

# Feedback request – profiling and automated decision-making

## Contents

Contents .....	1
Feedback request.....	2
Background .....	3
1. The definition of profiling.....	8
2. Transparency .....	9
3. Data minimisation, accuracy and retention .....	11
4. Lawful processing .....	13
5. Information to be provided to individuals .....	15
6. Rectification and objection to profiling.....	17
7. Automated individual decision-making, including profiling .....	19
8. Implementing appropriate safeguards .....	21
9. Data protection impact assessment (DPIA) .....	22
10. Children and profiling .....	23
Feedback request form .....	24

## Feedback request

We are asking for your feedback and comments on the new profiling provisions in the General Data Protection Regulation (GDPR).

Profiling is specifically addressed in the GDPR and there are new obligations for data controllers to consider. Our stakeholders have identified profiling as an area of concern and the Article 29 Working Party (WP29) has prioritised it for guidance.

This paper only covers certain aspects of profiling in the GDPR. It should not be interpreted as guidance.

It represents our initial thoughts on some key issues that we consider require further debate. Your responses will help inform the UK's contribution to the WP29 guidelines due to be published later this year.

You don't need to respond to every question, only the ones that are relevant to you. The deadline for responses is 28 April. Please email your responses to [profiling@ico.org.uk](mailto:profiling@ico.org.uk).

If you would like further information please telephone 0303 123 1113 and ask to speak to Karen Harris.

### Privacy statement

After the deadline has passed we will publish a summary of responses we receive. Feedback information you provide to us, including personal information, may be disclosed in accordance with the Freedom of Information Act 2000 and the Data Protection Act 1998. If you want the information that you provide to be treated as confidential please tell us, but be aware that we cannot guarantee confidentiality.

# Background

## What is profiling?

Profiling can enable aspects of an individual's personality or behaviour, interests and habits to be determined, analysed and predicted.

Profiling has already found its way into many areas of life in the form of consumer profiles, movement profiles, user profiles and social profiles.

Profiling is not always visible and may take place without an individual's knowledge.

## Sources of data used in profiling

Types of data used to build up a picture of an individual include but are not limited to the following:

- internet search and browsing history;
- education and professional data;
- data derived from existing customer relationships;
- data collected for credit-worthiness assessments;
- financial and payment data;
- consumer complaints or queries;
- driving and location data;
- property ownership data;
- information from store cards and credit cards;
- consumer buying habits;
- wearable tech, such as fitness trackers;
- lifestyle and behaviour data gathered from mobile phones;
- social network information;
- video surveillance systems;
- biometric systems;
- internet of things; and
- telematics.

## How profiling is used

Profiling is no longer simply a matter of placing individuals into traditional interest buckets based on purchases that they show an interest in, for example, sports, gardening or literature. Profiling in today's digital economy involves sophisticated technologies and is widely used in a variety of different applications, until recently with relatively limited publicity.

Profiling technologies are regularly used in marketing. Many organisations believe that advertising does not generally have a significant adverse effect on people. This might not be the case if, for example, the use of profiling in connection with marketing activities leads to unfair discrimination.

One study conducted by the Ohio State University revealed that behaviourally targeted adverts can have psychological consequences and affect individuals' self-perception. This can make these adverts more effective than ones relying on traditional demographic or psychographic targeting.<sup>1</sup>

For example, if individuals believe that they receive advertising as a result of their online behaviour, an advert for diet products and gym membership might spur them on to join an exercise class and improve their fitness levels. Conversely it may make them feel that they are unhealthy or need to lose weight. This could potentially lead to feelings of low self-esteem.

## Profiling and the GDPR

Article 15 of the Data Protection Directive 95/46/EC (Directive) already contained provisions on automated decision making, reflected in section 12 of the Data Protection Act 1998 (DPA). At that time decisions made by purely automated means without any human intervention were relatively uncommon.

The widespread availability of personal data on the internet and advances in technology, coupled with the capabilities of big data analytics mean that profiling is becoming a much wider issue, reflected in the more detailed provisions of the GDPR.

In May 2013 WP29 produced an advice paper<sup>2</sup> on how the connection and linking of personal data to create profiles could have a significant impact on individuals' basic rights to data protection, even though it is in itself a neutral process.

