ICO’s Feedback request on profiling and automated decision-making: summary of responses

Introduction

In April 2017 the ICO issued a request for feedback on profiling. We wrote a discussion paper summarising what we considered to be the key issues in the GDPR provisions on profiling and automated decision making, and posed a number of questions.

Overall we received 86 responses, broken down as follows:

- 52 private sector
- 19 public sector
- 8 third sector
- 7 private individuals

A wide variety of issues were raised and we are grateful to all those who took time to provide input. We have used this feedback to contribute to our work as lead drafters of the Article 29 Working Party (WP29) guidelines on profiling and automated decision-making.

Key themes

General issues:

- The potential burden that the new transparency requirements around profiling place on controllers and how to provide meaningful information to data subjects without overload.

- Whether or not certain activities would or wouldn’t be considered profiling – concern was expressed that the definition is unclear.

- Automated decision making, including profiling under Article 22:

    - How much human involvement (and at what point of the process) is required to take the processing out of the ‘solely automated’ category?
    - What are legal and similarly significant effects? For example, can direct marketing ever have a significant effect on individuals?

  - What derogations will be available in UK law to permit automated decision making, including profiling?
  - What sort of appropriate procedures can prevent discriminatory effects and how would we assess them?

Profiling definition and its use

Respondents said that they carry out profiling:

- to better understand the market in which they operate, provide tailored services and deliver more relevant targeted advertising;
- for underwriting and fraud prevention purposes;
- to track individuals' movements and behaviour;
- to understand and find the answer to a problem, for example to detect patterns of disease or which employees are likely to leave a company.

Respondents suggested that sometimes machines make better decisions than people and are arguably more consistent.

A large percentage of submissions commented that clear guidance is required on what profiling is and what it is not; including when the Article 22 provisions have effect.

There was a fairly even split between those who considered that there had to be an element of inference for processing to be considered profiling, and those who thought profiling did not necessarily involve prediction.

ICO's comment

The GDPR definition of profiling includes 'analysis' as well as 'prediction' so profiling will have a wide scope and doesn't have to include inference.

Fairness

Respondents expressed the following views:

- transparency isn't just about privacy notices, but the ongoing education of individuals so they can understand how their data is being used and how to exercise their rights;
- organisations need to understand themselves how the algorithms they are using work, so they can better explain them not just to their own customers but to the regulator;

- personal data processing should be backed up by strong governance, including policies and procedures that assess the risks of use of data and impact on individuals' rights.

Respondents raised other concerns:

- the need for clear privacy notices to explain the use of personal data. Explaining profiling in a way that most individuals can understand will be demanding for many businesses;
- methods of profiling change quickly and evolve – the requirement for privacy notices to be updated prior to processing will present a cost and time challenge, and could result in information overload for individuals.

Suggestions included:

- layered privacy notices that were easy to understand as a helpful way of conveying information;
- businesses to review their internal rules and guidelines and use DPIAs to ensure that any profiling undertaken is done so fairly and in a non-discriminatory manner;
- using anonymised data and avoiding discriminatory variables as ways to potentially minimise adverse effects.

Accuracy, relevance and retention

One respondent summed it up by stating that using old, out of date information defeats the purpose for profiling.

Comment was passed that in the financial services sector there can be a tension between the GDPR requirement to minimise the collection of personal data and financial services regulations that require the collection and processing of large amounts of personal data. For example, money laundering regulations require firms to retain customer records and records of clients' instructions for five years after the end of the business relationship.

Other feedback suggested:

- development of codes of practice or certification schemes covering the principles of data minimisation, accuracy and retention;
- preference centres for individuals to access and update or amend their own personal information;
- different retention or refreshment periods for more time sensitive variables;

- automatic deletion for profiling data not used or updated within a specific timeframe;
- refreshing personal data at regular intervals throughout the year to ensure relevance before overwriting profile data;
- the ICO to provide guidance on minimum standards in relation to record keeping of profiling activity.

ICO's comment
The ICO would be unable to provide guidance on this aspect given the scope for different retention schedules based on industry recommendations and other regulatory requirements.

