GDPR for marketers: The essentials

In partnership with

Data Protection Network

ISBA

Contents

Welcome to GDPR guidance for marketers

May 25, 2018 will see 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 people at the heart of everything we do – and echoes our commitment to a code that enshrines five key principles which 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 has actively influenced the evolution of the GDPR text since first drafts were circulated by the EU Commission in 2011, supported by our expert partners at the Advertising Association in London and FEDMA in Europe. We have worked closely with our partners in government and across the wider marketing community throughout the draft process.

Our advocacy has established vital building blocks within the GDPR that will safeguard the interests of our members and bolster the wider marketing community. Of particular importance to marketers is the clear statement in Recital 47 that the processing of personal data for direct marketing may be regarded as being carried out for legitimate interests.

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, GDPR for Marketers: The Essentials, is one of a series providing marketers with a framework for innovation and growth. Other guides take an in-depth look at Accountability, Legitimate Interests, Consent and Profiling.

While ICO and Article 29 working party guidance apply across all business sectors and functions, this DMA series aims to be the definitive guidance for applying GDPR to marketing and communications. That is why we have collaborated with our DMA members, the members of ISBA, and the Data Protection Network to produce a consensus view.

Our work has been reviewed and contributed to by the ICO and we are grateful for their support.

The DMA believe that organisations must use GDPR as a catalyst towards creating people-centric business models. From the C-suite down we must all create ethical approaches that balance innovation and privacy as we embark on a journey into the fourth industrial revolution powered by data and technology.

Businesses that make data protection a core brand value in the years ahead will blossom.

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.

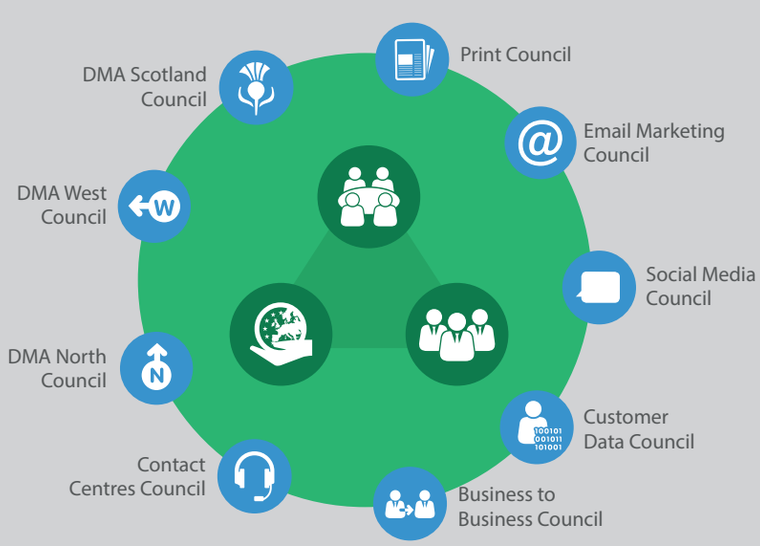
Elizabeth Denham
Information Commissioner

The DMA and the GDPR

How we create GDPR guidance

The GDPR Editorial Board leads the content direction of the DMA's GDPR outputs. We inform the work with expert advice and guidance from our Responsible Marketing Committee and the specially-appointed GDPR Taskforce.

To generate the right content for the right channels, the GDPR Editorial Board, Responsible Marketing Committee and the GDPR Taskforce work in collaboration with our Councils. This focuses our work onto the immediate needs of the marketers we serve.



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

Introduction

"For there is but one essential justice which cements society, and one law which establishes this justice. This law is right reason, which is the true rule of all commandments and prohibitions. Whoever neglects this law, whether written or unwritten, is necessarily unjust and wicked."
Marcus Tullius Cicero

The GDPR brings about legislative change that asserts that data belongs not to business, but to the individual. The new regulation aims to give people greater control over the collection and use of their personal data.

Implications are far-reaching, designed to make data protection law valid and viable long into the future. Businesses and marketers have a responsibility to take good care of consumer data and can't take it for granted.

This DMA guidance series will boost your understanding of this new data landscape. This introductory guide functions as an overall primer on the GDPR

You will be introduced to:

The origins of the GDPR

Understand why the GDPR is needed; the structure of the GDPR text; how consumer attitudes and DMA lobbying efforts shaped the GDPR; and how GDPR will function post-Brexit.

The scope of the GDPR

How far does the GDPR extend? What wider applications will it carry? What is personal data and a data subject – and what are special categories of data?

