SLAUGHTER AND MAY

Tracking, watching, predicting… lawfully: responsible profiling under the GDPR

September 2017

This article explores the impact of the new EU General Data Protection Regulation[1] (GDPR) on customer profiling. We focus on the retail sector, where the volume of data that retailers can access about their customers' preferences and the sophistication of the algorithms that are used to process that data continue to grow, allowing retailers to offer their customers a highly personalised shopping experience. We consider what sort of activities amount to profiling, the circumstances in which businesses will be able to profile their customers post GDPR, whether businesses must offer customers the choice not to be profiled and what businesses must tell customers about any profiling they undertake.

What do we mean by profiling?

Profiling covers a wide range of activity from online retailers using information on the shopping habits of their customers to suggest items that they may be interested in purchasing (for example, Netflix uses personal data to recommend films and TV programmes that it thinks customers are likely to enjoy) to automated decision-making, such as insurers tracking customer behaviour to predict the risks of claims when setting premiums (the insurer Admiral, for example, had proposed to use information on Facebook to identify personality traits linked to safe driving before the project was pulled following a backlash).[2]

The current EU Data Protection Directive already places restrictions on the automated processing. However, advances in technology mean that there has been a dramatic increase in automated profiling in the 20 years since the Directive was adopted. In many sectors, profiling is now an ordinary part of daily business.

In the retail sector, profiling is essentially a way for retailers to get to know their customers better and personalise their services so that customers only receive content that is relevant to them.

The definition of profiling in the GDPR covers this type of profiling:

"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

[1] Regulation (EU) 2016/679 of 27 April 2016.

[2] See https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts and https://www.theguardian.com/money/2016/nov/02/facebook-admiral-car-insurance-privacy-data

performance at work, economic situation, health, personal preferences, interests, reliability, behaviour location or movements".[3]

As such, profiling is widespread in the online retail sector. Many online retailers will need to review what they are doing under the GDPR.

Will online retailers be able to continue to profile in this way post GDPR?

Stricter rules where profiling has legal or similarly significant effects

The GDPR places significant restrictions on profiling where this has "*legal effects*" for individuals or "*similarly significantly*" affects them.[4]

Does the sort of profiling carried out by online retailers have legal or similarly significant effects? It is unlikely in most scenarios to have a legal effect. It arguably also does not "*similarly significantly*" affect individuals. This is quite a high threshold. While some individuals may find profiling intrusive or irritating, this is not equivalent to profiling that has legal consequences for individuals.

The examples given in the GDPR of profiling that similarly significantly affects individuals are of a very different character. They include, for example, automatically refusing an online credit application or e-recruiting practices without any

Profiling that has legal or similarly significant effects – key protection provisions:

1) An individual has the right not to be subject to a decision based solely on automated processing (including profiling) which produces legal effects, or similarly significantly affects him/her, unless the decision is:

a) necessary for the performance of a contract between the individual and the business;

b) authorised by EU or Member State law; or

c) based on the individual's explicit consent.

2) Where a business is relying on (a) or (c), above as its basis for lawful processing, it must implement suitable measures to safeguard the individual's rights and freedoms and legitimate interests. These must as a minimum include the right to obtain human intervention, to express his or her point of view and to contest the decision. Further detail on the suitable measures is set out in Recital 71.

[3] Article 4(4).

[4] Article 22(1).

human intervention.[5] These have clear tangible effects on individuals.

ICO lowers threshold?

Earlier in 2017, the Information Commissioner's Office (ICO) sought feedback from stakeholders on what might amount to a legal or significant effect, in its paper on profiling and automated decision-making. [6]

The ICO has suggested that the threshold may be quite low. Its paper gives a list of different types of processing that may have significant effects, a number of which could well apply to online retailers. They include profiling that "*causes damage, loss or distress to individuals*", has "*unlikely, unanticipated or unwanted consequences for individuals*" or "*leaves individuals open to discrimination or unfair treatment*."

These are broad and subjective. For example, is profiling unwanted if a personalised offer tempts a customer to buy chocolate they are trying to resist because they have just started a diet? Is it unfair that a discount for a toy is displayed to one customer but not another because the first customer bought a similar toy the week before? Are these consequences really *similarly significant* to legal effects?

