GDPR for marketers: Profiling

Responsible Marketing

DMA
Data & Marketing Association

Contents

Welcome to GDPR Guidance for marketers

May 25 2018 saw the new regulatory framework take effect – and it offers all of us the greatest opportunity for business transformation in a generation.

The General Data Protection Regulation (GDPR) mirrors the DMA's long-held view about the need to place the customer at the heart of everything we do. It also echoes our commitment to a code that enshrines five key principles that marketers should follow:

- Put your customer first
- Respect privacy and meet your customers' expectations
- Be honest, be fair, be transparent
- Exercise diligence with data
- Take responsibility, be accountable.

The DMA - supported by the Advertising Association in London and FEDMA in Europe - has actively influenced the evolution of the GDPR text since first drafts were circulated by the European Commission in 2011.

We have worked closely with our partners in government and across the wider marketing community throughout the drafting process.

Our advocacy has established vital building blocks within the GDPR that will safeguard the interests of our members and marketing professionals throughout the UK.

To support business transition to this new data landscape, we have crafted a guidance series that examines the GDPR through a marketer's lens.

This guide, which covers profiling under the GDPR, is one of several providing marketers with a framework for innovation and growth. Other guides take an in-depth look at Accountability, Legitimate Interests, Consent and Essentials.

We believe that organisations must use GDPR as a catalyst for transforming approaches, balancing privacy with innovation.

This DMA series will help you apply broad best practice principles to your marketing and your customer service approaches. The guidance uses live examples and practical tools, linking to new, channel-specific marketing information and insight from around the DMA's member community.

But let's be clear: Article 29 Working Party and ICO guidance are general across sectors. There is no established case law, so all advice will evolve as real-world applications emerge.

From the C-suite to all tiers of business, we must work together to create customer-centric business environments. Brands that make data protection a core value will blossom.

Finally, this guidance has been drafted with the collaboration of ISBA, DPN and the ICO, which have all made valuable contributions.

These partnerships inform our case studies and guidance with expert insights, and establish a consistent position on GDPR across the marketing industry.

Chris Combemale
CEO, DMA Group

Foreword by the Information Commissioner

This is a pivotal time for data protection and privacy.

We have a digital infrastructure that was unimaginable 20 years ago and data protection laws are converging across the globe. Consumer trust is ever more central to both business and the public sector, and a rapidly expanding digital economy is asking more questions of us all.

For me, the end game in the data protection field is always about increasing public trust and confidence in how their personal data is used.

Data protection reforms, including the GDPR, build on previous legislation, and provide more protections for consumers, and more privacy considerations for organisations. But this is a step-change. It's evolution, not revolution.

It's vital that organisations are prepared to comply but they can also prosper in the new regulatory landscape.

If your organisation can demonstrate that good data protection is a cornerstone of your business policy and practices, you'll see a real business benefit.

An upfront investment in privacy fundamentals offers a payoff down the line, not just in better legal compliance, but a competitive edge. I believe there is a real opportunity for organisations to present themselves on the basis of how they understand and respect the privacy of individuals.