Lawful basis for processing

Respondents indicated that consent would be used on a limited basis and in fact was unlikely to be practical for a number of them, particularly those from the public sector. Some responses said that the basis for processing might change depending upon the type of profiling carried out.

Some private sector respondents indicated that profiling might be necessary for contractual purposes, however legitimate interests might be a more appropriate lawful basis. Reference was made to the balancing test in WP29 Opinion 06/2014 on legitimate interests as a useful tool when considering this option.

There were suggestions that it would be useful for clear guidance on what 'necessary for the performance of a contract' means with supporting examples.

ICO's comment
Recital 45 says that Member State law can cover processing carried out under Article 6(1)(c)(compliance with a legal obligation) and 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority).

As indicated under 'Next Steps', the Data Protection Bill has had its initial reading in Parliament and we await further developments on this issue.

Special category data

Many respondents, particularly those in the direct marketing sector, indicated that they do not routinely collect sensitive information from individuals. A number of organisations accepted however that one of the biggest risks of profiling was the inadvertent inference of special category data (SCD). Approaches ranged from those who said they would go on to seek explicit consent from the data subject, and those who said that any SCD accidentally found would not be further processed or recorded.

Those that regularly process special category data, for example, public sector organisations and the health and insurance industry, said that they needed clarification about:

- the lawful bases for processing and what derogations might be available for them;
- what purposes might reasonably be considered to be in the 'substantial public interest'.

Transparency and fair processing

Layered privacy notices and just in time notices at the point of data collection are the most popular ways organisations believe they can achieve transparency. They recognise that information should be easily accessible and in a prominent position on websites.

Respondents expressed the following views:

- 'meaningful' implies that information given should be understandable to the user;
- there are inherent difficulties in explaining how algorithms work and individuals' general ability to understand machine learning;
- the logic of decision-making and amount of detail to be provided could be confusing and create more uncertainty;
- too much information might overwhelm consumers.

Some responses emphasised that in certain circumstances the purpose for the processing might outweigh individuals' rights to have complete transparency – for example automated decision-making carried out in order to accurately assess risk or prevent fraud.

There was some concern about protecting commercial confidentiality and trade secrets – for example revealing too much information about risk assessment and the weighting allocated to each area may allow the system to be manipulated.

Responses highlighted that clear guidance would be useful on what is considered a 'timely' period to give fair processing information when personal data has been obtained indirectly.

ICO's comment
The forthcoming transparency guidelines from WP29 will cover this aspect in more detail.

Objections to profiling

Views expressed on compelling legitimate grounds for overriding an objection to profiling included:

- the wider interests of society as a whole, for example areas such as national security and the prevention of crime;
- fraud detection and prevention;
- critical business interests.

Respondents also said that they would welcome clarification on:

- what constitutes compelling legitimate grounds for data controllers;
- legitimate interests generally as a basis for processing given that the right to object arises only where the processing is on the basis of 6(1)(e) performance of a public task or 6(1)(f) legitimate interests of the controller;
- the alignment of the E-privacy regulation with the GDPR.

Some respondents suggested that organisations could use the DPIA process to identify their compelling legitimate grounds for processing as part of the risk assessment.

Solely automated

Respondents requested more clarity on what this means and what type of situations Article 22(1) is designed to protect against. They expressed the following views:

- a common sense approach interprets this as excluding any human action that influences or affects the outcome;
- a decision making process that is totally automated and exercises no human judgement in its output;
- human involvement is where someone has the opportunity to consider whether a decision is unfair and the capability/willingness to alter it.

Other feedback suggested that:

- Article 22(1) wouldn’t apply where a human weighs up and interprets the result of an automated decision; however it might apply where a human loads the data to be processed and the decision making is carried out by a machine;
- whether a process is solely or partly automated depends on the degree of human involvement;

- individuals responsible for overseeing profiling should be suitably experienced and possess other qualities such as relevant qualifications, professional body membership, adherence to Codes of Conduct and accreditations

Legal and similarly significant effects

Although the GDPR does not specifically state that the ‘effect’ has to be negative for A22 to be engaged, most believed this to be the case.

