ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 251

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

Adopted on 3 October 2017

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

TABLE OF CONTENTS

INTRODUCTION

The General Data Protection Regulation (the GDPR), specifically addresses profiling and automated individual decision-making, including profiling.[1]

Profiling and automated decision-making are used in an increasing number of sectors, both private and public. Banking and finance, healthcare, taxation, insurance, marketing and advertising are just a few examples of the fields where profiling is being carried out more regularly to aid decision-making.

Advances in technology and the capabilities of big data analytics, artificial intelligence and machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms.

The widespread availability of personal data on the internet and from Internet of Things (IoT) devices, and the ability to find correlations and create links, can allow aspects of an individual's personality or behaviour, interests and habits to be determined, analysed and predicted.

Profiling and automated decision-making can be useful for individuals and organisations as well as for the economy and society as a whole, delivering benefits such as:

- increased efficiencies; and
- resource savings.

They have many commercial applications, for example, they can be used to better segment markets and tailor services and products to align with individual needs. Medicine, education, healthcare and transportation can also all benefit from these processes.

However, profiling and automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards.

These processes can be opaque. Individuals might not know that they are being profiled or understand what is involved.

Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. It can lead to inaccurate predictions, denial of services and goods and unjustified discrimination in some cases.

The GDPR introduces new provisions to address the risks arising from profiling and automated decision-making, notably, but not limited to, privacy. The purpose of these guidelines is to clarify those provisions.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Profiling and automated individual decision-making are also covered by Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. While these guidelines focus on profiling and automated individual decision-making under the GDPR, the guidance is also relevant regarding the two topics under Directive 2016/680, with respect to their similar provisions. The analysis of specific features of profiling and automated individual decision-making under Directive 2016/680 is not included in these Guidelines.

This document covers:

- Definitions of profiling and automated decision-making and the GDPR approach to these in general – Chapter II
- Specific provisions on automated decision-making as defined in Article 22 – Chapter III
- General provisions on profiling and automated decision-making - Chapter IV
- Children and profiling – Chapter V
- Data protection impact assessments – Chapter VI

The Annexes provide best practice recommendations, building on the experience gained in EU Member States.

The Article 29 Data Protection Working Party (WP29) will monitor the implementation of these guidelines and may complement them with further details as appropriate.

I. Definitions

The GDPR introduces provisions to ensure that profiling and automated individual decision-making (whether or not this includes profiling) are not used in ways that have an unjustified impact on individuals' rights; for example:

- specific transparency and fairness requirements;
- greater accountability obligations;
- specified legal bases for the processing;
- rights for individuals to oppose profiling and specifically profiling for marketing; and
- if certain conditions are met, a need to carry out a data protection impact assessment.

The GDPR does not just focus on the decisions made as a result of automated processing or profiling. It applies to the collection of data for the creation of profiles, as well as the application of those profiles to individuals.

A. Profiling

The GDPR defines profiling in Article 4(4) as:

> 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;

Profiling is composed of three elements:

- it has to be an *automated* form of processing;
- it has to be carried out *on personal data*; and
- the objective of the profiling must be *to evaluate personal aspects* about a natural person.

Article 4(4) refers to any form of profiling, rather than 'solely' automated processing (which is referred to in Article 22). Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition.

Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar.

The GDPR says that profiling is automated processing of personal data for evaluating personal aspects, in particular to analyse *or* make predictions about individuals. Therefore simply assessing or classifying individuals based on characteristics such as their age, sex, and height could be considered profiling, regardless of any predictive purpose.

The GDPR is inspired by but is not identical to the definition of profiling in the Council of Europe Recommendation CM/Rec(2010)13[2] (Recommendation), as the Recommendation *excludes* processing that does not include inference. Nevertheless the Recommendation is a useful reference tool - specifically its description of the three distinct stages of profiling:

- data collection;
- automated analysis to identify correlations;
- applying the correlation to an individual to identify characteristics of present or future behaviour.

Each of the above stages represents a process that falls under the GDPR definition of profiling.

Broadly speaking, profiling means 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, for example, their:

- ability to perform a task;
- interests; or
- likely behaviour.

Example

A data broker collects data from different public and private sources, either on behalf of its clients or for its own purposes. The data broker compiles the data to develop profiles on the individuals and places them into segments. It sells this information to companies who wish to improve the targeting of their goods and services. The data broker carries out profiling by placing a person into a certain category according to their interests.
Whether or not there is automated decision-making as defined in Article 22(1) will depend upon the circumstances.

B. Automated decision-making

Automated decision-making has a different scope and may partially overlap with profiling. Solely automated decision-making is the ability to make decisions by technological means without human involvement. Automated decisions can be based on any type of data, for example:

[2] 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 . Accessed 24 April 2017

- data provided directly by the individuals concerned (such as responses to a questionnaire);
- data observed about the individuals (such as location data collected via an application);
- derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score).

Automated decisions can be made with or without profiling; profiling can take place without making automated decisions. However, profiling and automated decision-making are not necessarily separate activities. Something that starts off as a simple automated decision-making process could become one based on profiling, depending upon how the data is used.

Example

Imposing speeding fines purely on the basis of evidence from speed cameras is an automated decision-making process that does not necessarily involve profiling.

It would, however, become a decision based on profiling if the driving habits of the individual were monitored over time, and, for example, the amount of fine imposed is the outcome of an assessment involving other factors, such as whether the speeding is a repeat offence or whether the driver has had other recent traffic violations.

Decisions that are not wholly automated might also include profiling. For example, before granting a mortgage, a bank may consider the credit score of the borrower, with additional meaningful intervention carried out by humans before any decision is applied to an individual.

C. How the GDPR addresses the concepts

There are potentially three ways in which profiling may be used:

(i) general profiling;
(ii) decision-making based on profiling; and
(iii) *solely* automated decision-making, including profiling (Article 22).

The difference between (ii) and (iii) is best demonstrated by the following two examples where an individual applies for a loan online:

- a human decides whether to agree the loan based on a profile produced by purely automated means(ii);
- an algorithm decides whether the loan is agreed and the decision is automatically delivered to the individual, without any meaningful human input (iii).

Although there are three types of profiling, only two legal frameworks apply.

Chapter III of these guidelines explains the specific provisions that apply to solely automated individual decision-making, including profiling.[3] A general prohibition on this type of processing exists to reflect the potentially adverse effect on individuals.

Chapter IV of these guidelines explains the legal framework for general profiling. This includes decision-making based on profiling that is not solely automated.

[3] As defined in Article 22(1) of the GDPR.

Under Article 23 Member States can introduce legislation to restrict[4] data subjects' rights and data controllers' obligations regarding profiling and automated decision making. This may be particularly relevant for processing that falls under Article 22.