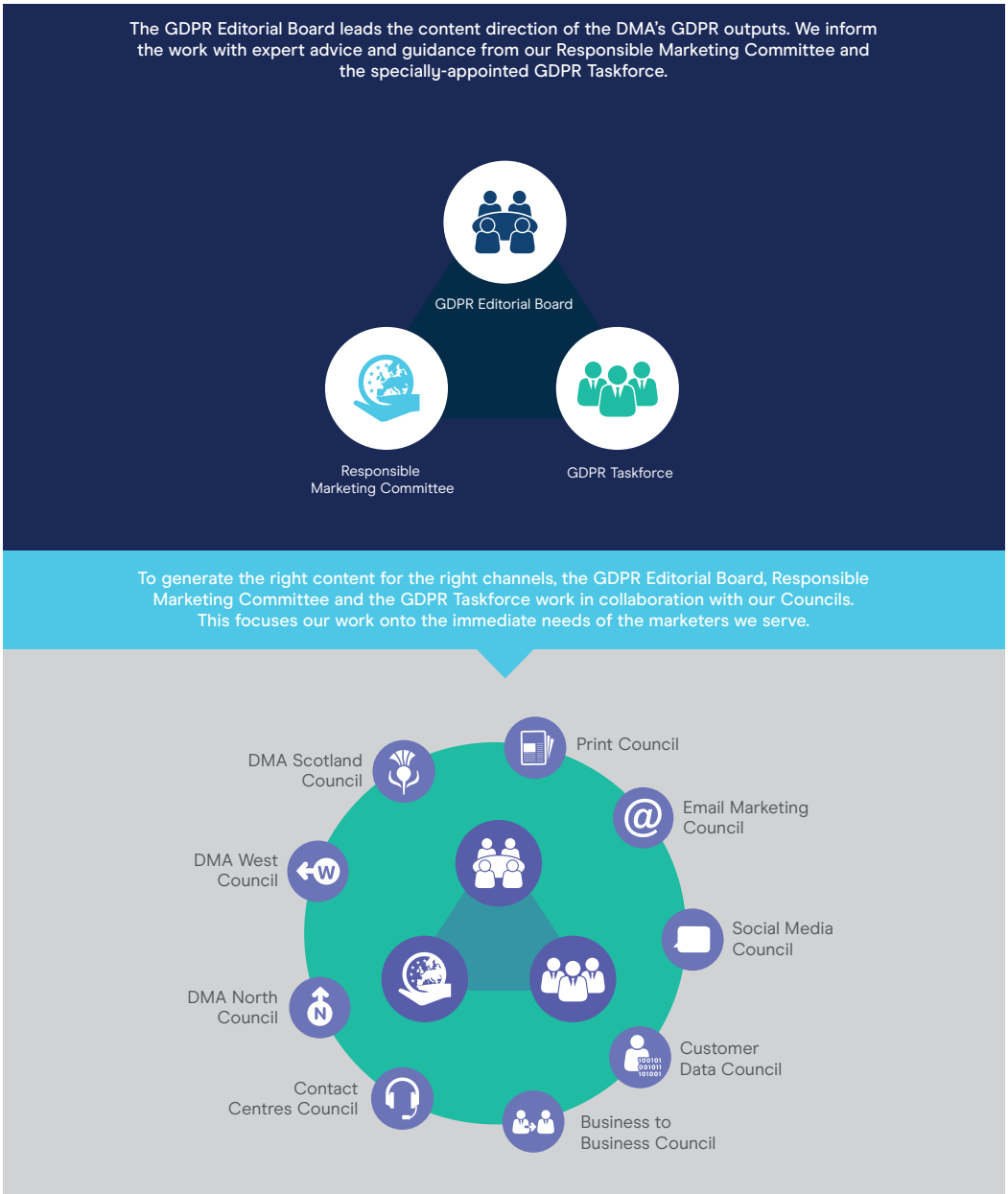
This helpful guidance has been drafted by the DMA with its members, members of ISBA and the Data Protection Network with input from the ICO. It will help marketers navigate through the GDPR and complements our own GDPR guidance and additional online checklists and resources.

I hope this guidance helps you be transparent, accountable and ensure people have appropriate control over their personal data.

Elizabeth Denham
Information Commissioner

The DMA and the GDPR

How we create GDPR guidance



Throughout our approach to preparing the industry for the GDPR, we work with the ICO and partner with:

Our GDPR guidance focuses on the key marketing impacts that May 2018 will bring

GDPR for marketers

- The essentials
- Accountability
- Consent & Legitimate Interests
- Profiling
- ePrivacy
- Information rights

Governed by the GDPR Editorial Board, the Responsible Marketing Committee and the GDPR Taskforce, the DMA's Councils and Committees produce

DMA GDPR advice for marketers

- Permission by design
- Checklist for trustees
- B2B mythbuster
- Cloud computing
- Action planning
- Data governance

All of which we underpin with our events and research calendar, online tools and channel-specific advice and guidance


DMA Events


DMA Research


DMA Insight


DMA Webinars


DMA Guides

Introduction

Profiling

Profiling enables the analysis, determination and prediction of certain aspects of an individual's personality or behaviour, interests and habits.

It is evident in many areas of life, taking the form of consumer, user, social or movement profiles. It is a requirement of GDPR to make individuals aware of any profiling you're carrying out, including for the purpose of sending direct marketing.

