GDPR Update: Profiling and Retail

April 19, 2018

Introduction

In this GDPR Update, we address the concept of profiling. In particular, we will focus on a number of aspects of the application of profiling in the retail sector.

Profiling and automated decision-making are used in an increasing number of sectors, both private and public, the retail sector being just one example.

Organizations apply automated decision-making (including profiling) inter alia for commercial purposes. Such purposes could include the retention of a profitable customer group, targeted marketing on the basis of predicted interests and the exclusion of certain customers with regard to certain services (for example loan requests).

Profiling and automated decision-making can impose significant risks on individuals regarding their rights and freedoms (in particular where the profiling includes processing of special or sensitive categories of personal data such as data related to health, ethnic origin or data subject's financial position). Risks include the creation of stereotypes, social segregation and inaccurate predictions. The GDPR contains provisions addressing such possible risks and protecting individuals against this type of personal data processing.

General profiling

The concept of profiling is not explicitly set out under the Directive 95/46/EG. The GDPR defines (general) 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 analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."

Put simply, profiling means gathering information about an individual (or group of individuals) and analyzing their individual characteristics or behavior patterns 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, their interests, or their likely behavior.

The GDPR distinguishes between 'general profiling' and, as we will call it in this GDPR Update, 'Article 22-profiling'.

Article 22-profiling

Article 22 GDPR provides that:

“Data subjects 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.”

Article 22 GDPR addresses decisions based solely on automated processing. This means decision-making by technological means without any human intervention. Although described as a right, this provision in fact regards a prohibition to undertake Article 22-profiling, unless one of the exceptions in the GDPR applies. These exceptions are:

a. The Article 22-profiling is necessary for entering into, or performance of, a contract between the data subject and the controller. Example: An organization receives a high volume of applications for a specific vacancy, from which it reasonably cannot select fitting candidates by hand. It may use automated decision-making for sifting out irrelevant applications and creating a short list of potential, suitable candidates;
b. The Article 22-profiling is authorized by EU 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 (for example, border security at the airport by the military police); or
c. It is based on data subject’s explicit consent.

In cases referred to under (a) – (c), the controller must implement suitable measures to safeguard the data subject’s rights and freedoms, and legitimate interests. According to the GDPR, such measures must include at least the right of the data subject to (i) obtain human intervention on the part of the controller, (ii) express his or her point of view, and (iii) contest the decision.

The general prohibition of Article 22-profiling, is not new and already set out in the Dutch Data Protection Act (article 42). The GDPR, however, introduces the exemption of ‘explicit consent’. Where the controller relies on explicit consent, it will have to make sure (and be able to demonstrate) that the data subjects understand exactly what they are consenting to.

Article 22 GDPR only prohibits automated decision-making if the decision-making produces legal effects concerning the data subject or similarly affects the data subject. The GDPR does not set out what legal effects or other serious consequences are. Generally, typical cases of targeted advertising are considered not to have significant effects on individuals. Examples of online advertising that could fall within the scope of Article 22 GDPR include differential pricing preventing individuals from purchasing certain goods.

Information obligation in case of automated decision-making

Articles 13 and 14 GDPR set out the controller’s information obligation . The articles require that, where applicable, the controller has to inform data subjects on the existence of automated decision-making, including, where applicable, Article 22-profiling. In addition, and at least in these Article 22-cases, the controller should provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The controller should find simple ways to inform the data subject on the rationale behind, or criteria relied on in reaching the decision. As the GDPR requires the controller to provide ‘meaningful information’ on the logic involved, complex mathematical explanations should be avoided. The use of realistic examples may make the significance and envisaged consequences of the processing easier to understand for data subjects.

Retail (customer journey)

Within the retail sector, the customer journey (i.e. mapping how a customer interacts with an organization during purchase and customer phase) becomes increasingly important. Organizations want to understand and predict their customers' behavior better, to be able to improve, among other things, targeted marketing and tailored offering of products, to increase sales. With the use of, for example, Wi-Fi-sensors within a store or shopping mall, it becomes possible to track the visitor's movements through—and shopping behavior in—the specific store or mall. The collected data allows retail stores and shopping malls to analyze visitors' movements and consumer shopping habits to improve store experiences and staff utilization.

To enable retailers to understand and predict customers' behavior more effectively and properly, large amounts of customer personal data are required. This is why customer tracking and profiling (e.g. through Wi-Fi tracking and Geo-location tracking) are becoming more important. Not only does the GDPR address customer journey, the draft e-Privacy Regulation sets out requirements as well. We expect the e-Privacy Regulation to replace the current e-Privacy Directive in the next one-two years. It is unfortunate that the e-Privacy Regulation does not apply from the same date as the GDPR, as this will create additional uncertainties for business in the coming period.

Legal basis

Under the GDPR, a controller requires a legal basis to be allowed to undertake profiling. The legal basis of legitimate interests (article 6(1)(f) GDPR) could be used for general profiling activities in the retail sector. Prior to processing on this basis, the controller must apply a balancing test, weighing its legitimate interests against data subjects' interests, fundamental rights and freedoms. The controller should take into account the following factors:

a. the level of detail of the profile;
b. the comprehensiveness of the profile;
c. the impact of the profiling; and
d. the safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process.

Where data subject's interests, fundamental rights and freedoms do not overrule controller's legitimate interests, this legal basis could be used for the profiling activities.

However, where profiling becomes more invasive (e.g. when detailed profiles are created or when the impact on the data subject is more significant), the controller will require the data subject's consent. Consent must be obtained prior to the processing and should be informed. The data subject must be able to make a free and informed decision. In practice, sufficiently informing data subject to obtain 'informed' consent is not straightforward. Furthermore, data subjects have the right to withdraw their consent at any time, which means that the controller no longer has a legal basis for the processing and will generally have to erase the data subject's personal data if he or she withdraws his or her consent.

Information obligations

Both the GDPR and the draft e-Privacy Regulation contain information obligations for the organizations using customer tracking systems. As set out above, controllers are obliged to inform data subjects about the processing of their personal data. When using tracking techniques such as Wi-Fi-tracking, it can be complicated to comply with these information obligations. Wi-Fi-sensors within shopping malls collecting MAC-addresses, do not distinguish between the MAC-address of a visitor of the mall or that of a person living in an apartment above the mall, an employee working in the mall or a passer-by. How to inform such persons on the existence of MAC-address sensors? The Dutch data protection authority suggests informing data subjects by means of attaching information signs to streetlights, or by marking sensor's range on the ground. In practice, however, such suggestions may often prove unachievable.

The draft e-Privacy Regulation also contains strict rules regarding information provision. Information must be displayed

in a clear and prominent way and must at least include information on the modalities of the processing, the purposes, the controller and other information as prescribed by the GDPR. Moreover, the information should also inform data subjects on how they can object to or minimalize the processing.

Retention periods

Personal data may be retained no longer than necessary for the purposes it was collected. Location data and other data allowing profiling may be retained for a short period only, unless the controller has obtained consent of the customer allowing it to retain the data for a longer period. However, as mentioned above, obtaining consent for processing activities in the context of customer journey mapping is not straightforward. To avoid complications, organizations could consider retaining the data in an anonymized or aggregated form, in such a way that the data does not qualify as personal data. In that case, the GDPR will not apply. For example: a controller may store information that 60 visitors entered the shopping mall via entrance A on Monday 13 August between 10 and 11 a.m.

Practical recommendations

It is common for organizations to collect as much data as possible. In practice, it is not always clear for what purposes the collected data is subsequently used. We regularly see that organizations collect data, but do not use (most of) that data. Such mass collection is not allowed under the GDPR, as personal data may only be collected for specified, explicit and legitimate purposes. Furthermore, untargeted mass collection of personal data introduces various privacy complications (in particular with regard to the information provision, balance of interests and retention periods).

In most cases, organizations will be looking for a targeted approach of individual customers (providing individual customers with personalized advertisements directed and customized at the interests of the individual). To this end, it may be a more efficient strategy to collect less but more insightful data. A retailer could, for example, limit the data collection to individuals who have actively opted-in for such processing, for instance by signing up as a member of that retailer's loyalty program. The individuals who actively signed-up for those programs are already interested in the advantages of loyalty schemes. Such individuals will receive tailored promotions, and, in return, they provide the retailer with valuable insights.

Please click here to subscribe to our monthly updates on the GDPR.

Overview of subjects

January 2017	Territorial scope of the GDPR(Dutch)
February 2017	The Concept of Consent
March 2017	Sensitive Data
April 2017	Accountability, Privacy by Design and Privacy by Default
May 2017	Rights of Data Subjects (information notices)
June 2017	Rights of Data Subjects (access, rectification and portability)
July2017	Rights of Data Subjects (erasure, restriction, objectand automated individual decision-making)
August 2017	Data Processors
September 2017	Data Breaches and Notifications

October 2017	Data Protection Officers
November 2017	Transfer of Personal Data (outside the EEA)
December 2017	Regulators (competence, tasks and powers)
January 2018	One Stop Shop
February 2018	Sanctions
March 2018	Processing of Personal Data in the Employment Context
April 2018	Profiling and Retail
May 2018	Overview

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com

Celine van Es
Associate, Amsterdam
D +31 20 795 31 22
M +31 6 11 16 30 45
celine.vanes@dentons.com