II. Specific provisions on automated decision-making as defined in Article 22

Article 22(1) says

> 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*.

In summary, Article 22 provides that:

(i) as a rule, there is a prohibition on fully automated individual decision-making, including profiling that has a legal or similarly significant effect;
(ii) there are exceptions to the rule;
(iii) there should be measures in place to safeguard the data subject's rights and freedoms and legitimate interests[5].

These safeguards, discussed in more detail below, include the right to be informed (addressed in Articles 13 and 14 – specifically meaningful information about the logic involved, as well as the significance and envisaged consequences for the data subject), the right to obtain human intervention and the right to challenge the decision (addressed in Article 22(3)).

The prohibition in Article 22(1) will *only apply* when a decision based solely on automated processing, including profiling has a legal effect on or similarly significantly affects someone.

A. 'Based solely on automated processing'

Article 22(1) refers to decisions 'based solely' on automated processing. This means that there is no human involvement in the decision process.

> **Example**
>
> An automated process produces what is in effect a recommendation concerning a data subject. If a human being reviews and takes account of other factors in making the final decision, that decision would not be 'based solely' on automated processing.

[4] 'when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society' for certain specifically listed purposes (e.g. crime prevention) or in certain specifically listed situations. Article 23 provides a full list. Specific provisions for some of these purposes are listed in Article 23(2)

[5] Recital 71 says that such processing should be "subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."

The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing.

To qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the available input and output data.

B. 'Legal' or 'similarly significant' effects

The GDPR recognises that automated decision-making, including profiling can have serious consequences for individuals. However, the GDPR does not define 'legal' or 'similarly significant' effects.

'Legal effects'

A legal effect suggests a processing activity that has an impact on someone's legal rights, such as the freedom to associate with others, vote in an election, or take legal action. A legal effect may also be something that affects a person's legal status or their rights under a contract. For example, automated decisions that mean someone is:

- entitled to or denied a particular social benefit granted by law, such as child or housing benefit;
- refused entry at the border;
- subjected to increased security measures or surveillance by the competent authorities; or
- automatically disconnected from their mobile phone service for breach of contract because they forgot to pay their bill before going on holiday.

'Similarly significantly affects him or her'

Even if a decision-making process does not have an effect on people's legal rights it could still fall within the scope of Article 22 if it produces an effect that is equivalent or similarly significant in its impact.

In other words, even where no legal (statutory or contractual) rights or obligations are specifically affected, the data subjects could still be impacted sufficiently to require the protections under this provision. The GDPR introduces the word 'similarly' (not present in Article 15 of Directive 95/46/EC) to the phrase 'significantly affects'. This suggests that the threshold for *significance* must be similar, whether or not the decision has a legal effect.

For data processing to significantly affect someone the effects of the processing must be more than trivial and must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned. At its most extreme, the decision may lead to the exclusion or discrimination of individuals.

Recital 71 provides the following typical examples: 'automatic refusal of an online credit application' or 'e-recruiting practices without any human intervention'. These suggest that it is difficult to be precise about what would be considered sufficiently *significant* to meet the threshold. For example, based on the recital each of the following credit decisions fall under Article 22, but with very different degrees of impact on the individuals concerned:

- renting a city bike during a vacation abroad for two hours;

- purchasing a kitchen appliance or a television set on credit;
- obtaining a mortgage to buy a first home.

This bring us also to the issue of online advertising, which increasingly relies on automated tools and involves solely automated individual decision-making.

In many typical cases targeted advertising does not have a significant effect on individuals, for example an advertisement for a mainstream online fashion outlet based on a simple demographic profile: 'women in the Brussels region'.

However it is possible that it may do, depending upon the particular characteristics of the case, including:

- the intrusiveness of the profiling process;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; or
- the particular vulnerabilities of the data subjects targeted.

Processing that might have little impact on individuals generally may in fact have a significant effect on certain groups of society, such as minority groups or vulnerable adults. For example, someone in financial difficulties who is regularly shown adverts for on-line gambling may sign up for these offers and potentially incur further debt.

Even where advertising or marketing practices do not fall under Article 22, data controllers must comply with the general legal framework applicable to profiling under the GDPR, covered in Chapter IV. The provisions of the proposed ePrivacy Regulation may also be relevant in many cases. Furthermore, children require enhanced protection, as will be discussed below in Chapter V.

Automated decision-making that results in differential pricing could also have a significant effect if, for example, prohibitively high prices effectively bar someone from certain goods or services.

Although the context and wording differ, the concept 'substantially affects' is discussed in the WP29 guidelines on the lead supervisory authority. The examples in these guidelines[6] may be helpful when considering the effects of automated decision-making on data subjects.

Similarly significant effects may be positive or negative. These effects may also be triggered by the actions of individuals other than the one to which the automated decision relates. An illustration of this is given below.

Example

Hypothetically, a credit card company might reduce a customer's card limit, based not on that customer's own repayment history, but on non-traditional credit criteria, such as an analysis of other customers living in the same area who shop at the same stores.

This could mean that someone is deprived of opportunities based on the actions of others.

In a different context using these types of characteristics might have the advantage of extending credit to those without a conventional credit history, who would otherwise have been denied.

[6] Article 29 Data Protection Working Party. Guidelines for identifying a controller or processor's lead supervisory authority. 5 April 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=44102 Accessed 24 April 2017

C. Exceptions from the prohibition

Article 22(1) sets out a general prohibition on solely automated individual decision with a significant effect, as described above.

This means that the controller should not undertake the processing described in Article 22(1) unless one of the following Article 22(2) exceptions applies:

(a) necessary for the performance of or entering into a contract;
(b) authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
(c) based on the data subject's explicit consent.

1. Performance of a contract

Controllers may wish to use automated decision-making, for example, because it:

- potentially allows for greater consistency or fairness in the decision making process (e.g. it might reduce the potential for human error, discrimination and abuse of power);
- reduces the risk of customers failing to meet payments for goods or services (for example by using credit referencing); or
- enables them to deliver decisions within a shorter time frame and improves the efficiency of the process. Routine human involvement may sometimes also be impractical or impossible due to the sheer quantity of data being processed.

Regardless of the above, these considerations alone are not always sufficient to show that this type of processing is *necessary* under Article 22(2)(a) for entering into, or the performance of, a contract. As described in the WP29 Opinion on legitimate interest, necessity should be interpreted narrowly.

The controller must be able to show that this profiling is necessary, taking into account whether a less privacy-intrusive method could be adopted. [7] If other less intrusive means to achieve the same goal exist, then the profiling would not be 'necessary'.