Sources of data used to build a picture of an individual include, but are not limited to, data from:

- internet search and browsing history
- existing customer relationships and buying habits
- credit cards, store cards and other transactions
- credit scoring
- consumer complaints or enquiries
- location and lifestyle habits (often gathered from mobile phones)
- social media
- driving (telematics)
- property ownership
- biometric systems
- the Internet of Things
- household
- address
- family information
- device ID

Here's an example of profiling conducted for marketing purposes:

An airline studies the behaviour of its online customers. It examines what they search for, look at and how much time they spend considering each destination. This data will be combined with the location and route the customer is most likely to use based on their previous flight history. The profile will then be used to serve the customer with a marketing communication that highlights the destination and route they're most likely to be interested in.

A new era for profiling

By creating profiles of similar people, marketers can accurately target the right individuals with offers they may be interested in. This also helps to reduce waste, with communications sent to consumers who might be genuinely keen to buy a product or service.

In modern marketing, however, profiling is no longer just a matter of segmentation - the practice of grouping people with similar characteristics or interests; for example, gender, age, business type and hobbies.

In the digital era, more sophisticated techniques are employed and they use a wide variety of technology. Nowadays, profiling for marketing often involves further data analysis to build a picture of the individual and deliver targeted, relevant communications and experiences. Additional information, which varies between organisations depending on the task at hand, is collated. Sources for this activity can include recent purchases, externally sourced data, geodemographic data and other useful information.

Profiling remains the bread and butter of marketing activity; it is used to define frequency and content of communications, giving consumers a positive and valuable experience.

Profiling is specifically addressed in the GDPR, which brings new obligations for data controllers to consider.

How the GDPR defines profiling

Profiling is specifically addressed in the GDPR, which brings new obligations for data controllers to consider. The text of the regulation refers to 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."

While this is not too dissimilar in meaning to the generally agreed marketing industry parameters set out in the previous section, the GDPR further breaks down the different types of profiling activity that can be performed.

The Article 29 Working Party – the group that represent the EU's various data protection authorities – has identified three main types of profiling:

- General profiling
- Decision-making based on profiling
- Solely automated decision-making, including profiling.

Automated decision-making differs in scope to general profiling, yet also overlaps with it.

Automation is the ability to make a decision without the opinion or consideration of a person. For example, an algorithm that calculates valuable customers and enables marketing to be sent to them automatically.

Because no human oversight is involved, this type of marketing is classified as automated decision-making. Automated decisions can be taken with or without profiling, and profiling can take place without making automated decisions.

Meanwhile, Article 22 of the GDPR introduces additional rules to protect individuals. It states: "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."There are several caveats where this would not apply, which we'll explore later.

The Information Commissioner's Office (ICO) has previously referred to profiling under GDPR as a key "area of concern"for its stakeholders. As we'll see below, the new regulations have a number of requirements to consider for organisations looking to build better profiles of their customers for marketing purposes.

Profiling in practice under the GDPR

The ICO has offered the following comprehensive summary about the changes that marketing professionals will face following GDPR's implementation: "The [1995 Data Protection] Directive focused on the outcome of automated decision-making (which could include profiling), rather than the act of profiling itself. The GDPR applies to profile creation as well as to automatic decision-making using profiling.

"In addition... GDPR introduces other new rights for data subjects and obligations for controllers. These extra elements provide for greater transparency and more individual control when profiling is being carried out on personal data, such as additional information requirements and greater accountability."

To fall under the definition in the GDPR, all of the following factors must apply:

- The processing must be automated. Profiling or decision-making by a human is not covered by the extra obligations placed upon automated profiling but is subject to the other obligations in GDPR
- Profiling must involve personal data. The use of non-personal data to make an automated decision is not covered. For example, this would include analysing the number of households in a specific geographical area by reference to roads and house numbers. However, if an organisation holds other personal data about the people that live in that catchment area, then house numbers or road names could become personal data. This is because they could be used to identify someone
- Profiling must be used to evaluate certain personal aspects relating to an individual. These aspects might include income, family composition or payment history of an identifiable individual.

The DMA and other groups lobbied extensively during drafting of the GDPR and during the implementation period to ensure that most profiling for marketing purposes was not considered to have a legal or significant impact.

