Automated decision-making and profiling

1.1.9 | 17 October 2022

Automated decision-making and profiling

About this detailed guidance

This guidance discusses automated decision-making and profiling in detail. Read it if you have detailed questions not answered in the Guide, or if you need a deeper understanding to help you apply the rules relating to automated decision-making and profiling in practice. DPOs and those with specific data protection responsibilities in larger organisations are likely to find it useful.

If you haven't yet read automated decision-making and profiling in brief in the Guide to UK GDPR, you should read that first. It sets out the key points you need to know, along with practical checklists to help you comply.

Contents

- What's a DPIA?
- What do we need to tell individuals and why?
- How can we explain complicated processes in a way that people will understand?
- What's the best way to provide privacy information?
- What other rights do individuals have?
- Will we need to make any other changes to our systems?

What if Article 22 doesn't apply to our processing?

- Are there any key areas we should focus on?
- Can individuals object to profiling?

What is automated individual decision-making and profiling?

In detail

What is profiling?

Profiling analyses aspects of an individual's personality, behaviour, interests and habits to make predictions or decisions about them.

The UK GDPR defines profiling as follows:

> 'profiling' means 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.
>
> Article 4 (4)

Organisations obtain personal information about individuals from a variety of different sources. Internet searches, buying habits, lifestyle and behaviour data gathered from mobile phones, social networks, video surveillance systems and the Internet of Things are examples of the types of data organisations might collect.

They analyse this information to classify people into different groups or sectors. This analysis identifies correlations between different behaviours and characteristics to create profiles for individuals. This profile will be new personal data about that individual.

Organisations use profiling to:

- find something out about individuals' preferences;
- predict their behaviour; and/or
- make decisions about them.

Profiling can use algorithms. An algorithm is a sequence of instructions or set of rules designed to complete a task or solve a problem. Profiling uses algorithms to find correlations between separate datasets. These algorithms can then be used to make a wide range of decisions, for example to predict behaviour or to control access to a service. Artificial intelligence (AI) systems and machine learning are increasingly used to create and apply algorithms. There is more information about algorithms, AI and machine-learning in our paper on big data, artificial intelligence, machine learning and data protection.

You are carrying out profiling if you:

- collect and analyse personal data on a large scale, using algorithms, AI or machine-learning;
- identify associations to build links between different behaviours and attributes;
- create profiles that you apply to individuals; or
- predict individuals' behaviour based on their assigned profiles.

Although many people think of marketing as being the most common reason for profiling, this is not the only application.

Example

Profiling is used in some medical treatments, by applying machine learning to predict patients' health or the likelihood of a treatment being successful for a particular patient based on certain group characteristics.

Less obvious forms of profiling involve drawing inferences from apparently unrelated aspects of individuals' behaviour.

Example

Using social media posts to analyse the personalities of car drivers by using an algorithm to analyse words and phrases which suggest 'safe' and 'unsafe' driving in order to assign a risk level to an individual and set their insurance premium accordingly.

What is automated decision-making?

Automated decision-making is the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data. Examples of this include:

- an online decision to award a loan; and
- an aptitude test used for recruitment which uses pre-programmed algorithms and criteria.

Automated decision-making often involves profiling, but it does not have to.

Example

An examination board uses an automated system to mark multiple choice exam answer sheets. The system is pre-programmed with the number of correct answers required to achieve pass and distinction marks. The scores are automatically attributed to the candidates based on the number of correct answers and the results are available online.

This is an automated decision-making process that doesn't involve profiling.

What are the benefits of profiling and automated decision-making?

Profiling and automated decision making can be very useful for organisations and also benefit individuals in many sectors, including healthcare, education, financial services and marketing. They can lead to quicker and more consistent decisions, particularly in cases where a very large volume of data needs to be analysed and decisions made very quickly.

What are the risks?

Although these techniques can be useful, there are potential risks:

- Profiling is often invisible to individuals.
- People might not expect their personal information to be used in this way.
- People might not understand how the process works or how it can affect them.
- The decisions taken may lead to significant adverse effects for some people.

Just because analysis of the data finds a correlation doesn't mean that this is significant. As the process can only make an assumption about someone's behaviour or characteristics, there will always be a margin of error and a balancing exercise is needed to weigh up the risks of using the results. The UK GDPR provisions are designed to address these risks.

