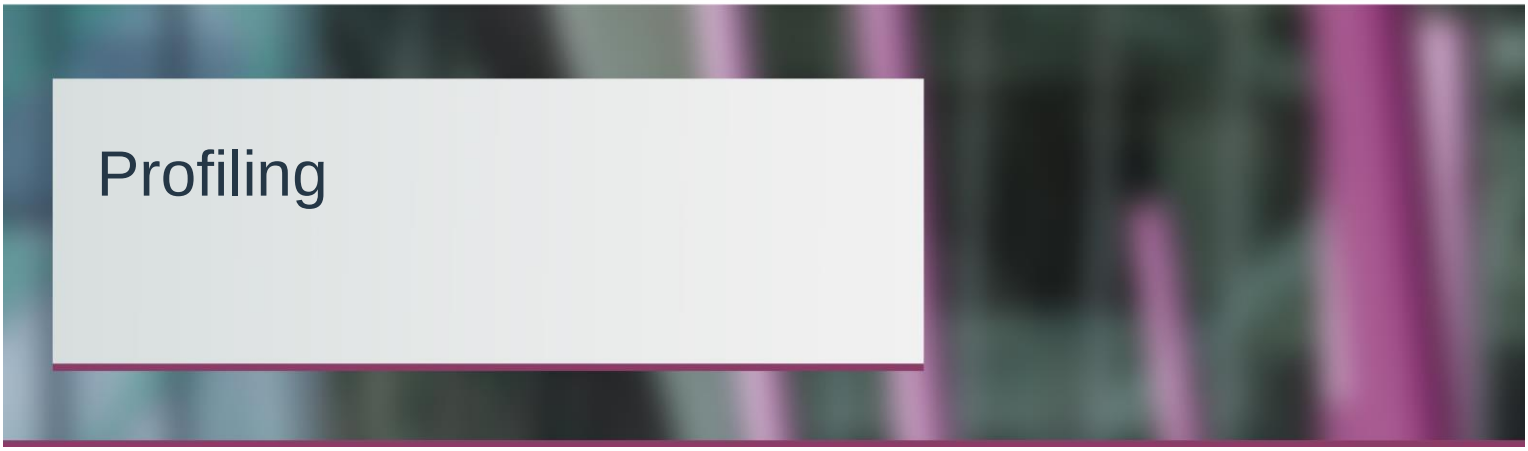
WILLIAM FRY

// PRIVACY SOURCE



Profiling

The EU General Data Protection Regulation ("**GDPR**") has introduced a number of changes with respect to profiling. The most significant of these include:

- a legal definition of "***profiling***" for the first time in European data protection law;
- **explicit consent** as a new legal basis to process personal data through profiling;
- the circumstances in which **sensitive personal data** may be profiled are limited further;
- a prescriptive obligation to inform data subjects at the time of collection of personal data (and on receiving a data access request) as to the existence of profiling (information provided must detail the "*logic involved*" in profiling *"as well as the significance and the envisaged consequences of such processing for the data subject"*); and
- where a non-European Economic Area based data **controller monitors the behaviour** of data subjects in the European Union ("EU") (i.e. profiling), such a data controller will be subject to the rules of the GDPR.

Data controllers must be aware of the more onerous obligations imposed on them in addition to the enhanced rights of data subjects with respect to profiling under GDPR.

What is profiling?

Profiling refers to the **automated processing of personal data** to evaluate a data subject and in particular, to analyse or predict future processing of personal data of a data subject. Opponents often point to the absence of human interaction or intervention as being the most objectionable element of profiling, particularly where this can give rise to significant consequences for the person being profiled.

Profiling is often used to analyse particular aspects of an individual's life, including:

Performance at work	**Economic situation**	**Interest or personal preferences**
Health	**Reliability or behaviour**	**Location or movements**