However, in certain contexts profiling for marketing purposes can have a legal or significant effect (explored overleaf). This is important for marketers as profiling with a legal or significant impact requires consent, while profiling that does not meet the above criteria can be carried out under legitimate interests.

Individuals have the right to object to profiling, and specifically profiling for marketing purposes, under Article 21. Meanwhile, there are additional restrictions on using special category and children's personal data. ICO draft guidance on the latter can be found here: https://ico.org.uk/media/about-the-ico/ consultations/2172913/children- and-the-gdpr-consultation-guidance-20171221.pdf

Automation

The 1995 Directive's provisions on automated decision-making were also reflected in Section 12 of the 1998 UK Data Protection Act (DPA). At that time, purely automated decisions that didn't involve any human intervention were unusual.

The situation today is very different thanks to the advent of the internet and all the data it brings, as well as widespread adoption of technology and great advances in big data analytics.

These innovations have changed the face of profiling for marketing activities, and this is consequently reflected in the GDPR.

As we've seen, GDPR applies to all automated individual decision-making and profiling. Automated decision-making that produces a legal or similarly significant effect is prohibited, unless it is done with an individual's explicit consent. This processing is prohibited apart from in three specific instances, contained in Article 22, when it's:

- necessary for the entry into or performance of a contract
- authorised by Union or Member State law applicable to the data controller
- based on the individual's explicit consent. This would need to be separate to consent for marketing.

These three grounds work in a similar way to individuals' existing rights under the DPA 1998.

Even when any or all three of these grounds apply, organisations must ensure individuals are informed about the data processing taking place, and also make it easy for them to request human intervention and to challenge a decision if they wish.

Furthermore, GDPR states organisations and any partners acting on their behalf must conduct regular checks to make sure systems are working as intended, correct errors and minimise bias or discrimination. They're also required to use appropriate mathematical or statistical procedures to safeguard individuals' rights and freedoms.

All of these requirements may involve implementation of the following systems:

- Measures to identify and resolve personal data inaccuracies
- Risk-appropriate security to protect the interests and rights of the data subject
- Prevention of discriminatory effects on individuals on the basis of special categories of personal data
- Provisions for data minimisation and clear retention periods for profiles
- Techniques to pseudonymise data in profiling activities
- Human intervention processes.

Finally, data controllers are also required to provide fair processing information about solely automated decision- making. They must tell people:

- Meaningful information about the logic involved
- The significance and envisaged consequences of the processing
- Sufficient information to make processing fair.

However, according to Recital 63 of GDPR, they are not required to divulge trade secrets or intellectual property.

Significant effect

Many organisations think marketing doesn't generally have a significant adverse effect on people. However, this isn't always the case, as profiling activity could lead to unfair discrimination.

For example, someone is in severe debt, which is causing distress in their daily life. This person's preferences while browsing online could lead to them being served ads for high-interest loans. This could be considered a significant effect.

This is because the indebted person is likely to sign up to the high-interest loan, which would have a severely negative impact on their personal life.

In many typical marketing examples a situation like the above would not arise and the profiling would not be deemed to produce a legal or similarly significant impact.

According to Article 22 (1), individuals have the right not to be subject to a decision based solely on automated decision-making - including profiling - which produces legal effects concerning the individual or "significantly affects"them. This is in effect a prohibition in the GDPR. As indicated above, this could apply in relation to processing for advertising or marketing, for example, where the individual is vulnerable or where the profiling is particularly intrusive.

Unfair profiling

Unfair profiling happens when profiling is deemed to discriminate against certain people; for example, resulting in them being offered costly or risky deals. It is an example of a significant effect.

This problem doesn't apply to all products or services, but industries including human resources or recruitment, insurance and credit sectors are vulnerable.

The example in the 'significant effect' section above is a case of unfair profiling.

In another example, an organisation is looking to fill a new role. They implement a job application process, which uses automated profiling. An individual then has their job application refused on the basis of a decision made following automated profiling. This would be deemed unfair on the individual under the GDPR.

Transparency in profiling

Organisations acting as the data controller, and agencies that carry out profiling on their behalf, must ensure all activity meets the core requirements of the GDPR.

Furthermore, organisations will have to provide consumers with clear and transparent guidance on what profiling activities are taking place, and for what purpose.

The controller should provide this information - sufficient to make the processing of their personal data fair - at the time the data is first collected from data subjects or within a reasonable period after collecting an individual's personal data, but always within one month.