The majority of respondents agreed with the ICO view on what would constitute a legal effect although views on what might be ‘similarly significant’ were more wide ranging.

One comment considered that a significant effect might be a result of profiling activity that influences the ability of an individual to receive an ‘equal’ and unbiased service in comparison to a peer.

There was widespread belief among respondents carrying out direct marketing that showing someone an advert won’t generally have a significant effect on them.

Respondents expressed concern that if the regulatory approach was too rigid it would stifle business operations.

A large percentage of submissions highlighted the need for:

- clarity on the meaning of legal and similarly significant effects;
- a set of examples highlighting what might constitute a significant effect and contrasting these with examples of minor effects.

There was a general consensus that levels of impact will depend upon the context. Respondents suggested that the following may help assess the level of impact:

- a risk based approach considering factors such as whether the decision has an impact on a right or freedom, for example the right to freedom of expression;
- consideration of what the decision enables the individual to do or prevents them from doing and whether this would more likely than not be noticed by a notional, reasonable individual sharing the same characteristics;
- the guidelines previously issued for breach management, for example whether sensitive personal data is involved or whether there are financial consequences.

ICO's comment
It is expected that the forthcoming WP29 guidelines on profiling will comment on this issue.

Safeguards

Most respondents considered that safeguards are still relevant even in cases where the decision is not solely automated.

A number of private sector respondents and privacy campaigners highlighted the importance of developing an ethical corporate culture and set of common standards to prevent discriminatory effects of profiling.

Respondents said that the following would be helpful:

- examples of good and bad practice;
- benchmarking;
- guidance for self-assessment.

Other responses suggested observing or developing codes of conduct to:

- secure an ethical, scientific and quality approach to the collection of customer data;
- test the effectiveness and fairness of systems in automated decision-making.

One comment mentioned the principles of the Fair Data Accreditation scheme, incorporating the need for:

- profiling to be carried out by qualified and competent professionals;
- informed transparent consent by the data subject;
- confidential treatment of personal data; and
- protection of participants to engender consumer trust.

DPIA

For most it seemed logical that organisations involved in profiling would need to carry out a DPIA. The private sector in particular indicated that effective DPIAs would be a key part of their information governance procedures.

Smaller organisations raised concerns over the potential administrative burden on staff and the challenge of carrying out the required changes in the time available.

Respondents said that carrying out a DPIA linked back to whether or not the processing had a legal or similarly significant effect and that they needed more guidance from the ICO.

Clarification was sought on whether a DPIA would only be required when the risk to rights and freedoms is high or where both limbs of Article 35(3)(a) are met.

ICO's comment
The recently published WP29 guidelines provide more information on DPIAs.

Children

Many respondents indicated that they would support lowering the age of consent to 13.

They also expressed the following concerns:

- collecting date of birth information in order to establish whether someone is a child could lead to excessive collection of personal data;
- children will often be present in households where profiling is carried out – for example, insurance companies for family travel purposes, housing associations to assess living accommodation requirements, vulnerability assessments – so clarification is required on how this processing can lawfully continue under the GDPR;
- the development of specific disease or health event models may include children as a target cohort.

Next steps

The WP29 guidelines on profiling are due to be adopted by the end of the year and we will then consider whether we need to supplement them with further UK specific guidance; however we won't be looking to duplicate or 'gold plate' the WP29 guidelines.

Sectoral guidance may be useful and we encourage the preparation of codes of conduct by trade associations and other bodies (as recommended in Article 40 of the GDPR). Having common standards for certain sectors or industry that encompass some best practice examples would assist organisations in meeting their obligations.

On 13 September the Data Protection Bill entered Parliament. Although profiling itself is not specifically mentioned, the bill includes provisions for the safeguards on automated decision-making authorised by law (Article 22(2)(b)).

We are also developing our Guide to the GDPR, as well as more specific guidance on other areas such as children's data and the lawful bases for processing, including legitimate interests. You can keep up to date on what guidance to expect and when by checking the data protection reform pages of our website.