Relevant provisions in the UK GDPR - See Articles 4(4), 22(1), (2) and Recital 71

https://www.legislation.gov.uk/eur/2016/679/contents

Further reading

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR. EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues

WP29 adopted guidelines on automated individual decision-making and profiling – Chapter II, which have been endorsed by the EDPB.

What does the UK GDPR say about automated decision-making and profiling?

In detail

The UK GDPR gives people the right not to be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect on them. These provisions restrict when you can carry out this type of processing and give individuals specific rights in those cases.

What type of processing is restricted?

Article 22(1) of the UK GDPR limits the circumstances in which you can make **solely automated decisions**, including those based on profiling, that have a **legal or similarly significant effect on individuals.**

> "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 affects him or her"
>
> Article 22(1)

What does 'solely' automated mean?

Solely means a decision-making process that is totally automated and excludes any human influence on the outcome. A process might still be considered solely automated if a human inputs the data to be processed, and then the decision-making is carried out by an automated system.

A process won't be considered solely automated if someone weighs up and interprets the result of an automated decision before applying it to the individual.

Example

A factory worker's pay is linked to their productivity, which is monitored automatically. The decision about how much pay the worker receives for each shift they work is made automatically by referring to the data collected about their productivity.

This is an example of solely automated decision making.

Many decisions that are commonly regarded as automated actually involve human intervention. However, the human involvement has to be active and not just a token gesture. The question is whether a human reviews the decision before it is applied and has discretion to alter it, or whether they are simply applying the decision taken by the automated system.

Example

An employee is issued with a warning about late attendance at work. The warning was issued because the employer's automated clocking-in system flagged the fact that the employee had been late on a defined number of occasions. However, although the warning was issued on the basis of the data collected by the automated system, the decision to issue it was taken by the employer's HR manager following a review of that data.

In this example the decision was not taken solely by automated means.

What types of decision have a legal or similarly significant effect?

A decision producing a **legal effect** is something that affects a person's legal status or their legal rights. For example when a person, in view of their profile, is entitled to a particular social benefit conferred by law, such as housing benefit.

A decision that has a **similarly significant effect** is something that has an equivalent impact on an individual's circumstances, behaviour or choices.

In extreme cases, it might exclude or discriminate against individuals. Decisions that might have little impact generally could have a significant effect for more vulnerable individuals, such as children.

Example

A social security process which automatically evaluates whether an individual is entitled to benefit and how much to pay is a decision 'based solely on automated processing' for the purposes of Article 22(1).

As well as having a legal effect, the amount of benefit received could affect a person's livelihood or ability to buy or rent a home so this decision would also have a 'similarly significant effect'.

Other similarly significant effects include:

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

Example

An individual applies for a loan online. The website uses algorithms and automated credit searching to provide an immediate yes/no decision on the application.

Example

As part of their recruitment process, an organisation decides to interview certain people based entirely on the results achieved in an online aptitude test. This decision has a significant effect, since it determines whether or not someone can be considered for the job.

By contrast, the following example is unlikely to have a significant effect on an individual:

Example

Recommendations for new television programmes based on an individual's previous viewing habits.

If you are unsure whether a decision has a similarly significant effect on someone you should consider the extent to which it might affect, for example, their:

- financial circumstances;
- health;
- reputation;
- employment opportunities;
- behaviour; or
- choices.

The guidelines produced by WP29 include more advice on identifying legal or similarly significant effects.

Automated decision-making systems are a key part of our business operations – do the UK GDPR provisions mean we can't use them?

Used correctly, automated decision-making is useful for many businesses. It can help you to interpret policies correctly and make decisions fairly and consistently.

The UK GDPR recognises this and doesn't prevent you from carrying out profiling or using automated systems to make decisions about individuals unless the processing meets the definition in Article 22(1), in which case you'll need to ensure it's covered by one of the exceptions in Article 22(2). See When can we carry out this type of processing for more information about the exceptions.

We profile our customers to send relevant marketing to them – does Article 22 stop us doing this?

Creating or applying a profile to someone in order to tailor your marketing is a decision about them, but for profiling or automated decision-making to be restricted by Article 22 there needs to be:

- no human involvement; **and**

- a legal or similarly significant effect on the individual.

The UK GDPR isn't designed to stop you from running your business or promoting your products and services. However, there could be situations in which marketing may have a significant effect on the recipients. You need to think about your target market. For example, vulnerable groups of individuals may be more easily influenced and affected by behavioural advertising.