In most cases, this information will be provided using a clear link to a privacy statement but an organisation could provide this information upfront in a pop-up, for example.

More importantly, the privacy statement must be written in easy-to-understand language and inform individuals about how their personal data will be used. For instance, you should avoid the word the "profiling"because it may scare people by conjuring up negative images, such as racial profiling. Instead, explain how personalisation improves the service and, crucially, how the individual benefits.

Marketing agencies processing consumer data for controllers must also be able to prove that the activity being carried out matches what is communicated to the consumer.

Compliance will necessitate organisations and their partners working in greater harmony than ever before.

Data retention

The GDPR does not set a specific retention period for profiles. As they tend to be dynamic and evolve over time, a regular review of the information organisations collect should be conducted to ensure profiles remain fit for purpose. Article 5 requires organisations to ensure that personal data they hold is accurate and up to date and that every reasonable step should be taken to maintain the accuracy of the data. This principle applies to customer profiles, so organisations need to set out processes that will keep profiles relevant and accurate.

Embedding a privacy-by-design approach, which we explore further in our Accountability Guidance, can aid compliance with these provisions and simultaneously enhance privacy awareness across an organisation.

Link to the Accountability Guidance: https://dma.org.uk/uploads/misc/5aabd8918b47e-gdpr- accountability_5aabd8918b3cb.pdf

New data

Profiling also creates new data that must be managed in a compliant way under GDPR in its own right. As profiling can take information from a variety of sources to create derived or inferred data, issues are raised about operating effective, timely and fair processing, and how to understand what individuals might reasonably expect.

This new data is also personal data because it relates to and could identify a living individual. Therefore, it must be given appropriate safeguards and people must be informed about how you may use this information. This should be clearly explained in your privacy policy.

Profiling and legitimate interests

Organisations will need a lawful basis in order to profile and segment personal data for marketing purposes under the GDPR. Profiling can potentially be carried out using legitimate interests as a lawful basis.

The Article 29 Working Party's draft guidance on profiling references Recital 47, which enables processing of data for the legitimate interests of an organisation.

However, in order to use this lawful basis, an organisation must conduct a robust Legitimate Interests Assessment (LIA), and only undertake the profiling if the LIA shows that the rights and freedoms of individuals won't be overridden by the proposed processing.

Details on how to carry out LIAs are contained in our Consent and Legitimate Interests guidance: https://dma.org.uk/uploads/ misc/5ae1fbf5c60fd-gdpr-for-marketers---consent-and-legitimate- interest_5ae1fbf5c6066.pdf and on the ICO's website: https://ico.org.uk/for-organisations/guide-to-the-general-data- protection-regulation-gdpr/legitimate- interests/

Example

A department store asks for consent to send electronic marketing to customers when they make a purchase in-store or online. The company only sends marketing communications to people who have given their opt-in consent.

The retailer also collects personal data about people when they complete forms in-store or when they visit its website. The department store processes personal data about its customers, so it can better understand the type of people who buy things from it, and their interests.

This type of profiling and data analytics is done under the banner of legitimate interests. However, there must always be a balance between the interests of an organisation in profiling and personalising offers to customers, and their reasonable expectations. Consider, therefore, the potential negative consequences of intruding on people's privacy.

Mitigating steps can be taken.

For example, retailers might consider implementing measures to prevent historic searches, or information about purchases of items of a sensitive nature, being used for profiling.

Additionally, they could offer an opt-out for customers who do not want to be profiled, and seek regular feedback from shoppers to understand what positive or negative impact profiling is having on them.

Adjustments should then be made accordingly.

Profiling and consent

The more extensive or intrusive profiling for direct marketing is, the more it is likely to infringe an individual's rights. If that is the case, legitimate interests cannot be used as a lawful basis.

For example, profiling may infer a person's racial or sexual status and would then be considered as processing special category data (previously referred to under the DPA 1998 as sensitive personal data). If this happened, explicit consent would be required from the person before the profiling could take place.

Consent is a possible lawful basis for profiling. If consent is explicit for profiling, it can also be relied on to carry out profiling that has legal or similarly significant effects.