---

<sup>1</sup> Reczek, Rebecca Walker, Summers, Christopher and Smith, Robert. Targeted ads don't just make you more likely to buy – they can change how you think about yourself. Harvard Business Review, 4 April 2016. <https://hbr.org/2016/04/targeted-ads-dont-just-make-you-more-likely-to-buy-they-can-change-how-you-think-about-yourself> Accessed 3 April 2017

<sup>2</sup> Article 29 Data Protection Working Party. Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, 13 May 2013. [http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513\\_advice-paper-on-profiling\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf) Accessed 4 April 2017

WP29 felt that more needed to be done to explain and mitigate the various risks that profiling can pose. They considered that the forthcoming data protection regulation should include a definition of profiling and specific provisions for this activity. This proposal then formed the basis for the definition in the final GDPR text. The definition of profiling is discussed in more detail below.

## Key GDPR provisions

Article 4(4)

## Profiling definitions

The Oxford English dictionary describes profiling as:

“the recording and analysis of a person’s psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people”

Other definitions exist to explain what a profile is and what profiling means:

“‘Profile’ refers to a set of data characterising a category of individuals that is intended to be applied to an individual”<sup>3</sup>

“the drawing of inferences about an individual instance within a population, by searching for those that exhibit patterns associated with a particular, previously computed profile, or with a profile generated from the data-set itself. This produces a set of suspect (id) entities, possibly ranked in priority order”<sup>4</sup>

Broadly speaking, we consider profiling to mean gathering information about an individual or group of individuals and analysing their characteristics or behaviour patterns in order to place them into a certain category or group, and/or to make predictions or assessments about their:

- ability to perform a task;

---

<sup>3</sup> Council of Europe. The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 and explanatory memorandum. Council of Europe 23 November 2010. [https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec\(2010\)13E\\_Profiling.pdf](https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf). Accessed 4 April 2017

<sup>4</sup> Clarke, Roger. Quality Assurance for Security Applications of Big Data. 2016 European Intelligence and Security Informatics Conference. <http://www.csis.pace.edu/~ctappert/papers/proceedings/2016EISIC/data/2857a001.pdf>. Accessed 4 April 2017

- interests; or
- likely behaviour.

## Benefits and risks

Organisations may perceive profiling to be beneficial. However, this does not necessarily make it fair. Nor does it remove the requirement to inform an individual about the processing and how to exercise their rights.

Profiling activity can have an impact even if no decisions are made on the basis of the profiles. This is because of the potential for the data to be harvested or mined for information and its commercial value.

The following table highlights some of the more widely recognised benefits and risks of profiling.

Benefits	Risks
Better market segmentation	Infringement of fundamental rights and freedoms
Permits analysis of risks and fraud	Certain sectors of society may be underrepresented – eg older generation/vulnerable individuals or those with limited social media presence
Adapting offers of goods and services as well as prices to align with individual consumer demand	Can be used to deduce sensitive personal data from non-sensitive personal data, with a reasonable degree of certainty
Improvements in medicine, education, healthcare and transportation	Unjustifiable deprivation of services or goods
Provide access to credit using different methods to traditional credit-scoring	Risk of data broking industry being set up to use information for their own commercial interests without individuals' knowledge
Can provide more consistency in the decision making process	Using profiling techniques can jeopardise data accuracy

## The effect of profiling on individuals

The GDPR provisions, discussed in more detail within the body of this paper, focus on profiling that has a “legal” or “significant” effect on individuals, rather than profiling that has little or no impact.

The GDPR provides limited examples<sup>5</sup> of activities where using automated processing (including profiling) would have a significant effect on an individual:

- automatic refusal of an online credit application; or
- e-recruiting practices without any human intervention.

Initial thoughts on other significant effects of profiling include processing that:

- 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 individuals.

It may be useful to establish an external recognised standard to measure such effects, instead of simply relying upon the subjective view of the controller or the data subject.

## How the GDPR addresses profiling

The Directive focussed on the outcome of automated decision-making (which could include profiling) rather than the act of profiling itself.

The GDPR applies to profile creation as well as to automatic decision-making using profiling.

In addition to the definition of profiling, the GDPR introduces other new rights for data subjects and obligations for controllers. These extra elements provide for greater transparency and more individual control when profiling is being carried out on personal data, such as additional information requirements and greater accountability.