The ICO challenges the perception that advertising (and related profiling) does not generally have a significant adverse effect on people. It gives the example of a person who receives advertisements for diet products and gym membership based on their online behaviour. While this might spur them to join an exercise class and improve their fitness levels, it may also make them feel that they are unhealthy or need to lose weight which could lead to feelings of low esteem.

Risk of over-caution

However, our view is that data protection regulators need to be very careful not to draw the net too widely. The better approach is that only in exceptional circumstances should profiling by online retailers be treated as having effects that are similar to legal effects. These exceptional circumstances might include making questionable inferences about someone's behaviour or preferences to send material that could, on an objective basis, cause offence or distress. For example, using someone's purchase of a pregnancy test to target them with material on safe sex or abortions through the post might legitimately be caught.

In deciding what might cause offence or distress (or other significant effects), the standard should be that of a reasonable person. Otherwise we risk over-caution and stifling profiling that most people would see as helpful. It is therefore reassuring that the ICO acknowledges that it may be useful to establish an external recognised

[5] Recital 71.

[6] ICO, Feedback request – profiling and automated decision-making, dated 6 April 2017.

standard to measure effects, instead of simply relying on the subjective view of the business or the individual.[7]

Neutral starting point

The starting position on profiling by retailers should be a neutral one. As the Direct Marketing Association has noted, profiling customers should not be seen as *inherently* bad.[8] Indeed, profiling can offer significant benefits for both customers and businesses: customers get information that is likely to be of interest to them and are not bombarded with information that is not; this in turn makes it more likely that they will buy something from the retailer. According to DMA customer engagement research, 63% of customers are interested in receiving offers tailored to what they had bought after a purchase.[9]

Retailers will need to consider carefully how profiling is done and in practice are likely to need to carry out a Data Protection Impact Assessment.[10] Nevertheless, the starting point should be neutral.

Future guidance

The Article 29 Working Party (an independent advisory body made up of representatives of the national data protection authorities, the European Commission and the European Data Protection Supervisor) intends to publish guidelines on profiling by December 2017. These will provide an important insight into the approach regulators will take. Although the ICO has stressed that the views expressed in its feedback paper represent its initial thoughts on issues which require further debate, it is the lead national authority in drafting the Article 29 Working Party guidance and so its initial views are likely to be influential.

Additional requirements for profiling with legal or similarly significant effects

In circumstances where profiling does have legal or similarly significant effects, as is likely to be the case, for example, where the premium quoted by an online insurer and the coverage offered is based on profiling, the additional requirements in the GDPR will need to be satisfied.[11] The key requirements are summarised in the box on page 2.

What legal grounds will online retailers be able to rely on for processing?

As with any processing by an organisation, businesses that profile their customers will need

[7] ICO, Feedback request – profiling and automated decision-making, dated 6 April 2017.

[8] See DMA Response to the ICO's Feedback request – profiling and automated decision-making, dated 6 April 2017.

[9] See DMA Response to the ICO's Feedback request – profiling and automated decision-making, dated 6 April 2017.

[10] See Article 35 which sets out the circumstances in which a data protection impact assessment is required.

[11] See in particular Article 22 and Recitals 71, 72.

to satisfy one of the grounds for the lawful processing of data under the GDPR to carry out that profiling (even where the profiling does not have legal or similarly significant effects).[12] These legal grounds are summarised in the box on page 6.

Which of these grounds for processing is most likely to be relied on by online retailers to profile their customers?

- **Consent:** Consent is a possibility, and has the advantage that – if explicit – it can also be relied upon to carry out profiling that has legal effects or similarly significant effects.[13] We are aware, for example, of insurance companies that intend to rely on consent to profile customers.

  However, some online businesses may find it challenging to demonstrate that consent is specific, informed, free and unambiguous in all cases. Consent can also be withdrawn so any retailer relying on consent will need a process to stop profiling customers that withdraw their consent. For a summary of the GDPR's rules on consent, see our article Processing of personal data: consent and legitimate interests under the GDPR.

