the algorithm's "logic process" in order to earn certification under Article 42.

(2) Privacy Enhancing Techniques and Data Minimization in Certification Criteria

The EDPB Guidance should require certification criteria to include organizational and technical processes to minimize the collection of personal data. EDPB and national DPAs should administer certification schemes with the purpose of promoting privacy-enhancing techniques that protect individual rights against preventable risks.

The scope and method of evaluation for certification should scrutinize the categories and amount of data collected, and the technical infrastructure deployed for processing—taking into account the nature, scope, content and purposes of the processing as well as the risks to the rights and freedoms of the concerned individuals.

Certification under Article 42 should impose core requirements that aim to minimize the collection of sensitive data and eliminate secondary uses of data that pose additional risks. Evaluation should also require a conscious and systematic effort[29] by the data controller at each step of the processing operation to 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.

EPIC makes the following suggestions for certification assessments:

- Certification procedures 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.

- Immediate re-certification should be mandatory for new technologies that collect more granular data on individuals or possess the capacity to collect larger quantities of data. National DPAs and the EDPB should assess whether the collection of this data is necessary or proportionate, and prohibit the excessive collection of data that pose a risk

[29] 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.

to individual rights.

- Certification should never be granted for data controllers engaging in data collections exceeding their purpose, or unspecified processing.

- Certification should increase accountability and transparency, and give data subjects greater access and control of their data.

- Certification should not make false representations of privacy standards to deceive consumers.

- Supervisory authorities should make clear to the public that GDPR certification under Article 42 does not equal GDPR compliance, which is an ongoing obligation.

III. Conclusion

EPIC appreciates the opportunity to comment on the consultation for the EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the GDPR. We urge the EDPB and national DPAs to establish strong procedural and substantive safeguards for certification mechanisms to ensure accountability for individual rights and the rule of law.

Respectfully Submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Sunny Seon Kang
Sunny Seon Kang
EPIC International Consumer Counsel