### **Key GDPR provisions**

Article 4(4), 9, 22 and Recitals 71 and 72

---

<sup>5</sup> GDPR Recital 71

# 1. The definition of profiling

Article 4(4) defines profiling as follows:

“Any form of **automated processing** of personal data consisting of the use of personal data to **evaluate certain personal aspects** relating to a natural person, **in particular to analyse or predict aspects** concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”

## Automated processing

Article 4(4) makes no mention of “solely” automated processing, unlike Article 22(1). It is debatable therefore whether “automated processing” means purely automated, or whether human involvement at any stage takes the processing out of the definition.

## Evaluate certain personal aspects...in particular to analyse or predict ....

We interpret this to mean taking and assessing known elements about someone, and analysing or predicting something about their behaviour in order to make a decision about them. The definition appears to include the analysis of personal aspects as well as processing that has a predictive element.

An organisation might simply use information provided directly by its customers and verified as being factually accurate. It might also combine this with other known data, such as publicly available information.

### Key GDPR provisions

Article 4(4)

## Feedback request

### Q1

When, how and why does your organisation carry out profiling? Do you agree that there has to be a predictive element, or some degree of inference for the processing to be considered profiling?

## 2. Transparency

### Fairness, transparency and purpose limitation

Individuals provide and organisations acquire personal data in order to meet some specific business need, or fulfil a particular purpose.

Organisations provide fair processing information so that individuals understand why their personal data is being processed, and the data is processed to achieve this aim.

Profiling is not as transparent as other forms of processing. Although profiling itself is a neutral process, a controller can use it to make a decision about someone that could have a significant impact on them, or other unforeseen consequences. It can emphasise existing stereotypes, social segregation, and limit individual choice and equal opportunities.

Profiling also creates new data that needs to be GDPR compliant in its own right.

The fact that profiling can use data from a variety of sources to create derived or inferred data raises the following issues:

- how to give effective and timely fair processing; and
- what individuals might reasonably expect.

If organisations are re-using publicly available personal data or personal data obtained from a third party organisation they should consider whether any third party privacy notice adequately describes the circumstances in which the data will be further processed and whether the further processing is compatible with the original purpose.

It is not always obvious how organisations might use information generated by seemingly unrelated transactions, or what the consequences might be. If individuals are unaware that profiling is taking place, they will find it difficult to exercise their rights around this new data.

Profiling also has to be fair. Correlations may include hidden biases that have an unintended or discriminatory effect on certain populations.

Organisations may find it difficult to decide when and how to give fair processing about profiling to individuals, both from a practical and technological perspective. Profiling can be a continuous, evolving process, with new correlations discovered all the time.

Feedback request – profiling and automated decision-making

Our code of practice, [Privacy Notices Transparency and Control](#)<sup>6</sup> illustrates how organisations can make fair processing notices relevant, concise and timely.

**Key GDPR provisions**

Article 5(1)(a) and (b); Recital 39

## Feedback request

### Q2

How will you ensure that the profiling you carry out is fair, not discriminatory, and does not have an unjustified impact on individuals' rights?

---

<sup>6</sup> Information Commissioner's Office. Privacy notices, transparency and control code of practice. ICO, 7 October 2016. <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/>. Accessed 4 April 2017

## 3. Data minimisation, accuracy and retention

### Data minimisation

Organisations may seek to gather as much information as possible about individuals in case it proves useful at a later date. This is particularly true of profiling where algorithms can regularly discover new correlations.

However, organisations must show that the data they are processing is limited to what is strictly necessary to meet the purpose. If an organisation cannot clearly identify what that purpose is, they will find it difficult to demonstrate the need to collect that amount of personal data.

### Accuracy

Profiling may generate new data for an individual based on data relating to other people.

Correlations are not necessarily relevant. Some people are more careful about revealing personal information. Not everyone has access to the internet. These groups of individuals may be underrepresented in data sets used for profiling, whereas those who are prolific users of the internet and social media will potentially be over-represented. Some individuals knowingly provide false data in an attempt to exercise some measure of privacy protection.