Explicit consent is not required if the profiling does not have a legal or similarly significant impact, which most profiling for marketing purposes lacks, although as we've seen, there are exceptions. The ICO has issued guidance about when it will be necessary to undertake a Data Protection Impact Assessment (DPIA), which includes automated decision-making that that has a legal or similarly significant effect, and for large-scale profiling. More information is available here: https://ico.org.uk/for-organisations/guide-to- the-general-data-protection-regulation-gdpr/data- protection-impact-assessments-dpias/examples-of-processing- likely-to-result-in-high-risk/.

However, some businesses that operate online may find it difficult to show that someone's consent is specific, informed, freely given and unambiguous in all cases, in order to allow profiling.

Consent can also be withdrawn by individuals at any time, so any organisation relying on it as a lawful basis must implement a process to immediately stop profiling customers if they withdraw their consent.

More information can be found in the DMA's Guidance on Consent and Legitimate Interests: https://dma.org.uk/uploads/misc/5ae1fbf5c60fd-gdpr-for-marketers---consent-and-legitimate- interest_5ae1fbf5c6066.pdf

Using third parties for profiling

Organisations profile their own customers using personal data that has been collected from them. However, marketers want to build as comprehensive a view as possible of these individuals, so they often appoint third parties to provide additional information.

Providers can enrich organisations' existing data sets with third-party data collected from various sources. Using this information, marketers can gain a better understanding of their customers and communicate with them more efficiently and effectively. Furthermore, they can improve the personalisation of marketing communications.

The products below are some of the most commonly used in the UK for the purpose of geodemographic segmentation, as well as better understanding consumers' lifestyle, behaviour and attitudes, allowing marketers to segment their database effectively:

Acxiom: Personicx

Link: http://www.personicx.co.uk/

CACI: Acorn

Link: https://acorn.caci.co.uk/

Experian: Mosaic UK

Link: http://www.experian.co.uk/marketing-services/products/mosaic-uk.html

Other commercially available solution are able to append information to specific customers on a database. NB: The ICO doesn't endorse the use of any particular product or organisation.

Using third-party products under GDPR

This is possible – but with some caveats.

It's the responsibility of the organisation purchasing third-party data to have robust processes in place to check the personal data was collected in line with GDPR at source. Furthermore, an organisation selling third-party data also needs its own lawful basis to transfer personal data to its client.

Additionally, if you're going to use these products to complement your marketing, your customers must be told this is the case. You can read more about this in the privacy statements section of this guidance.

When data is collected from an individual, the business collecting the personal data must provide sufficient information to the individuals they are collecting personal data from. The individual should know what will happen to their personal data under the transparency requirements of GDPR and also how they can object to their personal data being used for marketing.

In 2016, several charities were found to be in breach of the DPA 1998 when they conducted so-called “wealth screening”. The third-sector organisations used third-party data to calculate a person’s net worth then targeted them with fundraising messages. The wealth screening management companies gathered other information from publicly available sources to investigate income, property values, lifestyle and even friendship circles. They were also able to identify people most likely to leave legacy donations.

Unfortunately, target donors were not told about the full extent of the profiling activity in the charities’ privacy policies. In this instance, people weren’t aware of the processing and were unable to object to it, leading to the ICO taking enforcement action.

Audit your suppliers

You must also be satisfied that the organisations you use to enrich your data sets are GDPR compliant. Ensure the personal data that is supplied by them has been collected in line with the new regulations. Remember, your intended use of the data must also be compliant with the GDPR.

GDPR and Customers' Right to Complain

A person can object to profiling for marketing at any time.

Once a data subject exercises their right to object, the controller must interrupt or avoid starting the profiling process.

Controllers are required to make the data subject explicitly aware of the right to object to processing set out in the text of the GDPR. These details should be presented clearly and separately. Concealing this right within the organisation's general terms and conditions is not acceptable.

In terms of automated decision-making, Article 22 (1) states: "Someone has 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 DMA and the marketing industry made the argument in lobbying that, in general, profiling for direct marketing purposes does not have a legal or significant impact.

For example, an organisation offering discounts to its most valued customers does not produce a legal effect. It should not infringe on someone's legal rights nor their freedom to associate with others. "Legal"or "significant" implies an impact on this scale.

However, there are instances where profiling for marketing may have a legal or significant impact. See the example on page 11.