2. Authorised by Union or Member State law

Automated decision-making including profiling could potentially take place under 22(2)(b) if Union or Member State law authorised its use. Recital 71 says that this could include its use for monitoring and preventing fraud and tax-evasion or to ensure the security and reliability of a service provided by the controller.

[7] Buttarelli, Giovanni. Assessing the necessity of measures that limit the fundamental right to the protection of personal data. AToolkit European Data Protection Supervisor, 11 April 2017, https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf Accessed 24 April 2017

3. Explicit consent

Article 22 requires *explicit* consent. Processing that falls within the definition of Article 22(1) poses significant data protection risks and a high level of individual control over personal data is therefore deemed appropriate.

'Explicit consent' is not defined in the GDPR but suggests that the consent must be specifically confirmed by an express statement rather than some other affirmative action.

Explicit consent will be addressed in the forthcoming consent guidelines. Chapter IV.B provides more information on consent generally.

D. Rights of the data subject[8]

1. Articles 13(2) (f) and 14(2) (g) - Right to be informed

Given the potential risks and interference that profiling caught by Article 22 poses to the rights of data subjects, data controllers should be particularly mindful of their transparency obligations. This means ensuring that information about the profiling is not only easily accessible for a data subject but that it is brought to their attention.[9]

Articles 13(2) (f) and 14(2) (g) require controllers to provide specific information about automated decision-making, based solely on automated processing, including profiling, that produces legal or similarly significant effects.[10]

If the controller is making automated decisions as described in Article 22(1), they must:

- tell the data subject that they are engaging in this type of activity;
- provide meaningful information about the logic involved; and
- explain the significance and envisaged consequences of the processing.

Meeting these three specified transparency requirements will (along with other suitable safeguards) help controllers to better inform data subjects about the Article 22 (1) type of processing and the consequences.

It is good practice to provide the above information whether or not the processing falls within the narrow Article 22(1) definition. In any event the controller must provide sufficient information to the data subject to make the processing fair,[11] and meet all the other information requirements of Articles 13 and 14. These requirements are explained in more detail in Chapter IV(section D).

[8] GDPR Article 12 provides for the modalities applicable for the exercise of the data subject's rights

[9] Recital 60 states that "Furthermore the data subject should be informed of the existence of profiling and the consequences of such profiling".

[10] Referred to in Article 22(1) and (4).The forthcoming WP Guidelines on transparency will cover the general information requirements of Articles 13 and 14.

[11] GDPR Recital 60 "The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore the data subject should be informed of the existence of profiling and the consequences of such profiling."

Meaningful information about the 'logic involved'

The growth and complexity of machine-learning can make it challenging to understand how an automated decision-making process or profiling works.

The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision without necessarily always attempting a complex explanation of the algorithms used or disclosure of the full algorithm.[12] The information provided should, however, be meaningful to the data subject.

Example

A controller uses credit scoring to assess and reject an individual's loan application. The score may have been provided by a credit reference agency, or calculated directly based on information held by the controller.

Regardless of the source (and information on the source must be provided to the data subject under Article 14 (2) (f) where the personal data have not been obtained from the data subject), if the controller is reliant upon this score it must be able to explain it and the rationale, to the data subject.

The controller explains that this process helps them make fair and responsible lending decisions. It provides details of the main characteristics considered in reaching the decision, the source of this information and the relevance. This may include, for example:

- the information provided by the data subject on the application form;
- information about previous account conduct , including any payment arrears; and
- official public records information such as fraud record information and insolvency records.

The controller also includes information to advise the data subject that the credit scoring methods used are regularly tested to ensure they remain fair, effective and unbiased.
The controller provides contact details for the data subject to request that any declined decision is reconsidered, in line with the provisions of Article 22(3).

'Significance' and 'envisaged consequences'

This term suggests that information must be provided about intended or future processing, and how the automated decision-making might affect the data subject.[13] In order to make this information meaningful and understandable, real, tangible examples of the type of possible effects should be given.

[12]Complexity is no excuse for failing to provide information to the data subject. Recital 58 states that the principle of transparency is "of particular relevance in situations where the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him are being collected, such as in the case of online advertising".

[13] Council of Europe. Draft Explanatory Report on the modernised version of CoE Convention 108, paragraph 75: "Data subjects should be entitled to know the reasoning underlying the processing of their data, including the consequences of such a reasoning, which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated-decision making including profiling. For instance in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a 'yes' or 'no' decision, and not simply information on the decision itself. Without an understanding of these elements there could be no effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority."

Example

An insurance company uses an automated decision making process to set motor insurance premiums based on monitoring customers' driving behaviour. To illustrate the significance and envisaged consequences of the processing it explains that dangerous driving may result in higher insurance payments and provides an app comparing fictional drivers, including one with dangerous driving habits such as fast acceleration and last-minute braking.

It uses graphics to give tips on how to improve these habits and consequently how to lower insurance premiums.

Controllers can use similar visual techniques to explain how a past decision has been made.

2. Article 15(1) (h) - Right of access

Article 15(1) (h) entitles data subjects to have the same information about solely automated decision-making, including profiling, as required under Articles 13(2) (f) and 14(2) (g), namely:

- the existence of automated decision making, including profiling;
- meaningful information about the logic involved; and
- the significance and envisaged consequences of such processing for the data subject.

The controller should have already given the data subject this information in line with their Article 13 obligations.[14]

3. Article 22(1) – Right not to be subject to a decision based solely on automated decision-making

As explained earlier in this chapter, Article 22(1) acts as a prohibition on solely automated individual decision-making, including profiling with legal or similarly significant effects. Instead of the data subject having to actively object to the processing, the controller can only carry out the processing if one of the three exceptions covered in Article 22(2) applies.

Even where one of these exceptions does apply, the GDPR provides a further layer of protection for data subjects in Article 22(3)[15] "at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision". The controller must provide a simple way for the data subject to exercise these rights.

Human intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject.

---

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2 . Accessed 24 April 2017

[14] GDPR Article 12(3) clarifies the timescales for providing this information

[15] Where the basis for processing is Article 22(2)(a) or (c)

E. Special category data – Article 22(4)

Automated decision-making (described in Article 22(1)) that involves special categories of personal data is only allowed under certain conditions provided for in the GDPR or by Union or Member State Law (Article 22(4), referring to Article 9(2), (a) or (g)), namely:

> 9(2) (a) - the explicit consent of the data subject; or

> 9(2) (g) - processing necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

F. Establishing appropriate safeguards

If the basis for processing is 22(2)(a) or 22(2)(c), Article 22(3) requires controllers to implement suitable measures to safeguard data subjects' rights freedoms and legitimate interests. Such measures should include as a minimum a way for the data subject to obtain human intervention, express their point of view, and contest the decision. Recital 71 highlights that *in any case* suitable safeguards should also include:

> .. specific information to the data subject …… to obtain an explanation of the decision reached after such assessment and to challenge the decision.