Even if raw data is recorded accurately, the dataset may not be fully representative and the analytics may contain hidden bias. Decisions may be made based on outdated or inaccurate data or on the basis of the incorrect interpretation of external or third party data. Errors or bias in collected or shared data can increase the risk of an organisation making inaccurate classifications or incorrect decisions

Organisations should have robust procedures in place to protect the quality and accuracy of the personal data they process. They should have ways of testing their systems and the algorithms they use to demonstrate that the data is accurate and free from bias.

### Retention

The GDPR does not set a specific retention period for profiles. As profiles tend to be dynamic and evolving organisations need to regularly review the information they collect to ensure it remains relevant for the purpose.

Embedding a 'privacy by design' approach can aid compliance with these provisions and can enhance privacy awareness across an organisation.

**Key GDPR provisions**

Article 5(1)(c)(d) and (e); Article 25; Recital 39

## Feedback request

### Q3

How will you ensure that the information you use for profiling is relevant, accurate, and kept for no longer than necessary? What controls and safeguards do you consider you will need to introduce, internally and externally to satisfy these particular requirements?

## 4. Lawful processing

Organisations need to consider what their legal basis for processing will be in the context of profiling, and document this in line with the accountability requirements<sup>7</sup>.

If the controller is to rely upon consent as their legal basis for profiling, they should bear in mind that consent has to be freely given, specific, informed and unambiguous (and explicit in the case of special category data). This may be difficult to demonstrate given the nature of profiling.

Other lawful bases the controller may consider using for profiling include processing:

- necessary for the performance of a contract; or
- necessary for the purposes of the legitimate interests pursued by the controller or by a third party (neither of which are available for special category data).

However, they must be able to demonstrate that the profiling is **necessary** to achieve that purpose, rather than simply useful.

Profiles tend to comprise derived or inferred data, rather than information provided directly by the data subject. There is a risk that organisations identify special category data (sensitive personal data) as a result of their profiling activity.

Profiling can infer special category data from other data which is not itself special category data, for example inferring someone's state of health from the records of their food shopping combined with non-personal data on the energy content of foods.

Processing special category personal data for profiling can be difficult because of the restrictions around its use. It is only allowed in specific circumstances provided for in the GDPR, or by member state law.<sup>8</sup> This restriction also applies when organisations identify one or more special categories of personal data as a result of profiling.

### **Key GDPR provisions**

Article 6; Article 9; Article 22(4). Recital 71

---

<sup>7</sup> GDPR Article 5(2)

<sup>8</sup> GDPR Article 22(4)

## Feedback request

### **Q4a**

Have you considered what your legal basis would be for carrying out profiling on personal data? How would you demonstrate, for example, that profiling is necessary to achieve a particular business objective?

### **Q4b**

How do you mitigate the risk of identifying special category personal data from your profiling activities? How will you ensure that any 'new' special category data is processed lawfully in line with the GDPR requirements?

## 5. Information to be provided to individuals

The GDPR specifically requires the controller to provide the data subject with fair processing information about solely automated decision-making (including profiling) that has significant or legal effects (as defined in Article 22(1) and (4)), as well as:

- meaningful information about the logic involved; and
- the significance and envisaged consequences of such processing.

The controller should provide this information at the time the data is first collected from data subjects or within a reasonable period of obtaining the data.

The controller must provide the data subject with sufficient information to make the processing of their personal data fair.<sup>9</sup> Depending upon the context in which the personal data are processed the controller may still have to provide information about profiling that does not fall into the above definition.

The right of access entitles the data subject to request the same information about solely automated decision-making (including profiling) that has significant or legal effects.

Recital 63 provides some protection for controllers concerned about revealing business sensitive information by stating that the right of access:

“...should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.”

### Meaningful information about the logic involved

Instead of providing a detailed technical description about how an algorithm or machine learning works, the controller should consider clarifying:

- the categories of data used to create a profile;
- the source of the data; and
- why this data is considered relevant.

---

<sup>9</sup> GDPR Recital 60

## Significance and envisaged consequences of profiling

One of the key areas for consideration is whether this information is about intended processing or an explanation of how a particular decision has been made.

We think the term suggests that the controller should provide information about how profiling might affect the data subject generally, rather than information about a specific decision.

### **Example**

An online retailer offering credit facilities could outline the data and features it takes into account in arriving at a credit score. The score might impact on someone's credit worthiness which means they have to pay in advance for a product rather than being offered credit.