- **Necessary to perform contract:** We would generally expect it to be challenging for a retailer to show that they could not have fulfilled the contract (i.e. sold goods or services to the customer) without profiling their customer. That said, there may be circumstances where it is possible to argue that profiling customers is so integral to the type of service supplied by an online retailer that profiling is necessary to perform the contract. This might be the case, for example, where the main feature of the service provided by an online retailer is the high level of personalisation.

- **Legitimate interests:** Online retailers should be able to rely on this ground. The Article 29 Working Party recognises that retailers have a legitimate interest in getting to know their customers' preferences and marketing to them.[14] Online retailers will need to balance on the one hand their own interests in profiling and personalising offers to customers, and on the other the potential negative consequences for customers resulting from the intrusion into their privacy.

[12] Article 6(1).

[13] Article 22(1), 22(2)(c).

[14] 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. See pages 25 and 26.

The reasonable expectations of customers will be important here.

Mitigating steps may also help to tip the balance. For example, retailers might consider putting in place measures to prevent historic searches or purchases of potentially more sensitive items (such as contraception) being used in profiling, offering an opt-out for customers that do not want to be profiled and/or seeking regular feedback from customers to understand what impact (positive or negative) profiling is having and considering whether any adjustments should be made to the way customers are profiled in light of that feedback.

The other 3 grounds for lawful processing are less likely to be relevant to profiling by online retailers.

Do online retailers need to worry about sensitive personal data?

Most profiling of customers by online retailers is unlikely to require the use of any sensitive personal data (referred to as "special categories of personal data under the GDPR"). Clearly to the extent that online retailers do use special categories of data to profile customers they will need to satisfy the stricter requirements for the processing of such data.[15]

Online retailers will also need to be careful to avoid inadvertently transforming data that is not a special category of data into data that is. Data analytics algorithms used to perform the profiling should be designed in a way that avoids, for example, shopping preferences being used to categorise customers by political belief, health or disability, or religion.

Summary of grounds for lawful processing of personal data under the GDPR

1. Individual has consented
2. Necessary to perform contract with individual
3. Necessary to comply with a legal obligation
4. Necessary to protect vital interests of a person
5. Necessary to perform public interest task or in exercise of official authority
6. Necessary for the purposes of the legitimate interests of the business or a third party

Must customers have the right to opt out of profiling?

Qualified right to opt out where retailer is relying on its legitimate interests

[15] See Article 9.

If the online retailer is relying on the 'necessary for legitimate interests' grounds as a basis for lawful processing, then customers must be given the right to object.[16]

However, this right is qualified. If a retailer can demonstrate compelling legitimate interests that override the interests and rights of the individual, the retailer will be able to continue to profile. This will involve a balancing act having regard to the individual's particular situation and any specific concerns raised by the individual when they object to the profiling.[17] Retailers will similarly want to consider the reputational impact of refusing someone's objection.

Absolute right to opt out of direct marketing

In addition, individuals also have the right to object to their data being processed for direct marketing (including any related profiling).[18] If a customer objects, the profiling and direct marketing must stop.[19]

Boundary between direct marketing and online selling

The Directive already includes a right to object to the processing of personal data for direct marketing.[20] However, there have been significant technological changes since 1995 (when that Directive came into force) in particular with the way retailers achieve online marketing and communications with customers. There are therefore likely to be difficult questions about the exact boundary between what is direct marketing online and what is part of an online retail service following the introduction of the GDPR.

There is no definition of direct marketing in the GDPR and, as yet, no guidance on what the term means. Direct marketing is defined in the Data Protection Act 1998 (the "DPA") as:

"the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals."[21]

The ICO has emphasised that this definition covers any advertising or marketing material however communicated including both traditional forms of marketing (e.g. telesales or mailshots), as well as online marketing, social networking and other emerging channels of communication. The

[16] Article 21(1).

[17] See 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, at page 45.

[18] Article 21(2).

[19] Article 21(3).

[20] Article 14(b) Directive 95/46/EC.

[21] Section 11(3).

key is whether the material is *directed* at an individual.[22]

It is clear then that customers must have the right to object to profiling that leads to marketing emails, texts and messages on social media (e.g. Facebook). This is unlikely to be controversial.