Whether the profiling has a legal or significant impact depends on:

- the intrusiveness of the profiling process
- the expectations and wishes of the individuals concerned
- the way the marketing communication is delivered
- the particular vulnerabilities of the data subject.

If the result of the profiling is considered to have a legal or significant impact then an organisation will need someone's explicit consent to profile them. If not, the organisation might decide to not go ahead with the profiling. It would also need to carry out a DPIA before processing personal data.

Privacy statements

Under the GDPR, it's imperative that you tell people about your organisation's intention to use third parties to enrich an existing database and complement your marketing strategy.

You should explain in your privacy statement that you do this and the reasons why. You can explain how people can benefit from this activity and why it's necessary to provide them with the products or services that you offer. In other words, clearly set out the value exchange.

Article 13.2 (f) states that an organisation should include "the existence of automated decision-making, including profiling... meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

Meanwhile, the ICO advises:

> *"If organisations are re-using publicly available personal data, or personal data obtained from a third-party organisation, they should consider whether the third party's privacy notice adequately describes the circumstances in which the data will be further processed and whether the further processing is compatible with the original purpose."*

Examples

Below are several sections from the privacy statements of various commercial and charitable organisations. In each case, the statement is intended to explain profiling, covering the use of third-party supplier data as well as existing information held on in-house databases.

It's important to note that these examples are just passages of longer statements and should not be judged in isolation:

Age UK

We may analyse your personal information to create a profile of your interests and preferences so that we can contact you with information relevant to you. We may make use of additional information about you when it is available from external sources to help us do this effectively. We may also use your personal information to detect and reduce fraud and credit risk.

Royal Opera House

We may share your details with:

- Third party data services, for example Experian, who help us to segment and understand our audience by providing additional information so that we can send the most relevant and targeted communications possible.
- Third party advertisers (such as Facebook or Google) to help us identify customers similar to our audience or to serve relevant adverts to you on third party websites. The information shared with these advertisers is pseudonymised to protect your personal data.

BBC

Where we provide personalised services, we may analyse the information you supply, as well as your activity on our (and other) services, so that we can offer a more relevant, tailored service. For instance, we could use your viewing history on iPlayer to provide personalised recommendations or, if the first thing you look at every day on BBC Online is the weather for Luton, we could present this information or a link to it on our homepage. If you are signed-in or subscribed to email newsletters, you will receive a personalised service. If you don't want to receive these services you can unsubscribe from email newsletters, or disable personalisation. Please visit Your Account in Using the BBC to find out more.

Sky

Types of information we may hold about you and where it comes from:

- Information you've provided to us, including through our websites or when you access our services through applications on websites operated by other organisations.
- Information about our content, products and services you've ordered or enquired about.
- Information provided by other organisations who've obtained your permission to share information about you with us.

How we may use your information:

In addition to using your information for such necessary purposes, we may also use your information to improve our products, services and customer experiences, in the following ways:

- To monitor, improve and protect our content, products and services, work with our agents and business partners to improve the products and services we offer, and develop new content, products and services.
- To help us define groups of audiences to send adverts to, based on factors like interests, age, location and more, so we can show adverts to the people most likely to be interested in the products and services being promoted.

Conclusion

The Article 29 Working Party has explained that in many typical cases profiling for marketing purposes will not have a legal or similarly significant impact. This is crucial to the marketing industry as it means legitimate interests can be used a legal ground for profiling activity in most cases, subject to a successful Legitimate Interests Assessment (LIA).

Marketers were worried that they may need a separate tick box or permission for profiling as well as asking for consent to send marketing. This would have led to confusing marketing statements with an array of tick boxes that would not inform consumers; therefore running contrary to the spirit of GDPR, which aims to ensure that consumers are informed and organisations are transparent with them.

The new legislation has been provoked by the huge amounts of data made available by a plethora of new digital channels, and impressive advances in technology and big data analytics. These developments make it even more important for organisations to be upfront with individuals about how they will use individuals' personal data.

GDPR is an opportunity. Staying on the right side of regulations will require you to be proactive and engaged, but there's no reason why organisations can't do just that, and run effective marketing programmes to existing and new customers that are mutually beneficial.

GDPR Glossary

The GDPR uses terminology that marketers may not be familiar with. In order to provide clarity, the DMA has translated these legal terms so that marketing teams – those implementing the changes GDPR requires – and not just legal teams can fully understand the language used.

Anonymous data: The process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.

Consent: "... means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Controller: The organisation or individual that determines how the personal data is processed.

Legitimate interests: A legal ground that can be used to process personal data for direct marketing. As well as providing the right for individuals to object to the processing of personal data based on LI, the GDPR sets out strict criteria for organisations that seek to rely on it. These include establishing that the processing is necessary and that a balancing test has been conducted.

Personal data: Any information that can be used to identify a person is personal data. For example, names and email addresses are personal data because they reveal someone's identity. The GDPR expands the definition of personal data to include IP addresses and online identifiers such as cookies.

Personal data breach: A breach of security that means unauthorised individuals or groups are able to access personal data. This could be the result of hacking by outside groups or because an employee made a mistake.

Data protection by design: A concept introduced by Information and Privacy Commissioner of Ontario Dr Ann Cavoukian in the 1990s. It was globally recognised in 2010 by the assembly of International Data Protection and Privacy Commissioners as an essential component of fundamental privacy protection. It has been adopted in GDPR, whereby an organisation considers what impact a particular campaign, product, system or process may have on privacy from the start. In a marketing context, this means identifying a campaign's risks for privacy and/or data protection, recording and taking appropriate steps to mitigate them - considering privacy from the start and not as an afterthought.

Data protection by default: Similar to data protection by design, this phrase refers to privacy settings on goods or services. For example, when a phone app goes to market it should have its default privacy settings on the highest possible level. The user could then decide to lower the privacy settings.

Processing: Any operation conducted on personal data, which may include collecting, recording, storing, structuring, organising, transmission or dissemination of personal data.

Processor: The organisation that only processes personal data according to the instruction of the data controller. For example, an email services organisation only processes personal data in line with what its client discloses, making the email company a data processor.

Profiling: Any type of automated processing of personal data that evaluates the characteristics of someone to decide. Marketing segmentation or targeting is a type of profiling.

Pseudonymisation: A method of making personal data no longer personal, meaning someone could not be identified from the data. It is a process that reduces the privacy risks for people as they can no longer be identified.

Special categories of personal data: Criteria of personal data that are subject to stricter requirements because of their sensitive nature. GDPR lists the following as special categories of personal data: "... racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Supervisory authority: An independent public authority responsible for enforcing GDPR. The ICO is the supervisory authority in the UK.

Third party: Any organisation or individual that is not the data controller or processor that is authorised by either the controller or processor to process personal data. For example, if an organisation sold personal data to another organisation, the organisation purchasing the personal data would be classed as a third party.

About the DMA

The Data & Marketing Association (DMA) comprises the DMA, Institute of Data & Marketing (IDM) and DMA Talent.

We seek to guide and inspire industry leaders; to advance careers; and to nurture the next generation of aspiring marketers.

We champion the way things should done, through a rich fusion of technology, diverse talent, creativity, insight – underpinned by our customer-focussed principles.

We set the standards marketers must meet in order to thrive, representing over 1,000 members drawn from the UK's data and marketing landscape.

By working responsibly, sustainably and creatively, together we will drive the data and marketing industry forward to meet the needs of people today and tomorrow.

www.dma.org.uk

About our partners

The Data Protection Network is an online community dedicated to providing expert opinion, quality resources, informative events and learning materials, to both experts and non-experts in the field of data protection and privacy.

dpnetwork.org.uk

ISBA represents the leading UK advertisers. We champion the needs of marketers through advocacy and offer our members thought leadership, consultancy, a programme of capability and networking.

We influence necessary change, speaking with one voice to all stakeholders including agencies, regulators, platform owners and government.

Our members represent over 3,000 brands across a range of sectors. Over 100 members are represented on our Data Action Group, which provides discussion, events and guidance on GDPR.

ISBA is a member of the Advertising Association and represents advertisers on the Committee of Advertising Practice and the Broadcast Committee of Advertising Practice, sister organisations of the Advertising Standards Association, which are responsible for writing the Advertising Codes.

We are also members of the World Federation of Advertisers. We are able to use our leadership role in such bodies to set and promote high industry standards as well as a robust self-regulatory regime.

isba.org.uk

Copyright and disclaimer