The UK GDPR highlights that children in particular deserve additional protection, especially where their personal information is used for the purposes of marketing and creating online profiles.

> "Children merit specific protection with regard to their personal data, 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..."
>
> Recital 38

Also remember that people can object to you profiling them for marketing purposes under Article 21. You must bring details of this right to their attention and present it separately from other information. If you receive this type of objection you must stop the processing and confirm to the individual that you have done so within a month of receipt.

Any telephone/electronic direct marketing you carry out must also meet PECR requirements – see our direct marketing guidance for more information.

Relevant provisions in the UK GDPR - See Articles 22(1) and Recital 71

https://www.legislation.gov.uk/eur/2016/679

Further reading - ICO guidance

ICO Guidance on Children and the UK GDPR

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR. EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

WP29 adopted guidelines on automated individual decision-making and profiling – Chapter IV, which have been endorsed by the EDPB.

When can we carry out this type of processing?

In detail

You can only carry out this type of processing if you can rely on one of the three exceptions set out in Article 22(2). These exceptions are not the same as the lawful bases for processing required under Article 6.

What are the exceptions?

- **When the decision is necessary for a contract**

You need to consider whether the decision is actually necessary for the performance of a contract with the individual. This means that it does not have to be essential, but it should be a targeted and reasonable way of meeting your contractual obligations. It should also be the least privacy intrusive way to reasonably achieve your objective.

The wording of this exception implies that the decision-making defined in Article 22(1) could potentially be carried out by a different controller than the one who is party to the contract with the individual.

> "if the decision is necessary for entering into, or performance of, a contract between the data subject and a (*not the*) data controller."
>
> Article 22(2) (a)

Example

A loan application might represent a contract between a financial organisation and a potential borrower. The financial organisation relies on an automatically generated credit score carried out by a credit reference agency to decide whether or not to agree the loan.

Even though the contract is not between the data subject and the credit reference agency the decision is covered by Article 22(2)(a) as long as it can be shown that it is necessary for the contract to be fulfilled.

- **When the decision is authorised by law.**

The decision has to be authorised by law, but this doesn't mean that there has to be a law which explicitly states that solely automated decision-making is authorised for a particular purpose. The Data Protection Act 2018 (DPA 2018) refers only to a decision which is 'required or authorised by law' (Chapter 2, Part 2, Section 14 (3)(b)).

If you have a statutory or common law power to do something, and automated decision-making/profiling is the most appropriate way to achieve your purpose, then you may be able to justify this type of processing as authorised by law and rely on Article 22(2)(b). However you must be able to show that it's reasonable to do so in all the circumstances.

Example

In the financial services sector, an organisation might use automated decision-making, including profiling, to identify fraud, in order to comply with a high level regulatory requirement to detect and prevent crime. It identifies cases of potential fraud by comparing data from credit reference agencies, bank accounts, the Land Registry, the DVLA, credit card sales, online marketplaces and social media.

- **When the decision is based on the individual's explicit consent.**

Firstly you need to understand what explicit consent looks like. Consent generally under the UK GDPR must be a freely given, specific, informed and unambiguous affirmative indication of the individual's wishes.

Explicit consent means that the individual should expressly confirm their consent, for example by a written statement, filling in an electronic form or sending an email. Our guidance on consent provides more information on this area.

In the context of Article 22, in order to be specific and informed your consent request needs to explain that the decision will be entirely automated.

What about special categories of personal data?

Article 22(4) provides an additional layer of protection for special category personal data. You can **only** carry out the processing described in Article 22(1) if one of the above exceptions applies and:

- you have the individual's explicit consent; **or**
- the processing is necessary for reasons of substantial public interest. Substantial public interest conditions are set out in Schedule 1 Part 2 of the DPA 2018.

Relevant provisions in the UK GDPR - Article 7, Article 9(2)(a) and (g), Article 22(2), Article 22(4), Recital 71

https://www.legislation.gov.uk/eur/2016/679

Further reading – ICO guidance

ICO consent guidance

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR. EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

WP29 published the following guidelines which have been endorsed by the EDPB:

- Guidelines on automated individual decision-making and profiling – Chapter IV
- Guidelines on consent

What else do we need to consider if Article 22 applies?

In detail

This type of processing is high risk so you need to carry out a DPIA and introduce other appropriate safeguards, such as providing specific information to individuals about the processing and the rights available to them.