Similarly, Article 22(2) (b) requires that the Member State law which authorises the processing includes suitable protections for data subjects.

This emphasises the need for transparency about the processing. The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis. Transparency requirements are discussed in Chapter III(section D).

Errors or bias in collected or shared data or an error or bias in the automated decision-making process can result in:

- incorrect classifications; and
- assessments based on imprecise projections; that
- impact negatively on individuals.

Controllers should carry out frequent assessments on the data sets they process to check for any bias, and develop ways to address any prejudicial elements, including any over-reliance on correlations. Systems that audit algorithms and regular reviews of the accuracy and relevance of automated decision-making including profiling are other useful measures.

Controllers should introduce appropriate procedures and measures to prevent errors, inaccuracies or discrimination on the basis of special category data[16]. These should be used on a cyclical basis; not

[16] GDPR Recital 71 says that:
"In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised,…."

only at the design stage, but also continuously, as the profiling is applied to individuals. The outcome of such testing should feed back into the system design.

Further examples of appropriate safeguards can be found in the Recommendations section.

III. General provisions on profiling and automated decision-making

This overview of the provisions applies to both profiling and automated decision-making.

A. Data protection principles

The principles are relevant for all profiling and automated decision-making involving personal data.[17] To aid compliance, controllers should consider the following key areas:

1. Article 5(1) (a) - Lawful, fair and transparent

Transparency of processing[18] is a fundamental requirement of the GDPR.

The process of profiling is often invisible to the data subject. It works by creating derived or inferred data about individuals – 'new' personal data that has not been provided directly by the data subjects themselves. Individuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes.

Under Article 12.1 the controller must provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data.[19]

For data collected directly from the data subject this should be provided at the time of collection (Article 13); for indirectly obtained data the information should be provided within the timescales set out in Article 14(3).

Example

Some insurers offer insurance rates and services based on an individual's driving behaviour. Elements taken into account in these cases could include the distance travelled, the time spent driving and the journey undertaken as well as predictions based on other data collected by the sensors in a (smart) car. The data collected is used for profiling to identify bad driving behaviour (such as fast acceleration, sudden braking, and speeding). This information can be cross-referenced with other sources (for example the weather, traffic, type of road) to better understand the driver's behaviour.

[17] GDPR – Recital 72 "Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles."

[18] The forthcoming WP29 Guidelines on transparency will cover transparency generally in more detail.

[19] Office of the Australian Information Commissioner. Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016 says: "Privacy notices have to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. *The very technology that leads to greater collection of personal information also presents the opportunity for more dynamic, multi-layered and user centric privacy notices."* https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles . Accessed 24 April 2017

The controller must ensure that they have a lawful basis for this type of processing. The controller must also provide the data subject with information about the collected data, the existence of automated decision-making, the logic involved, and the significance and envisaged consequences of such processing.

The specific requirements surrounding information and access to personal data are discussed in Chapters III (section D) and IV (section D).

Processing also has to be fair, as well as transparent.

Profiling may be unfair and create discrimination, for example by denying people access to employment opportunities, credit or insurance, or targeting them with excessively risky or costly financial products. The following example illustrates how unfair profiling can lead to some consumers being offered less attractive deals than others.

Example

A data broker sells consumer profiles to financial companies without consumer permission or knowledge of the underlying data. The profiles define consumers into categories (carrying titles such as "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Tough Start: Young Single Parents,") or "score" them, focusing on consumers' financial vulnerability. The financial companies offer these consumers payday loans and other "non-traditional" financial services (high-cost loans and other financially risky products).[20]

2. Article 5(1) (b) Further processing and purpose limitation

Profiling can involve the use of personal data that was originally collected for something else.

Example

Some mobile applications provide location services allowing the user to find nearby restaurants offering discounts. However, the data collected is also used to build a profile on the data subject for marketing purposes - to identify their food preferences, or lifestyle in general. The data subject expects their data will be used to find restaurants, but not to receive adverts for pizza delivery just because the app has identified that they arrive home late. This further use of the location data may not be compatible with the purposes for which it was collected in the first place, and may thus require the consent of the individual concerned.[21]

[20] This example is taken from: United States Senate, Committee on Commerce, Science, and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, December 18, 2013. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf . See page ii of the Executive Summary and 12 of the main body of the document in particular. Accessed 21 July 2017

[21] Note that the provisions of the future ePrivacy Regulation may also apply.

Whether this additional processing is compatible with the original purposes for which the data were collected will depend upon a range of factors[22], including what fair processing information the controller initially provided to the data subject. These factors are reflected in the GDPR[23]and summarised below:

- the relationship between the purposes for which the data have been collected and the purposes of further processing;
- the context in which the data were collected and the reasonable expectations of the data subjects as to their further use;
- the nature of the data and the impact of the further processing on the data subjects; and
- the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

3. Article 5(1) (c) Data minimisation

The business opportunities created by profiling, cheaper storage costs and the ability to process large amounts of information can encourage organisations to collect more personal data than they actually need, in case it proves useful in the future.

Controllers should be able to clearly explain and justify the need to collect and hold personal data, or consider using aggregated or otherwise anonymised (not just pseudonymised) data for profiling.

4. Article 5(1) (d) Accuracy

Controllers should consider accuracy at all stages of the profiling process, specifically when:

- collecting data;
- analysing data;
- building a profile for an individual; or
- applying a profile to make a decision affecting the individual.

If the data used in an automated decision-making or profiling process is inaccurate, any resultant decision or profile will be flawed. Decisions may be made on the basis of outdated data or the incorrect interpretation of external data. Inaccuracies may lead to inappropriate predictions or statements about, for example, someone's health, credit or insurance risk.

Even if raw data is recorded accurately, the dataset may not be fully representative or the analytics may contain hidden bias.

Controllers need to introduce robust measures to verify and ensure on an ongoing basis that data re-used or obtained indirectly is accurate and up to date. This reinforces the importance of providing clear information about the personal data being processed, so that the data subject can correct any inaccuracies and improve the quality of the data.

5. Article 5(1) (e) Storage limitation

Machine-learning algorithms are designed to process large volumes of information and build correlations. Storing collected personal data for lengthy periods of time means that organisations will

[22] Highlighted in the Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation,2 April 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf . Accessed 24 April 2017

[23] GDPR Article 6(4)

be able to build up very comprehensive, intimate profiles of individuals, since there will be more data for the algorithm to learn. Even if collection of the information fulfils the requirements of purpose specification and relevance, storing it for a long time may conflict with the proportionality consideration, i.e. the method may be too intrusive in terms of the individual's right to privacy.[24]

Keeping personal data for too long also increases the risk of inaccuracies.