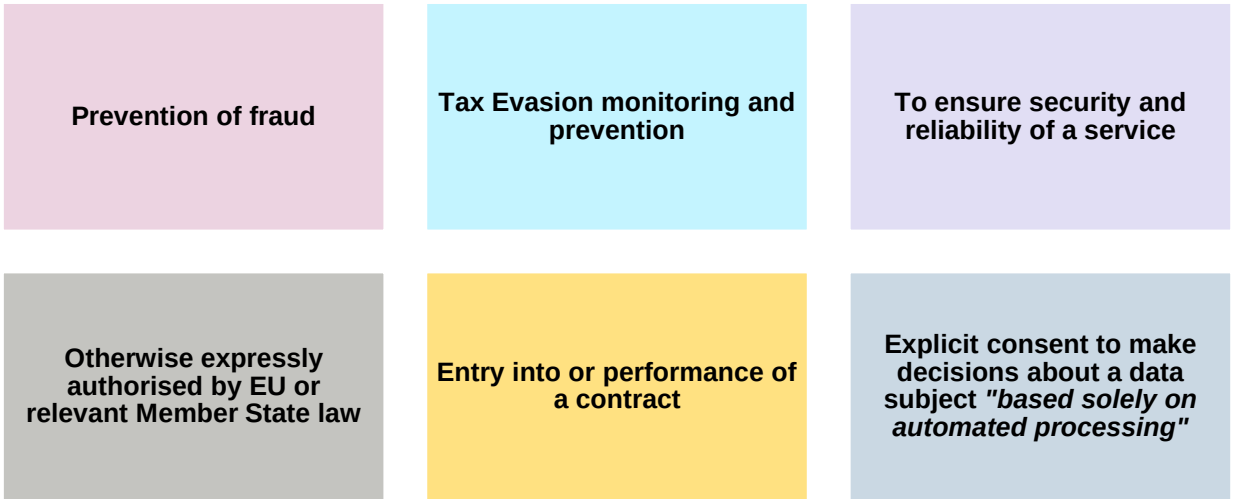
Profiling requires some sort of outcome (i.e. "*consequences*") affecting a data subject as a result of the processing of their personal data. Under the terms of the GDPR, this means a decision must have legal effects or otherwise significantly affect a data subject.

Therefore, profiling is not simply the collection the personal data in relation to personal aspects of a data subject's life - it is the automated processing of such data for the purposes of making a decision about that data subject.

Three key features of profiling

Lawful profiling

To profile personal data lawfully, a data controller must be able to rely on one of the following legal bases:



Once a data controller has a legal basis, a data controller must then implement suitable safeguards to protect the rights, freedoms and legitimate interests of data subjects. For example, appropriate safeguards could be the use of encryption or pseudonymisation.

A data controller must also use appropriate mathematical or statistical procedures, implement technical and organisational measures to correct personal data inaccuracies and avoid errors, secure all personal data, and minimise the risk of "*discriminatory effects against natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status, or sexual orientation.*"

Restrictions with respect to profiling

Under GDPR, a data subject has protection against being subjected to a decision based solely on automatic processing (including profiling) which produces "legal effects" or "significantly affects" him/her and can in certain instances, restrict such processing. These terms await interpretation and the European Data Protection Board is expected to issue guidance on this area in due course.

There are three criteria which may trigger a data subject's ability to restrict automated processing of personal data (of which profiling is included):

1. a decision has been made about the data subject;
2. which has a legal effect for that data subject or significantly affects him or her; and
3. the decision is based solely on automated processing.

If these three criteria are met, then the automated processing can be restricted, unless one of the following conditions applies:

- EU or Member State law or regulation within a Member State to which the controller is subject authorises the profiling activity;
- the profiling activity is necessary for the purpose of entering into or performing a contract with the individual concerned; or
- the data subject concerned has given his/her explicit consent to use his/her personal data for profiling purposes.

Rights of data subjects in the context of profiling

The following rights must be communicated to data subjects and clearly separated from other information at the time of data collection or, at the latest, at the time of the first communication between a data controller and a data subject.

Notice

Data subjects must be informed as to the existence of profiling, the "logic involved" in that profiling and the "envisaged consequences" of profiling

Access

Data subjects can inquire with a data controller and receive confirmation of any processing, including profiling and its consequences at any time.

Objection

Even where profiling is lawful, a data subject can object to such processing at any time (subject to the overriding principles discussed in the next section below).

Human intervention

There is a right for a data subject to obtain human intervention, to express his/her point of view, to obtain an explanation of the decision reached after the assessment (determined on profiling) and to challenge the decision. The ability of a data subject to contest the decision will continue to apply even where explicit consent or performance of a contract are the legal bases for processing.

Data controllers with compelling legitimate grounds to continue profiling where the right to object is exercised

The right to object exists at all times and a data controller must stop the profiling activities in question unless it can demonstrate *"compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims".* It is not yet clear what evidence a data controller would be required to demonstrate in such circumstances, although it is expected that the bar will be set quite high.

Of particular relevance to data controllers; when profiling is for the purposes of direct marketing, a data controller cannot rely on compelling legitimate grounds to continue profiling.

Sensitive or special categories of personal data

Decisions based on profiling cannot be based on special categories of personal data such as racial, ethnic, or religious information unless:

- the data subject has given explicit consent, except where prohibited by EU or Member State law; or
- processing is necessary for reasons of substantial public interest, on the basis of EU or Member State law. Even in these circumstances, again the data controller must still ensure "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

It is likely the European Data Protection Board will provide additional guidance on the circumstances under which profiling-based decisions are permissible for special categories of personal data.

Conclusion

With advancements in technology, profiling is easier than ever before and with the trend towards customisation, profiling may seem an attractive tool for companies. While further guidance will be necessary, companies as data controllers must nonetheless understand their obligations and restrictions with respect to profiling and data subjects' enhanced rights under GDPR.

Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partner below, or your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 51823
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA