OneTrust
Privacy Management Software

WP29 Guidelines on Profiling and Automated Decision-Making for the Purpose of GDPR

October 24, 2017

Introduction

Profiling and automated decision-making is a growing practice across all sectors of society (including finance, healthcare, insurance, marketing, employment, etc.) The recent developments in technology – especially AI (Artificial Intelligence), machine learning technology, and big data analytics – along with the increasing amount of personal data available (e.g., through IoT), allow companies to engage in profiling and automated decision-making much more easily than before.

While these processing activities can be beneficial to individuals, organizations, and society, as a whole, in some circumstances, they also pose important risks for individuals.

The GDPR contains specific provisions about profiling and automated decision-making, but has also raised questions about their scope and how they may apply in practice. The WP29 recently released proposed guidelines on profiling and automated decision-making which attempt to answer some of these questions.

Clarification of the Concepts

Profiling

Article 4(4) GDPR defines profiling 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."

The WP29 clarifies the three key criteria for an activity to be considered profiling. It must be:

- ⇨ *Automated (in any form, whether fully automated or without human intervention, or not),*
- ⇨ *Carried out on personal data,*
- ⇨ *With the objective of evaluating personal aspects of a person.*

It also clarifies that there is profiling as soon as a controller collects personal information about individuals to analyze their characteristics and/or behaviors and put them into categories or groups. While there is also profiling when the controller uses the profiles to make predictions about the individuals, this predictive aspect is not necessary.

- ⇨ *The WP29 confirms what organizations already suspected –– the concept of profiling is extremely broad, simply putting individuals into categories based on their characteristics or behaviors constitutes profiling.*

Automated Decision-Making

The WP29 clarifies that automated decision-making is a concept that is distinct from profiling. Automated decision-making happens when a decision is made using technological means, whether the decision is based on profiling (e.g., detecting a speeding infraction and imposing a fine tailored to the infringer's driving behaviors and past infringements), or not (e.g., detecting a speeding infraction and automatically imposing a fine, without analyzing the infringer's behavior.)

A solely automated decision-making process is one where the decision is made exclusively by technological means, without any human intervention.

- ⇨ *Being able to distinguish between profiling activities, automated decision-making, and solely automated decision-making is crucial, as different data protection principles apply to these different processing activities:*
- ⇨ *The GDPR legal framework applies to profiling in general (including when it is used for non-solely automated decision-making), and*
- ⇨ *Specific provisions apply when solely automated decision-making, including profiling, which is used to produce legal or similarly significant effects on individuals (Article 22 GDPR.)*

Application of GDPR Principles to Profiling in General

GDPR Principles

All profiling and automated decision-making processes, regardless of their scope, must comply with the general principles of the GDPR. The WP29 guidelines provide an overview of these principles and some key considerations to keep in mind when developing a profiling or automated decision-making processing activity.

Lawfulness, fairness, and transparency	Controllers should be particularly mindful of their transparency obligations in the context of profiling, as most of the processing is often invisible to individuals. Fairness of the processing must also be carefully considered, as inaccurate profiling or decision-making can often lead to discrimination. ⇨ *Organisations should ensure that they inform individuals about any personal data that they derive from inferences and correlations with other data. For instance, an insurer applying driving behaviours based rates should explain what specific behaviours are considered (e.g., fast acceleration, etc.), and how it cross-references this data with other sources (e.g., weather, traffic, etc.).*
Purpose limitation	Controllers should not re-use data collected for a specific purpose to create profiles and make new decisions based on those profiles, unless that new processing is considered compatible. ⇨ *The creation and use of profiles will generally be considered incompatible when it is outside what individuals would reasonably expect or would have unjustified adverse effect on them.*
Data minimisation	In the context of big data and machine learning, the tendency is often to collect more data. Not all data collected may however be justified for the purpose. ⇨ *Organisations should carefully review the necessity of the data they collect for profiling or automated decision-making, and use aggregated or anonymised data where possible.*
Accuracy	Data accuracy is particularly crucial in profiling or automated decision-making as any inaccuracy in the dataset will necessarily lead to flawed results and decisions. Controllers should also be mindful of the risk of hidden bias resulting from non-fully representative datasets. ⇨ *Organisations should implement robust measures to verify – on an ongoing basis – the accuracy of their datasets.*
Storage limitation	Machine learning and big data technology is usually designed to process a large amount of data, and the tendency is often to retain data for long periods of time. ⇨ *Organisations should make sure they only keep personal data to the extent necessary and proportionate to the purpose. Deleting personal data no longer necessary will also help them making sure their datasets remain accurate and up to date, and therefore limits the risk of inaccuracies.*

Lawful Basis for Processing

In the context of profiling and automated decision-making, only some of the legal bases listed under Article 6 GDPR will be relevant. In the guidelines, the WP29 reviews each of them and provide examples or recommendations on how and when it is appropriate for organizations to rely on them.