B. Lawful bases for processing

For automated decision making under Article 22, please note that only some of the lawful bases listed here are available, as described in Chapter III (section C) above.

1. Article 6(1) (a) consent

Consent as a basis for processing generally will be addressed in the upcoming WP29 Guidelines on consent. Explicit consent is one of the exceptions from the prohibition on automated decision-making and profiling defined in Article 22(1).

Profiling can be opaque. Often it relies upon data that is derived or inferred from other data, rather than data directly provided by the data subject.

Controllers seeking to rely upon consent as a basis for profiling will need to show that data subjects understand exactly what they are consenting to. In all cases, data subjects should have enough relevant information about the envisaged use and consequences of the processing to ensure that any consent they provide represents an informed choice.

Where the data subject has no choice, for example, in situations where consent to profiling is a pre-condition of accessing the controller's services; or where there is an imbalance of power such as in an employer/employee relationship, consent is not an appropriate basis for the processing.

2. Article 6(1) (b) – necessary for the performance of a contract

This is covered in more detail in Chapter III(section C). The following is an example of profiling that would *not* meet the Article 6(1)(b) basis for processing.

Example

A user buys some items from an on-line retailer. In order to fulfil the contract, the retailer must process the user's credit card information for payment purposes and the user's address to deliver the goods. Completion of the contract is not dependent upon building a profile of the user's tastes and lifestyle choices based on his or her visits to the website. Even if profiling is specifically mentioned in the small print of the contract, this fact alone does not make it 'necessary' for the performance of the contract.

[24] Norwegian Data Protection Authority. The Great Data Race – How commercial utilisation of personal data challenges privacy, Report, November 2015. Datatilsynet https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/ Accessed 24 April 2017

3. Article 6(1) (c) – necessary for compliance with a legal obligation

There may be instances where there will be a legal obligation[25] to carry out profiling – for example in connection with fraud prevention or money laundering. For more detail, including the safeguards to be applied, see the WP29 Opinion on legitimate interests.

4. Article 6(1) (d) – necessary to protect vital interests

This covers situations where the processing is necessary to protect an interest which is essential for the life of the data subject or that of another natural person.

Certain types of processing may serve important public interest grounds as well as the vital interests of the data subject. Examples of this may include profiling necessary to develop models that predict the spread of life-threatening diseases or in situations of humanitarian emergencies. In these cases, however, and in principle, the controller can only rely on vital interest grounds if no other legal basis for the processing is available.[26] If the processing involves special category personal data the controller would also need to ensure that they meet the requirements of Article 9(2) (c).

5. Article 6(1) (e) – necessary for the performance of a task carried out in the public interest or exercise of official authority

Article 6(1) (e) might be an appropriate basis for public sector profiling in certain circumstances.

6. Article 6(1) (f) – necessary for the legitimate interests[27] pursued by the controller or by a third party

Profiling is allowed if it is necessary for the purposes of the legitimate interests[28] pursued by the controller or by a third party. However, Article 6(1) (f) does not automatically apply just because the controller has a legitimate interest. The controller must carry out a balancing exercise to assess whether their interests are overridden by the data subject's interests or fundamental rights and freedoms.

The following are particularly relevant:

- the level of detail of the profile (a data subject profiled within a broadly described cohort such as 'native English teachers living in Paris', or segmented and targeted on a granular level);
- the comprehensiveness of the profile (whether the profile only describes a small aspect of the data subject, or paints a more comprehensive picture);
- the impact of the profiling (the effects on the data subject); and
- the safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process.

The WP29 opinion on legitimate interests[29] explains the more common contexts where this issue arises and gives examples that may be relevant to profiling.

---

[25] GDPR Recitals 41 and 45

[26] GDPR Recital 46

[27] Legitimate interests listed in GDPR Recital 47 include processing for direct marketing purposes and processing strictly necessary for the purposes of preventing fraud.

[28] The controller's "legitimate interest" cannot render profiling lawful if the processing falls within the Article 22(1) definition.

[29] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. European Commission, 9 April 2014 ,P59 – examples 5and 7

The controller should also consider the future use or combination of profiles when assessing the validity of processing under Article 6(1) (f).

C. Article 9 – Special categories of data[30]

Controllers can only process special category personal data if they can meet one of the conditions set out in Article 9(2), as well as a condition from Article 6. This includes special category data derived or inferred from profiling activity.

Profiling can create special category data by inference from other data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods.

Correlations may be discovered that indicate something about individuals' health, political convictions, religious beliefs or sexual orientation, as demonstrated by the following example:

Example

One study[31] combined Facebook 'likes' with limited survey information and found that researchers accurately predicted a male user's sexual orientation 88% of the time; a user's ethnic origin 95% of the time; and whether a user was Christian or Muslim 82% of the time.

Informing data subjects is particularly important in the case of inferences about sensitive preferences and characteristics. The controller should make the data subject aware that not only do they process (non-special category) personal data collected from the data subject or other sources but also that they *derive* from such data other (and special) categories of personal data relating to them.

D. Rights of the data subject[32]

The GDPR introduces stronger rights for data subjects and creates new obligations for controllers.

In the context of profiling these rights are actionable against the controller creating the profile and the controller making an automated decision about a data subject (with or without human intervention), if these entities are not the same.

---

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Accessed 24 April 2017

[30] This Section is relevant for both profiling and automated decision-making. For automated decision-making under Article 22, please note the additional, specific provisions, as described in Chapter IV.F above.

[31] Michael Kosinski, David Stilwell and Thore Graepel. Private traits and attributes are predictable from digital records of human behaviour. Proceedings of the National Academy of Sciences of the United States of America, http://www.pnas.org/content/110/15/5802.full.pdf . Accessed 29 March 2017

[32] This Section is relevant for both profiling and automated decision-making. For automated decision making under Article 22, please note that there are also additional requirements when it comes to special categories of data, as described in Chapter III(section E) above.

Example

A data broker undertakes profiling of personal data. In line with their Article 13 and 14 obligations the data broker should inform the individual about the processing, including whether it intends to share the profile with any other organisations. The data broker should also present separately details of the right to object under Article 21(1).

The data broker shares the profile with another company. This company uses the profile to send the individual direct marketing.

The company should inform the individual (Article 14(1) (c)) about the purposes for using this profile, and from what source they obtained the information (14(2) (f)). The company must also advise the data subject about their right to object to processing, including profiling, for direct marketing purposes (Article 21(2)).