However, must customers also be able to opt out of personalised offers or recommendations that appear when they are logged into their account with the online retailer and are adding items to their shopping basket? Is this direct marketing, or is it simply part of the customer's online shopping experience? This is an area where online retailers are likely to welcome clarity from the regulators.

Future guidance

The Digital Economy Act 2017 requires the ICO to prepare a statutory code of practice on direct marketing.[23] This must include guidance on how to comply with the DPA and the Privacy and Electronic Communications (EC Directive) Regulations 2003, and may also include guidance on good practice. It is possible that the code will address profiling in the context of direct marketing. The ICO is required to put the guidance out to consultation so this will be a good opportunity for organisations to share their views on what the relevant rules require and what constitutes good practice. Retailers should also take this opportunity to provide the ICO with knowledge and insight into how the industry uses profiling.

Options for retailers

If regulators decide to adopt a broad definition of direct marketing in the guidance, online retailers and other service providers will need to make the difficult decision whether to provide alternative versions of their services (one using and offering profiling and one without it), or whether to make access to their services conditional on being able to profile users.

What will customers need to be told about profiling?

Transparency is a key principle of the GDPR. It will therefore be important that customers understand that they are being profiled and what this means for them in practice.

What information needs to be provided to customers will depend on the type of profiling being carried out. The box on page 9 sets out some of the key requirements in the GDPR that businesses will need to bear in mind. In practice there is likely to be a tension between the obligation to provide information at a sufficient level of detail to satisfy the granular requirements in the GDPR and the obligation to

[22] ICO's Guidance on Direct marketing (Data Protection Act Privacy and Electronic Communications Regulations). See paragraphs 36 and 37.

[23] Section 96 of the Digital Economy Act 2017.

present information in a clear, concise and intelligible form.

In the profiling context, concerns have also been expressed by some about the requirement to disclose information on the "logic" involved in automated decision making and whether this could mean the "logic" employed by algorithms, given that this will often be highly commercially sensitive. However, it is unlikely to be necessary (or indeed helpful to customers) to disclose this sort of detail about an algorithm.

The ICO has suggested that rather than providing a technical description of how an algorithm works, controllers should consider clarifying the categories of data used to create a profile, the source of the data and why the data is considered relevant.[24] Recital 63 of the GDPR which provides that data access rights should not adversely affect the freedoms of others, including trade secrets or intellectual property, should also provide some comfort.

Achieving the right balance

While the data protection rules are designed to protect individuals, they should not be applied in a manner that stifles good business innovation. It should be possible to balance the two. Indeed, the Information Commissioner Elizabeth Denham has stated:

Keeping individuals informed – key GDPR provisions

The GDPR requires businesses to provide information:

- on the purposes of and legal basis for processing (Article 13(1)(c));
- on the legitimate interests they are pursuing, if they are relying on legitimate interests as the legal basis for processing (Article 13(1)(d));
- about solely automated decision making (including profiling) that has legal or similarly significant effects, as well as meaningful information about the logic involved and significance and envisaged consequences of processing (Article 13(2)(f)); and
- on the right of individuals to object to processing where applicable (Article 13(2)(b) and Article 21(4)).

This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 12).

[24] ICO, Feedback request – profiling and automated decision-making, dated 6 April 2017 at page 15.

"I do not believe data protection law is standing in the way of your success. It's not privacy or innovation - it's privacy and innovation. The personal information economy can be a win win situation for everyone. Get it right, and consumers and business benefits."

The new rules on profiling should not be treated as an exception to this. The GDPR gives individuals important rights that will ensure that they know when they are being profiled and what this means for them and are not subject to intrusive monitoring of their online behaviour without justification. It will require retailers to put in place appropriate safeguards to ensure responsible profiling. It will be equally important that these rules are not interpreted in a way that blocks the ability of businesses to innovate and benefit customers.

This article was written by Rob Sumroy and Rebecca Cousin. Slaughter and May advises on all aspects of data protection and privacy, including GDPR compliance audits. If you would like further information, please contact Rob, Rebecca or your usual Slaughter and May advisor. Further publications are available on our website.

Rob Sumroy
T +44 (0)207 090 4032
E rob.sumroy@slaughterandmay.com

Rebecca Cousin
T +44 (0)207 090 3049
E rebecca.cousin@slaughterandmay.com