### **Key GDPR provisions**

Article 13(2)(f); Article 14(2)(g); Article 15(1)(h); Recital 60,61 and 63

## Feedback request

### **Q5**

How do you propose handling the requirement to provide relevant and timely fair processing information, including “meaningful” information on the logic involved in profiling and automated decision-making? What, if any, challenges do you foresee?

## 6. Rectification and objection to profiling

### Right to rectification

Profiling can involve predictive elements, which potentially increases the risk of inaccuracy. Under Article 16 individuals can challenge both the accuracy of the data used in a profile (the input data), and the profile itself (the output data).

Similarly the rights to erasure (Article 17) and restriction of processing (Article 18) will apply to the different stages of the profiling process.

### Right to object

The GDPR right to object to processing in Article 21(1) specifically mentions profiling. The right only applies to processing carried out on the basis of Articles 6(1)(e) and (f), namely performance of a public task or legitimate interests.

Once a data subject exercises their right to object, the controller must interrupt or avoid starting the profiling process unless they can show:

“compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.”<sup>10</sup>

In any case there should be a balancing exercise between the competing interests of the controller and the data subject. The burden of proof to show “compelling legitimate grounds” is on the controller rather than the data subject.

Article 21(4) requires the controller to make the data subject explicitly aware of the right to object to processing set out in Articles 21(1) and (2). They should present details of this right clearly and separately. It will not be acceptable to conceal it within the organisation’s general terms and conditions.

### Right to object to processing for direct marketing purposes

The right to object to processing (including profiling) for direct marketing purposes is set out in Article 21(2) and is **absolute** (Article 21(3)).

#### Key GDPR provisions

Article 16,17,18, 21; Recital 69 and 70

<sup>10</sup> GDPR Article 21(1)

## Feedback request

### Q6

If someone objects to profiling, what factors do you consider would constitute “compelling legitimate grounds” for the profiling to override the “interests rights and freedoms” of the individual?

## 7. Automated individual decision-making, including profiling

Article 22(1) says that:

“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

The right does not apply where the decision is:

- necessary for a contract;
- authorised by Union or Member State law;
- based on the data subject’s explicit consent.<sup>11</sup>

However, even in the above circumstances the data subject can still express their view, obtain human intervention and challenge the decision.<sup>12</sup>

The interpretation of the word “solely” in the context of Article 22(1) requires further consideration. However, we think it is intended to cover those automated decision-making processes where a human exercises no real influence on the outcome of the decision, for example where the result of the profiling or process is not assessed by a person before being formalised as a decision.

### Producing legal or significant effects

“Legal” and “significant” effects are not defined in the GDPR.

A legal effect might be something that adversely impacts an individual’s legal rights, or affects their legal status. A significant effect is more difficult to explain but suggests some consequence that is more than trivial and potentially has an unfavourable outcome.

#### **Further reading**

Overview of the GDPR - [rights relating to automated decision making and profiling](#).

#### **Key GDPR provisions**

Article 22; Recital 71 and 72

---

<sup>11</sup> GDPR Article 22(2)

<sup>12</sup> GDPR Article 22(3)

## Feedback request

### Q7a

Do you consider that “solely” in Article 22(1) excludes any human involvement whatsoever, or only actions by a human that influence or affect the outcome? What mechanisms do you have for human involvement and at what stage of the process?

### Q7b

What is your understanding of a “legal” or “significant” effect? What measures can you put in place to help assess the level of impact?

## 8. Implementing appropriate safeguards

The GDPR requires organisations to use appropriate mathematical or statistical procedures to safeguard individuals' rights and freedoms when carrying out automated processing or profiling.<sup>13</sup>

Organisations must also introduce technical and organisational measures to avoid and correct errors and minimise bias or discrimination. These requirements may involve implementing:

- 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 minimisation and clear retention periods for profiles;
- anonymisation or pseudonymisation techniques in the context of profiling; and
- a process for human intervention in defined cases.

Organisations might also want to consider:

- new ways to test their big data systems;
- the introduction of innovative techniques such as algorithmic auditing;
- accountability/certification mechanisms for decision making systems using algorithms;
- codes of conduct for auditing processes involving machine learning;
- ethical review boards to assess the potential harms and benefits to society of particular applications for profiling.

### **Key GDPR provisions**

Article 22(3); Recital 71

## Feedback request

### Q8

What mechanisms or measures do you think would meet the GDPR requirements to test the effectiveness and fairness of the systems you use in automated decision making or profiling?

---

<sup>13</sup> GDPR Recital 71

## 9. Data protection impact assessment (DPIA)

A data protection impact assessment is required in the case of:

Article 35(3)(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;”

Examples of these activities include, but are not limited to:

- profiling and scoring for purposes of risk assessment (for example for credit scoring, insurance premium setting, fraud prevention, detection of money laundering);
- location tracking, for example by mobile apps, to decide whether to send push notifications;
- loyalty programmes;
- behavioural advertising; and
- monitoring of wellness, fitness and health data via wearable devices.

Article 35(3)(a) refers to evaluation and decisions “based” on automated processing, including profiling. This differs from the provisions in Article 22 that apply to decisions “based **solely** on automated processing, including profiling”.

We take this to mean that a DPIA may also be required in the case of partially automated processing that meets the rest of the criteria set out in Article 35(3).

WP29 will issue guidelines on DPIAs later this year.

### **Key GDPR provisions**

Article 35, Recital 91

## Feedback request

### Q9

Do you foresee any difficulties in implementing the GDPR requirement to carry out a DPIA, when profiling?

## 10. Children and profiling

The GDPR states that children need particular protection with regard to their personal data.

Recital 38 expands

“...as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles.....”<sup>14</sup>

Controllers must not carry out solely automated processing, including profiling, that produces legal or similar significant effects (as defined in Article 22(1)) in respect of a child.<sup>15</sup>

We are continuing our analysis of the GDPR provisions specific to children’s personal data and will look to publish some outputs this year.

**Key GDPR provisions**  
Article 8; Recitals 38, 71

### Feedback request

#### Q10

Will your organisation be affected by the GDPR provisions on profiling involving children’s personal data? If so, how?

---

<sup>14</sup> GDPR Recital 38

<sup>15</sup> GDPR Recital 71

# Feedback request form

Please provide us with your views by answering the following questions, where relevant to your organisation:

**1. When, how and why does your organisation carry out profiling?  
Do you agree that there has to be a predictive element, or some degree of inference for the processing to be considered profiling?**

**2. How will you ensure that the profiling you carry out is fair, not discriminatory, and does not have an unjustified impact on individuals' rights?**

**3. How will you ensure that the information you use for profiling is relevant, accurate and kept for no longer than necessary?  
What controls and safeguards do you consider you will need to introduce, internally and externally, to satisfy these particular requirements?**

**4. (a) Have you considered what your legal basis would be for carrying out profiling on personal data? How would you demonstrate, for example, that profiling is necessary to achieve a particular business objective?**

**4. (b) How do you mitigate the risk of identifying special category personal data from your profiling activities? How will you ensure that any 'new' special category data is processed lawfully in line with the GDPR requirements?**

**5. How do you propose handling the requirement to provide relevant and timely fair processing information, including "meaningful" information on the logic involved in profiling and automated decision-making? What, if any, challenges do you foresee?**

**6. If someone objects to profiling, what factors do you consider would constitute “compelling legitimate grounds” for the profiling to override the “interests rights and freedoms” of the individual?**

**7. (a) Do you consider that “solely” in Article 22(1) excludes any human involvement whatsoever, or only actions by a human that influence or affect the outcome? What mechanisms do you have for human involvement and at what stage of the process?**

**7. (b) What is your understanding of a “legal” or “significant” effect? What measures can you put in place to help assess the level of impact?**

**8. What mechanisms or measures do you think would meet the GDPR requirements to test the effectiveness and fairness of the systems you use in automated decision-making or profiling?**

**9. Do you foresee any difficulties in implementing the GDPR requirement to carry out a DPIA, when profiling?**

**10. Will your organisation be affected by the GDPR provisions on profiling involving children's personal data? If so, how?**

# About you

---

**Are you:**

A representative of a public sector organisation? Please specify:	<input type="checkbox"/>
A representative of a private sector organisation? Please specify:	<input type="checkbox"/>
A representative of a community, voluntary or charitable organisation, or of a trade body? Please specify:	<input type="checkbox"/>
Other? Please specify:	<input type="checkbox"/>

**Thank you for your input.**