Consent	⇨ *When they rely on consent for justifying the profiling or automated decision-making, organisations should ensure they provide sufficiently clear and comprehensive information about the profiling, use granular consent where they process data for different purposes, seek new consent before any new processing, and inform individuals of the right to withdraw consent.* ⇨ *Where the processing consists in fully automated decision-making producing legal or similarly significant effects on individuals, organisations must ensure the consent is explicit.*
Contract	⇨ *Contract necessity should be careful considered. Merely mentioning profiling in the contract will not constitute a valid basis for the processing where the profiling is not necessary for performance of the contract, e.g., completing an online purchase.*
Legal obligation	⇨ *Controllers may be required to conduct profiling under specific laws, e.g., in the context of fraud prevention or money laundering.*
Vital interests	⇨ *Although these circumstances will be exceptional, certain profiling activities may meet this requirement, e.g., developing a model that predicts the spread of a life-threatening disease or for humanitarian emergencies.*
Public interest	⇨ *According the WP29, this legal basis may be appropriate for public sector profiling, in certain circumstances only.*
Legitimate interests	⇨ *Organisations should only rely on this legal basis for their profiling activities if the interests of individuals do not override they legitimate business interests.* ⇨ *This balancing exercise requires assessing the level of detail of the profiles and its comprehensiveness, the impact of the profiling for individuals, and the safeguards in place to ensure fairness, non-discrimination and accuracy of the processing.*

Data Subject Rights

The guidelines also provide some explanation on how data subject rights may be exercised in the context of profiling and automated decision-making. The WP29 main findings can be summarized as follows:

- Data subject rights may be enforced against **both** the controller that creates profiles (e.g., a data broker) and the controller that uses them for automated decision-making (e.g., the company using the profiles for direct marketing), where there are different entities,
- Controllers should make sure that **information** provided to individuals allows them to adequately understand the profiling and its consequences (see also below,)
- Controllers may invoke the protection of trade secrets or intellectual property as a limitation to the **right of access** in the context of profiling, but should not use this as an excuse for not providing any information; a balancing exercise is required,
- The **right of rectification** applies to both input and output data,
- Where the profiling is beneficial to society at large, (e.g., in the context of scientific research or for analyzing the spread of a contagious disease,) controllers may oppose to the right of individuals to **object** to the profiling, based on a compelling legitimate ground, but when the profiling is carried out for marketing purposes, the right to object is absolute.

Prohibition of Solely Automated Individual Decision-Making – Article 22 GDPR

Article 22 GDPR Establishes a General Prohibition on Processing

Article 22 GDPR provides that "data subjects shall have *the right not to be subject to* a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

The guidelines expressly state that Article 22 imposes a general prohibition on this kind of processing, unless one of the three exceptions listed in the provision apply (e.g. contract necessity, legal authorization, or explicit consent).

> ⇨ *By clearly stating that Article 22 GDPR acts as a general prohibition on processing (unless one of the three exceptions apply), the WP29 closes a long-standing debate on the scope of this provision: legitimate interest is **not** a valid legal basis for this type of processing.*

Clarification of Key Criteria

The WP29 also clarifies the key criteria of this provision:

- *To be considered **not solely automated**, the decision-making process needs meaningful oversight by a person that has the authority and competence to change the decision – human involvement cannot be fabricated.*
- *A **"legal effect"** refers to the impact on the individual's legal rights, whether they derive from a statutory provision or a contract. This includes, for example: refused entry at the border, denial of social benefit, automatic disconnection from phone service, as well as increased surveillance by the authorities.*
- ***"Similarly significantly affects"** refers to a decision that has sufficiently important impact on an individual, as opposed to trivial, (e.g. one that can potentially influence the circumstances, behaviors, or choices of the individual.) Traditional examples include refusal of a loan or automatic e-recruiting decisions. The WP29 also specifies that this concept covers both positive and negative impacts. The "significant impact" could also be triggered by actions of other individuals than the one to which the decision relates (e.g., granting of credit line based on profiling of individuals living in the same neighborhood.)*

Most typical cases of **targeted advertising** will not be considered as having "similarly significant effects," although it may be the case under certain circumstances (e.g., targeted advertising isolating a minority group or vulnerable persons.)