These safeguards and rights are highlighted in the UK GDPR and explained in more detail in the WP29 Guidelines on automated decision-making and profiling.

What's a DPIA?

A DPIA is a tool to help you assess the risks to individuals from a processing operation and identify ways to address those risks. They are mandatory for processing that is likely to result in a high risk to individuals. For information about the types of processing requiring a DPIA please read our guide to the UK GDPR.

A DPIA can help you decide whether or not the intended processing is going to be subject to the provisions of Article 22. If you already know that this is the case you must carry out a DPIA.

Even if Article 22 doesn't apply (because the processing isn't solely automated), you are still required to carry out a DPIA if the processing constitutes:

> "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"
>
> Article 35(3)(a)

It's also a good way to meet your accountability obligations by showing that you have:

- considered the risks involved in any profiling or automated individual decision-making process; **and**
- put procedures in place to mitigate those risks and comply with the UK GDPR requirements.

What do we need to tell individuals and why?

You must inform individuals if you are using their data for solely automated decision-making processes with legal or similarly significant effects. This applies whether you have received the data directly from the individuals concerned or from another source.

You must also provide meaningful information about the logic involved and what the likely consequences are for individuals.

This type of processing can be invisible to individuals so in circumstances where it can have a significant impact on them you need to make sure they understand what's involved, why you use these methods and the likely results.

How can we explain complicated processes in a way that people will understand?

Providing 'meaningful information about the logic' and 'the significance and envisaged consequences' of a process doesn't mean you have to confuse people with over-complex explanations of algorithms. You should focus on describing:

- the type of information you collect or use in creating the profile or making the automated decision;

- why this information is relevant; and
- what the likely impact is going to be/how it's likely to affect them.

Example

An online retailer uses automated processes to decide whether or not to offer credit terms for purchases. These processes use information about previous purchase history with the same retailer and information held by the credit reference agencies, to provide a credit score for an online buyer.

The retailer explains that the buyer's past behaviour and account transaction history indicates the most appropriate payment mechanism for the individual and the retailer.

Depending upon the score customers may be offered credit terms or have to pay upfront for their purchases.

What's the best way to provide privacy information?

You must provide specific information if you carry out automated decision-making described in Article 22(1), namely information on:

"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 envisaged consequences of such processing for the data subject."

Articles 13(2)(f) and 14(2)(g)

Our guidance on the right to be informed explains the different techniques you can use, but it is good practice to use the same medium you use to collect personal data to deliver privacy information.

If you're operating in an online environment it shouldn't be too difficult. Layered privacy notices or just-in-time notifications that tell people what

you’re going to do with their data at the point you collect it are good approaches to adopt.

Privacy dashboards that inform people how their data is used, allow access to the information you hold on them, including details of any profiles and the data input into them, and allow them to manage what happens with it are other useful tools.

If you plan to use personal data for any new purposes, you must update your privacy information and proactively bring any changes to people’s attention.

What other rights do individuals have?

If someone is unhappy with a decision you’ve made using a solely automated process, they can ask for a review. It makes sense for you to explain how they can do this at the point you provide the decision.

You need to show how and why you reached the decision, so it’s important that you understand the underlying business rules that apply to automated decision-making techniques.

You must be able to verify the results and provide a simple explanation for the rationale behind the decision.

The systems you use should be able to deliver an audit trail showing the key decision points that formed the basis for the decision. If your system considered any alternative decisions you need to understand why these were not preferred.

You should have a process in place for individuals to challenge or appeal a decision, and the grounds on which they can make an appeal. You should also ensure that any review is carried out by someone who is suitably qualified and authorised to change the decision.

The reviewer should take into consideration the original facts on which the decision was based as well as any additional evidence the individual can provide to support their challenge.

Example

Your request/application has been declined.

> We have made this decision using an automated scoring system that takes into account the information you provided as well as...
>
> If you wish to discuss or appeal the decision then please contact us using the attached form. You can send this electronically or by post.
>
> Our review panel will consider your request and contact you within xxx days with our findings.
>
> Please attach any evidence that you believe might help your appeal. Examples of the types of information that may be useful in the review process are detailed below…
>
> Information about...
>
> Copies of...
>
> Documentary evidence of...

You must act upon the request without undue delay and at the latest within one month of receipt.

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

Will we need to make any other changes to our systems?

Individuals have a right of access to the same details about automated decision-making that you must provide under your privacy information. If someone submits an access request Article 15 says that you have to tell them about:

> "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 envisaged consequences of such processing for the data subject."

Article 15(1)(h)

The UK GDPR says that where possible you should be able to provide remote access to a secure system that provides individuals with direct access to their personal data. This is also a good way for individuals to verify and check that the data you are using is accurate.

Example

An organisation that uses profiling in order to determine insurance premiums allows its customers to inspect and correct any inaccuracies in the personal data used in the profiles assigned to them. As well as addressing any errors, this also helps improve the precision of the system used to carry out the processing.

You need to make sure that you have mechanisms in place to diagnose any quality issues or errors and a process to document how these are resolved.

These mechanisms should also allow you to check that your systems are working as intended and highlight any inaccuracies or bias.

Consider how you can:

- introduce sample quality checks on the results from your systems to remove any bias and/or discriminatory effects;
- ensure any special category data that may have been inferred by the profiling is deleted if it is not required;
- identify appropriate retention policies for the information you use and keep these under review;
- implement suitable security measures such as access controls and encryption; and
- audit your machine-learning tools to check for decision-making rationale and consistency.

Relevant provisions in the UK GDPR - Article 22(3), Article 35, Article 40, Article 42, Recital 71

https://www.legislation.gov.uk/eur/2016/679

Further reading – ICO guidance

- Guide to the UK GDPR – right to be informed
- Big data, artificial intelligence, machine learning and data protection

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR. EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

WP29 published the following guidelines which have been endorsed by the EDPB:

- Guidelines on automated individual decision-making and profiling Chapter IV and VI
- Guidelines on Data Protection Impact Assessment
- Guidelines on transparency

What if Article 22 doesn't apply to our processing?

In detail

Even if Article 22 does not apply to your processing, for example because there is human involvement in the decision-making process, you must still comply with the UK GDPR principles and identify and record your lawful basis for the processing. This is also the case for any new profiles you create.

Are there any key areas we should focus on?

You may want to revise your privacy policy and inform individuals about any automated decision-making involving profiling that you carry out, especially if it's unlikely they would expect it. You should still tell people what data you're using and where it's come from.

Even if you don't think the processing falls within Article 22, it's good practice to do this and helps you be more transparent – particularly because this type of processing won't necessarily be obvious to individuals.

As part of assessing whether your processing is fair, you also need to think about whether any profiling is fundamentally linked with the reason for using the service and what people would reasonably expect you to do with their data. Although a retailer analysing loyalty card data to decide what new products to suggest to a customer might be an expected activity; analysing someone's social media posts to reject them for a job, refuse a loan, or increase their insurance might not be.

Individuals have access rights to the personal information you process about them, including information used in any profiling you carry out.

Remember as well that if the data you're using isn't correct then any profile or decision based on the data will also be flawed.

Don't collect too much information or keep it for too long. Just because your systems allow you to retain vast quantities of data doesn't mean you should.

It also makes it more difficult to keep the data up to date, accurate and relevant for any profiling you're carrying out.

Read our guide to the UK GDPR for information on compliance with the data protection principles and the different lawful bases for processing. Our guidance on lawful bases includes an interactive guidance tool which helps you to assess which lawful basis is likely to be appropriate for your processing.

Can individuals object to profiling?

Article 21 of the UK GDPR gives individuals the right to object to any profiling that you carry out:

- on the basis of legitimate interests or on the basis of public task or official authority. In these cases an individual can object on grounds relating to his or her particular situation. You'll have to stop the processing unless you can show that you have a compelling reason to continue the profiling that overrides the individual's interests;
- for direct marketing purposes. You must stop the profiling as soon as you receive an objection. There are no exemptions or grounds to refuse.

You must bring this right to the attention of individuals and present it separately from other information.

If you receive an objection under Article 21 you need to respond within one month and confirm the action you've taken.

Relevant provisions in the UK GDPR - See Articles 13, 14, 15, 21 and Recitals 60, 63, 71

https://www.legislation.gov.uk/eur/2016/679

Further reading - ICO guidance

- Guide to the UK GDPR – principles, lawful bases for processing, individuals rights
- Guidance on Children and the UK GDPR

Further reading - Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR. EDPB guidelines are no longer be directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

The WP29 published the following guidelines which have been endorsed by the EDPB:

- Guidelines on Automated individual decision-making and profiling Chapters III and V
- Guidelines on consent
- Guidelines on transparency