

## UK Information Commissioner's Office Publishes Consultation Paper on Profiling and Automated Decision-Making under GDPR

Article By:

Daniel P. Cooper

---

On April 2, 2017, the **Information Commissioner's Office ("ICO")** released a consultation paper for **UK** organizations to comment on how the new profiling provisions under the **General Data Protection Regulation ("GDPR")** could be interpreted and applied when the GDPR comes into force in May 2018.

The public consultation on what is described as "initial thoughts on some key issues" which require "further debate" expires on April 28, 2017. Stakeholders and the public can review the paper and provide their views on the [ICO's website](#). The ICO will then publish a summary of the feedback it receives. Guidance on profiling is anticipated from the **Article 29 Working Party**, which has prioritized it for release in 2017.

Profiling under the GDPR is the automated processing of personal data to evaluate personal aspects of an individual, in particular to analyze or predict professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. In interpreting this definition, the ICO has asked for feedback on whether stakeholders agree that there must be "a predictive element, or some degree of inference for the processing to be considered profiling."

The ICO suggests that sources of data for profiling may include: an individual's internet and browsing history; education and professional information; credit-rating assessments and financial data; property ownership and location data; wearable tech and the internet of things; social network information; and lifestyle and behavior data gathered from mobile phones and other devices.

The GDPR specifically regulates profiling and introduces new obligations for data controllers, applying to profile creation and automated decision-making. The GDPR provisions go beyond those arising under the Data Protection Directive 95/46, and implementing Member State legislation, such as the UK Data Protection Act 1998, in order to address the perceived additional risks arising from profiling. The ICO consultation paper specifically references the following risks:

- infringement of fundamental rights and freedoms;

- 
- underrepresentation of certain sectors of society;
  - use of non-sensitive personal data to deduce sensitive personal data;
  - unjustifiable deprivation of services or goods;
  - risk of commercial use of information without individuals' knowledge; and
  - loss of data accuracy.

To protect against these risks, the GDPR requires organizations to safeguard individuals' rights and freedoms when carrying out profiling, by using appropriate mathematical or statistical procedures and introducing technical and organizational measures to avoid and correct errors, bias, or discrimination. The paper suggests that organizations may need to implement the following safeguards:

- measures that identify and quickly resolve any inaccuracies in personal data;
- security appropriate to the potential risks to the interests and rights of the data subject;
- safeguards to prevent discriminatory effects on individuals on the basis of special categories of personal data;
- specific measures for data minimization and clear retention periods for profiles;
- anonymization or pseudonymization techniques in the context of profiling; and
- a process for human intervention in defined cases.

The paper proposes that organizations may need to consider introducing codes of conduct for auditing processes involving machine learning; accountability/certification mechanisms for algorithm-based decision making; algorithmic audition; and ethical review boards to assess potential harms and benefits of profiling mechanisms. The ICO has asked stakeholders to suggest other mechanisms and measures to test the effectiveness and fairness of systems in order to comply with GDPR requirements.

Safeguards and controls are also required to ensure data minimization (restricting data to what is "strictly necessary" to meet the purpose(s) of processing), accuracy and appropriate retention periods. To ensure accuracy, the ICO advises organizations to have robust procedures in place to protect the quality and accuracy of personal data being processed to ensure it is free from errors and bias which may be present in the dataset, notwithstanding the accuracy of recording mechanisms. The consultation paper makes limited comment in relation to data retention periods, which are not specified in the GDPR, advising that organizations regularly review data sets to ensure they remain relevant for the purpose(s) of processing. The ICO has asked organizations to provide feedback on what controls and safeguards they will use to ensure relevance, accuracy and appropriate retention periods.

As well as ensuring data meets the purpose(s) of processing, businesses must also ensure that they

---

document the legal basis of processing, such as consent, or that the processing is “necessary” for the performance of a contract or for the purposes of the legitimate interests of the controller or a third party. Organizations are asked to inform the ICO how they intend to demonstrate that processing is necessary, for example, to achieve a particular business objective.

The provisions of the GDPR focus on profiling that has a “legal” or “significant” effect on individuals, allowing organizations to engage in profiling where it has little or no impact. For example, according to the ICO, profiling can be used to align prices and offers of goods and services with individual consumer demand; facilitate improvements in medicine, education, healthcare and transportation; provide wider access to credit using different methods to traditional credit-scoring; and analyze and prevent risks and fraud.

The ICO also offers some practical thoughts on what may amount to profiling producing “legal” or “similarly significant” effects. The GDPR does not define “legal” or “significant”, but the paper suggests that a legal effect “might be something that adversely impacts an individual’s legal rights, or affects their legal status.” A significant effect might be “more than trivial” with potentially unfavorable outcomes. Feedback is requested on how organizations understand these terms, as well as how organizations will ensure that their profiling is “fair, not discriminatory, and does not have a unjustified impact on individuals’ rights.” Going forward, the ICO recommends that organizations be aware of processing which:

- causes damage, loss or distress to individuals;
- limits rights or denies an opportunity;
- affects individuals’ health, well-being or peace of mind;
- affects individuals’ financial or economic status or circumstances;
- leaves individuals open to discrimination or unfair treatment;
- involves the analysis of the special categories of personal or other intrusive data, particularly the personal data of children;
- causes individuals to change their behaviour in a significant way; or
- has unlikely, unanticipated or unwanted consequences for the individual.

Individuals may object to processing, including profiling, carried out for the performance of a public task or legitimate interests. However, organizations can refuse to cease processing where they can show compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject, or otherwise where data is processed in relation to legal claims. Rather than provide examples of what might constitute “compelling legitimate grounds” at this stage, the ICO has requested feedback on what factors stakeholders consider would satisfy this test.

This is the ICO’s second topic-specific review of the GDPR, following draft guidance on consent released on March 2, 2017. More guidance is expected on the topic of profiling from the Article 29 Working Party, which also intends to release guidance on such topics as transparency, certification, breach notification and data transfers, which will supplement their previous guidance on Data

Portability, Data Protection Officers and the One Stop Shop.

*Rosie Klement is co-author of this article.*

© 2024 Covington & Burling LLP

---

National Law Review, Volumess VII, Number 101

Source URL: <https://natlawreview.com/article/uk-information-commissioner-s-office-publishes-consultation-paper-profiling-and>