Relevant criteria of the assessment include: intrusiveness of the processing, expectations and wishes of the individual, the way the ad is delivered, and the vulnerabilities of the individual targeted.

⇨ *Organizations should carefully assess all possible consequences of their profiling and automated decision-making activities on individuals as the concept of "similar significant effects," as defined by the WP29, appears relatively broad. It will have to be assessed on a case-by-case basis.*

Processing Only Permitted Under Three Circumstances

The WP29 clarifies that the three conditions listed in the provision (contract necessity, legal authorization, and explicit consent) are exceptions to the general prohibition on processing. Consequently, the contract necessity requirement needs to be narrowly interpreted and consent needs to be explicit, which means that it must be specifically confirmed by an express statement rather than some other affirmative action.

Establishing Appropriate Safeguards

Article 22(3) GDPR provides that when the automated decision-making is based on contract necessity or explicit consent, appropriate safeguards need to be put in place to protect the rights of individuals. They must include, at minimum, a way for individuals to obtain human intervention, to express their point of view, and to contest the decision.

The WP29 also insists on the need for controllers to carry out regular assessments of their datasets to identify potential errors and biases and correct them, to audit their algorithms, and to implement procedures to prevent errors and discrimination based on sensitive data.

- ⇨ *Safeguards must include, at minimum, a way for individuals to obtain human intervention, to express their point of view, and to contest the decision.*
- ⇨ *As good practice, organizations should also implement data minimization measures (including retention periods for profiles), anonymization and pseudonymization techniques, quality assurance checks (to prevent errors, unfair or discriminatory results), and algorithm auditing and testing.*
- ⇨ *These measures and procedures should be used on a cyclical basis – the outcome of any testing should feed back into the system.*
- ⇨ *Organizations are invited to consider adoption of certification mechanisms, codes of conduct, and ethical review boards to help them identify and implement appropriate safeguards.*

Need for Transparency

The WP29 insists that, to be able to adequately challenge a fully automated decision, individuals need to have clear understanding of how the decision is made. Transparency is therefore crucial in this context. Articles 13(2)(f) and 14(2)(g) GDPR require controllers to:

- *Inform individuals of the existence of a fully automated decision-making process,*
- *Provide meaningful information about the logic involved, and*
- *Explain the significance and envisaged consequences of the processing.*

Algorithms and machine learning technologies used in automated decision-making are sometimes very complex. The WP29, however, expressly states that complexity is not an excuse for not providing information.

These guidelines provide some clarification on the type of information that needs to be provided. In essence, the information must relate to the rationale behind the decision-making process (e.g., what criteria are relied on to make the decision, what is the source of the information used, why these criteria are relevant for the decision, etc.), rather than complex and technical information about the algorithm itself (although this information may also be relevant in certain circumstances).

For instance, in the case of loan application based on credit score, the controller should explain what information is used to compile the score, where it comes from (e.g., loan application form, public registries, previous loan payment history, etc.) and why it is relevant in making the decision.

- ⇨ *Organizations should be able to explain what information is used to make the automated decision, what is the source of this information, how profiles are built, why they are relevant to the particular decision, and how it is used in the decision-making process.*

Conclusion

With the broad definition of profiling and the increase of automated decision-making based on machine learning and AI, a guidance from the WP29 in this matter was more than necessary.

These guidelines answer some of the questions that organizations engaging in this type of processing activity face, but certainly do not exhaust the debate.

The clarification provided on what "meaningful information about the logic involved" should entail, for instance, while valuable, may not appear sufficient for organisations engaged in more complex processing based on advanced machine learning technologies.

For instance, controllers may not be able to explain in a meaningful way what weight the algorithm puts on a specific criterion or how the balancing of various criteria actually takes place. Further guidance may be needed on this area.

The guidelines are also followed by Annexes, one of which contains a list of good practice recommendations about how to implement a profiling or automated decision-making process that is compliant with the GDPR principles.

The proposed guidelines are open for consultation until 28 November 2017.