The data broker and the company should allow the data subject the right to access the information used (Article 15) to correct any erroneous information (Article 16), and in certain circumstances erase the profile or personal data used to create it (Article 17). The data subject should also be given information about their profile, for example in which 'segments' or 'categories' they are placed.[33]

If the company uses the profile as part of a solely automated decision-making process with legal or similarly significant effects on the data subject, the company is the controller subject to the Article 22 provisions. (This does not exclude the data broker from Article 22 if the processing meets the relevant threshold.)

1. Articles 13 and 14 – Right to be informed

Given the core principle of transparency underpinning the GDPR, controllers must ensure they explain clearly and simply to individuals how the profiling or automated decision-making process works.

In particular, where the processing involves profiling-based decision making (irrespective of whether it is caught by Article 22), then the fact that the processing is for the purposes of both (a) profiling and (b) making a decision based on the profile generated, must be made clear to the data subject.[34]

Recital 60 states that giving information about profiling is part of the controller's transparency obligations under Article 5(1) (a). The data subject has a right *to be informed* by the controller about and, in certain circumstances, a right *to object to* 'profiling', *regardless* of whether a fully automated individual decision based on profiling takes place.

Further information about the different approaches to transparency in the context of profiling is provided in the Recommendations section. More generally, the WP29 will also publish guidelines on transparency under the GDPR.

[33] The Norwegian Data Protection Authority. The Great Data Race -How commercial utilisation of personal data challenges privacy. Report, November 2015. https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/ Accessed 24 April 2017

[34] GDPR – Article 13(1)(c) and Article 14(1)(c)

2. Article 15 – Right of access

Article 15 gives the data subject the right to obtain details of any personal data used for profiling, including the categories of data used to construct a profile.

Article 15 implies a more general form of oversight, rather than a right to an explanation of *a particular* decision. Nevertheless, through the exercise of this right the data subject can become aware of a decision made, including one based on profiling him or her.

Recital 63 provides some protection for controllers concerned about revealing trade secrets or intellectual property, which may be particularly relevant in relation to profiling. It says that the right of access 'should not adversely affect the rights or freedoms of others'. However, only under rare circumstances should these rights outweigh individuals' rights of access; controllers should not use this as an excuse to deny access or refuse to provide any information to the data subject. These rights should be considered in context and balanced against individuals' rights to have information.

Recital 63 also specifies that 'where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.'

In addition to information about the profile, the controller should make available the data used as input to create the profile.

3. Article 16 - Right to rectification, Article 17 Right to erasure and Article 18 Right to restriction of processing

Profiling can involve an element of prediction, which increases the risk of inaccuracy. The input data may be inaccurate or irrelevant, or taken out of context. There may be something wrong with the algorithm used to identify correlations.

The Article 16 right to rectification might apply where, for example, an individual is placed into a category that says something about their ability to perform a task, and that profile is based on incorrect information. Individuals may wish to challenge the accuracy of the data used and any grouping or category that has been applied to them.

Article 16 also provides a right for the data subject to complement the personal data with additional information.

Example

A local surgery's computer system places an individual into a group that is most likely to get heart disease. This 'profile' is not necessarily inaccurate even if he or she never suffers from heart disease. The profile merely states that he or she is *more likely* to get it. That may be factually correct as a matter of statistics.

Nevertheless, the data subject has the right, taking into account the purpose of the processing, to provide a supplementary statement. In the above scenario, this could be based, for example, on a more advanced medical computer system (and statistical model) carrying out more detailed examinations and factoring in additional data than the one at the local surgery with more limited capabilities.

The right to rectification applies to the 'input personal data' (the personal data used to create the profile) and to the 'output data' (the profile itself or 'score' assigned to the person, which is personal data relating to the person concerned).

Similarly the right to erasure (Article 17) will apply to both the input and the output data. If the basis for profiling is consent and that consent is withdrawn, the controller must erase the relevant personal data – unless there is another legal basis for the profiling. [35] The right to restrict processing (Article 18) will apply to any stage of the profiling process.

4. Article 21 – Right to object

The controller has to bring details of the right to object under Article 21(1) and (2) *explicitly* to the data subject's attention, and present it clearly and separately from other information (Article 21(4)).

Under **Article 21(1)** the data subject can object to processing (including profiling), on grounds relating to his or her particular situation. Controllers are specifically required to provide this right in all cases where processing is based on Article 6(1) (e) or (f).

Once the data subject exercises this right, the controller must interrupt[36] (or avoid starting) the profiling process unless it can demonstrate compelling legitimate grounds that override the interests or rights and freedoms of the data subject. The controller may also have to erase the relevant personal data.[37]

The GDPR does not provide any explanation of what would be considered compelling legitimate grounds. [38] It may be the case that, for example, the profiling is beneficial for society at large (or the wider community) and not just the business interests of the controller, such as the interest in carrying out scientific research, or profiling to predict the spread of contagious diseases.

The controller would also need to prove that:

- the impact on data subjects is limited to the minimum necessary to meet the particular objective (i.e. the profiling is the least intrusive way to achieve this); and
- the objective is critical for the organisation .

There must always be a balancing exercise between the competing interests of the controller and the basis for the data subject's objection (which may be for personal, social or professional reasons). Unlike in the Directive, the burden of proof to show compelling legitimate grounds lies with the controller rather than the data subject.

Article 21(2) grants an *unconditional* right for the data subject to object to the processing of their personal data for direct marketing purposes, including profiling to the extent that it is related to such direct marketing. This means that there is no need for any balancing of interests; the controller must respect the individual's wishes without questioning the reasons for the objection. Recital 70 provides additional context to this right and says that it may be exercised at any time and free of charge.

---

[35] GDPR – Article 17(1)(b)

[36] GDPR- Article 18(1)(d)

[37] GDPR – Article 17(1)(c)

[38] See explanation on legitimacy p. 24, Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. European Commission. 9 April 2014. Page 26 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Accessed 24 April 2017

IV. Children and profiling

The GDPR creates additional obligations for data controllers when they are processing children's personal data.

Article 22 itself makes no distinction as to whether the processing concerns adults or children. However, recital 71 says that solely automated decision-making, including profiling, with legal or similarly significant effects should not apply to children.[39] Given that this wording is not reflected in the Article itself, WP29 does not consider that this represents an absolute prohibition on this type of processing in relation to children. However, in the light of this recital, WP29 recommends that, wherever possible, controllers should not rely upon the exceptions in Article 22(2) to justify it.

There may nevertheless be some circumstances in which it is necessary for controllers to carry out solely automated decision-making, including profiling, with legal or similarly significant effects in relation to children, for example to protect their welfare. If so, the processing may be carried out on the basis of the exceptions in Article 22(2)(a), (b) or (c) as appropriate.

In those cases there must be suitable safeguards in place, as required by Article 22(2)(b) and 22(3), and they must therefore be appropriate for children. The controller must ensure that these safeguards are effective in protecting the rights, freedoms and legitimate interests of the children whose data they are processing.

The need for particular protection for children is reflected in recital 38, which says:

> 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 and the collection of personal data with regard to children when using services offered directly to a child.*

Article 22 does not prevent controllers from making solely automated decisions about children, if the decision will not have a legal or similarly significant effect on the child. However, solely automated decision making which influences a child's choices and behaviour could potentially have a legal or similarly significant effect on them, depending upon the nature of the choices and behaviours in question.

Because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes. Children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising. For example, in online gaming, profiling can be used to target players that the algorithm considers are more likely to spend money on the game as well as providing more personalised adverts. The age and maturity of the child may affect their ability to understand the motivation behind this type of marketing or the consequences.[40]

Article 40(2) (g) explicitly refers to the preparation of codes of conduct incorporating safeguards for children; it may also be possible to develop existing codes.[41]

---

[39] Recital 71 – "such measure should not concern a child".

[40] An EU study on the impact of marketing through social media, online games and mobile applications on children's behaviour found that marketing practices have clear impacts on children's behaviour.

[41] One example of a code of conduct dealing with marketing to children is that produced by FEDMA Code of conduct, explanatory memorandum, available at: http://www.oecd.org/sti/ieconomy/2091875.pdf Accessed 15

V. Data protection impact assessments (DPIA)

Accountability is an important area and an explicit requirement under the GDPR. [42]

A DPIA enables the controller to assess the risks involved in automated decision-making, including profiling. It is a way of showing that suitable measures have been put in place to address those risks and demonstrate compliance with the GDPR.

Article 35(3) (a) highlights the need for the controller to carry out a DPIA in the case of:

> *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) refers to evaluations including profiling and decisions that are 'based' on automated processing, rather than 'solely' automated processing. We take this to mean that Article 35(3) (a) will apply in the case of decision-making including profiling with legal or similarly significant effects that is *not* wholly automated, as well as solely automated decision-making defined in Article 22(1).

Controllers could consider additional measures[43] such as:

- informing the data subject about the existence of and the logic involved in the automated decision-making process;
- explaining the significance and envisaged consequences of the processing for the data subject;
- providing the data subject with the means to oppose the decision; and
- allowing the data subject to express their point of view.

Other profiling activities may warrant a DPIA, depending upon the specifics of the case. Controllers may wish to consult the WP29 guidelines on DPIAs[44] for further information and to help determine the need to carry out a DPIA.

May 2017. See, in particular: "6.2 Marketers targeting children, or for whom children are likely to constitute a section of their audience, should not exploit children's credulity, loyalty, vulnerability or lack of experience.; 6.8.5 Marketers should not make a child's access to a website contingent on the collection of detailed personal information. In, particular, special incentives such as prize offers and games should not be used to entice children to divulge detailed personal information."

[42] As required by the GDPR Article 5(2)

[43] Mirroring the requirements in Article 13(2)(f), Article 14(2)(g) and Article 22(3)

[44] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 4 April 2017. European Commission. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Accessed 24 April 2017.

ANNEX 1 - Good practice recommendations

The following good practice recommendations will assist data controllers in meeting the requirements of the GDPR provisions on profiling and automated decision making.[45]

Article	Issue	Recommendation
5(1)(a),12, 13, 14	Right to have information	Controllers may wish to consider: • layered notices, where data subjects are informed about the processing of their data on a step by step basis. This type of approach can work by providing the key privacy information in a short notice, with links to expand each section to its full version, and a just in time notification at the point where the data is collected; • visualisation and interactive techniques to aid algorithmic transparency[46]; • standardised icons[47] to inform individuals about profiling and automated decision-making, for example: o The organisation shares their personal data with other organisations; o Details of the other organisations with whom their personal data is shared; o Whether this/these organisation(s) is/are using their personal data to profile them; o Whether the profile is being used to make decisions about them. Meaningful information about the logic involved will in most cases require controllers to provide details such as: • the information used in the automated decision-making process, including the categories of data used in a profile; • the source of that information; • how any profile used in the automated decision-making process is built, including any statistics used in the analysis; • why this profile is relevant to the automated decision-making process; and • how it is used for a decision concerning the data subject.
5(1)(b)	Further processing	If the processing is outside what the individual concerned would reasonably expect, or would have an unjustified adverse effect on them, controllers should regard the use or disclosure as incompatible with the original purpose for obtaining the information.

[45] Controllers also need to ensure they have robust procedures in place to ensure that they can meet their obligations under Articles 15 – 22 in the timescales provided for by the GDPR.
[46] Information Commissioner's Office .Big data, artificial intelligence, machine learning and data protection , page 87, paragraph 194. ICO, 1 March 2017. https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ Accessed 24 April 2017
[47] As envisaged in Article 12(7)

Article	Issue	Recommendation
6(1)(a)	Consent as a basis for processing	If controllers are relying upon consent as a basis for processing they should: • provide sufficiently clear and comprehensive information about the profiling to ensure that data subjects understand what they are consenting to ; • consider introducing a process of granular consent where they provide a clear and simple way for data subjects to agree to different purposes for processing; • actively seek consent from the data subject before any new processing takes place; • inform the data subject that they can withdraw consent.
15	Right of access	Information about the categories of data that have been or will be used in the profiling or decision making process and why these are considered pertinent will generally be more relevant than providing a complex mathematical explanation about how algorithms or machine-learning work, although the latter should also be provided if this is necessary to allow experts to further verify how the decision –making process works. Controllers may want to consider implementing a mechanism for data subjects to check their profile, including details of the information and sources used to develop it.
16	Right to rectification	Controllers providing data subjects with access to their profile in connection with their Article 15 rights should allow them the opportunity to update or amend any inaccuracies in the data or profile. This can also help them meet their Article 5(1) (d) obligations. Controllers should consider introducing online preference management tools such as a privacy dashboard. This gives data subjects the option of managing what is happening to their information across a number of different services – allowing them to alter settings, update their personal details, and review or edit their profile to correct any inaccuracies.
21(1) and (2)	Right to object	The right to object in Article 21(1) and (2) has to be explicitly brought to the attention of the data subject and presented clearly and separately from other information (Article 21(4). Controllers need to ensure that this right is prominently displayed on their website or in any relevant documentation and not hidden away within any other terms and conditions.

Article	Issue	Recommendation
22 and Recital 71	Appropriate safeguards	The following list, though not exhaustive, provides some good practice suggestions for controllers to consider when profiling: • regular quality assurance checks of their systems to make sure that individuals are being treated fairly and not discriminated against, whether on the basis of special categories of personal data or otherwise; • algorithmic auditing – testing the algorithms used and developed by machine learning systems to prove that they are actually performing as intended, and not producing discriminatory, erroneous or unjustified results; • specific measures for data minimisation to incorporate clear retention periods for profiles and for any personal data used when creating or applying the profiles; • using anonymisation or pseudonymisation techniques in the context of profiling; • ways to allow the data subject to express his or her point of view and contest the decision; and, • a mechanism for human intervention in defined cases, for example providing a link to an appeals process at the point the automated decision is delivered to the data subject, with agreed timescales for the review and a named contact point for any queries . Controllers can also explore options such as: • certification mechanisms for processing operations; • 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.

ANNEX 2 – Key GDPR provisions

Key GDPR provisions that reference automated decision-making as defined in Article 22

Article	Recital	Comments
13(2)(f) and **14(2)(g)**	**61**	Right to be informed about: • the existence of automated decision-making under **A22(1)** and **(4);** • meaningful information about the logic involved; • significance and envisaged consequences of such processing.
15(h)		Specific access rights to information about the existence of solely automated decision-making, including profiling.
22(1)	**71**	Prohibition on decision-making based solely on automated processing, including profiling, which produces legal/similarly significant effects. **Recital 71**: "…Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements"……. "*Such measure should not concern a child*"
22(2)(a-c)	**71**	**Article 22(2)** lifts the prohibition for processing based on **(a)** the performance of or entering into a contract, **(b)** Union or Member state law, or **(c)** explicit consent. **Recital 71** provides further context on **22(2)(b)**and says that processing described in **A22(1):** "should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller…"
22(3)	**71**	**Article 22 (3) and Recital 71** also specify that even in the cases referred to in **22(2)(a)** and **(c)** the processing should be subject to suitable safeguards. **Recital 71:** "which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child."
23	**73**	**Recital 73:** "Restrictions concerning specific principles and concerning …….the right to object and decisions based on profiling …….may be imposed by Union or Member State law as far as necessary and proportionate in a democratic society…" to safeguard specific objectives of general public interest.
35(3)(a)	**91**	Requirement to carry out a DPIA.
47(2)(e)		Binding corporate rules referred to in **47(1)** should specify at least "…….the right not to be subject to decisions based solely on automated processing, including profiling in accordance with **Article 22**..."

Key GDPR provisions that reference general profiling and automated decision-making

Article	Recital	Comments
3(2)(b)	**24**	Monitoring behaviour of EU citizens. **Recital 24** "….tracked on the internet ……use of personal data processing techniques which consist of profiling a natural person, *particularly in order to take decisions* concerning her or him or for analysing or predicting her or his personal preferences, behaviours or attitudes".
4(4)	**30**	**Article 4(4)** definition of profiling **Recital 30** "online identifiers …., such as Internet Protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags… may leave traces which, in particular when combined with unique identifiers and other information received by the servers, *may be used to create profiles of the natural persons and identify them*."
5 and 6	**72**	**Recital 72**: "Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing **(Article 6)** or data protection principles **(Article 5)**."
8	**38**	Use of children's personal data for profiling. **Recital 38:** "Children merit specific protection ….. in particular,…to the use of personal data of children for the purposes of….creating personality or user profiles."
13 and 14	**60**	Right to be informed. **Recital 60**: "Furthermore, the data subject *shall be informed of the existence of profiling and the consequences of such profiling*."
15	**63**	Right of access. **Recital 63:** "right to know and obtain communication…..with regard to the purposes for which the personal data are processed,…..and, *at least* when based on profiling, the consequences of such profiling".
21(1)(2) and (3)	**70**	Right to object to profiling. **Recital 70** "…the right to object to such processing, including profiling to the extent that it is related to such direct marketing."
23	**73**	**Recital 73:** "Restrictions concerning specific principles and concerning …….the right to object and decisions based on profiling …….may be imposed by Union or Member State law as far as necessary and proportionate in a democratic society…" to safeguard specific objectives of general public interest.
35(3)(a)	**91**	A DPIA is required in the case of "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;" **Covers decision-making including profiling that is not solely automated.**

ANNEX 3 - Further reading

These Guidelines take account of the following:

- WP29 Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted 13 May 2013;
- WP29 Opinion 2/2010 on online behavioural advertising, WP171;
- WP29 Opinion 03/2013 on Purpose limitation, WP 203;
- WP29 Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217
- WP29 Statement on the role of a risk-based approach to data protection legal frameworks, WP218;
- WP29 Opinion 8/2014 on the Recent Developments on the Internet of Things, WP223;
- WP29 Guidelines on Data Protection Officers (DPOs), WP243;
- WP29 Guidelines on identifying a controller or processor's lead supervisory authority, WP244;Council of Europe. Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling;
- Council of Europe. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 01/2017
- Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017
- Office of the Australian Commissioner - Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016
- European Data Protection Supervisor (EDPS) Opinion 7/2015 – Meeting the challenges of big data, 19 November 2015
- Datatilsynet – Big Data – privacy principles under pressure 09/2013
- Council of Europe. Convention for the protection of individuals with regard to automatic processing of personal data - Draft explanatory report on the modernised version of CoE Convention 108, August 2016
- Datatilsynet – The Great Data Race – How commercial utilisation of personal data challenges privacy. Report, November 2015
- European Data Protection Supervisor – Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit
- Joint Committee of the European Supervisory Authorities. Joint Committee Discussion Paper on the use of Big Data by financial institutions 2016-86. https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf.
- Commission de la protection de la vie privée. Big Data Rapport https://www.privacycommission.be/sites/privacycommission/files/documents/Big%20Data%20voor%20MindMap%2022-02-17%20fr.pdf.
- United States Senate, Committee on Commerce, Science, and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, December 18, 2013. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf
- Lilian Edwards & Michael Veale. Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for. Research paper, posted 24 May 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855
- NYTimes.com. Showing the Algorithms behind New York City Services. https://mobile.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city-services.html?referer=https://t.co/6uUVVjOIXx?amp=1. Accessed 24 August 2017

- Council of Europe. Recommendation CM/REC(2018)x of the Committee of Ministers to Member States on Guidelines to promote, protect and fulfil children's rights in the digital environment (revised draft, 25 July 2017). https://www.coe.int/en/web/children/-/call-for-consultation-guidelines-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in-the-digital-environment?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fchildren . Accessed 31 August 2017
- Unicef. Privacy, protection of personal information and reputation rights. Discussion paper series: Children's Rights and Business in a Digital World. https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf. Accessed 31 August 2017
- House of Lords. Growing up with the internet. Select Committee on Communications, 2nd Report of Sessions 2016 – 17. https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm. Accessed 31 August 2017