Data security and the GDPR

Data protection by design and data protection by default are explained; learn how the GDPR will be enforced; and the penalties non-compliance will carry.

Accountability and data security

An introduction into accountability under the GDPR, with a focus on what measures organisations will need to carry out in order to help demonstrate data protection compliance.

The Data Protection Officer (DPO)

What is a DPO? Will your business need to appoint one? What obligations do data processors have? Understand the data protection requirements for new products and services.

Data breaches

Providing data breach notifications to the ICO; communicating with data subjects following a breach; and a case study examining a data breach.

Legitimate interests

Get a DMA view on legitimate interests; why the DMA lobbied so hard to have this ground recognised in the legislation; and when and where legitimate interests can be used as a basis for marketing. Understand why the legislation recognises that the interests of business must be balanced with the customer's right to privacy.

Consent

A definition of consent under the GDPR; advice on gaining consent; a sample consent form; and insights into database requirements and records management.

Information rights

The brand benefits of direct engagement with consumers; how to collect personal data under the GDPR; what information must be provided to data subjects; and a brief Facebook case note.

Profiling

Tackle the GDPR definition of profiling and understand the key elements. You'll also grow an understanding of the legal effects of profiling.

Individual's rights

The spirit of GDPR is to give individuals greater control over their personal data, including certain rights relating to privacy and data protection. Organisations are obligated to respect individual rights.

GDPR key terms and phrases

A glossary of the most important terms in and around GDPR and data protection.

The Essentials guidance is the starting point for a more detailed exploration of the GDPR across other DMA guides in this series.

The origins of the GDPR

Why was the GDPR needed?

The first GDPR text was published by the EU Commission in January 2012. The Commission wanted to update data protection law because there had been huge technological advances since the 1995 Data Protection Directive, particularly in the marketing sector.

The law needed to consider new technological developments, the resulting proliferation of consumer data, and changing consumer attitudes and expectations.

Until the GDPR comes into force data protection standards still vary across the EU, but the new law will harmonise member states' data protection laws because it has a direct effect on national legislation.

What was the DMA's role in the GDPR?

The DMA represented the interests of the marketing industry while the GDPR was being debated in Brussels, in order to ensure a fair balance between the customer's right to privacy and the legitimate interests of business.

The work of the DMA, in collaboration with the Advertising Association and other marketing trade associations, including FEDMA in Brussels, helped achieve a more balanced final regulation when compared to early drafts from the European Commission and the European Parliament.

For example, the DMA advocated that the legislation should recognise the legitimate interests of business alongside the customer's right to privacy, and to have direct marketing recognised among legitimate interests for processing personal data in Recital 47.

What is the structure of the GDPR text?

The GDPR text is a lengthy document divided into articles covering specific issues. The text also has explanations of the articles, known as recitals.

The articles and the recitals both need to be taken into account to get a complete picture of the law. There are 99 articles which make up the letter of the law and 173 recitals.

What about the role of consumer attitudes to data?

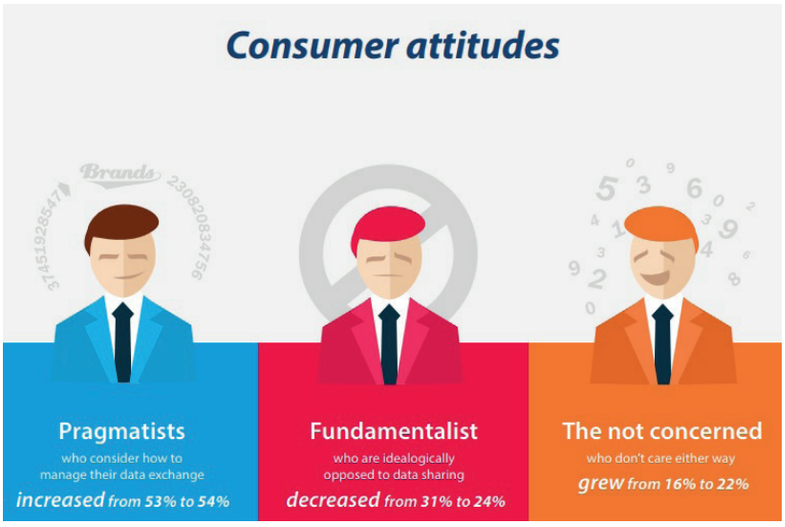
The GDPR is written in a more EU citizen-centric way than any of the data protection laws that came before it. That said, recent research has suggested that there are varying opinions on data privacy and these have been grouped into three distinct segments: pragmatists, fundamentalists and those not concerned.

These opinions are explored in more detail in research carried out by the DMA.

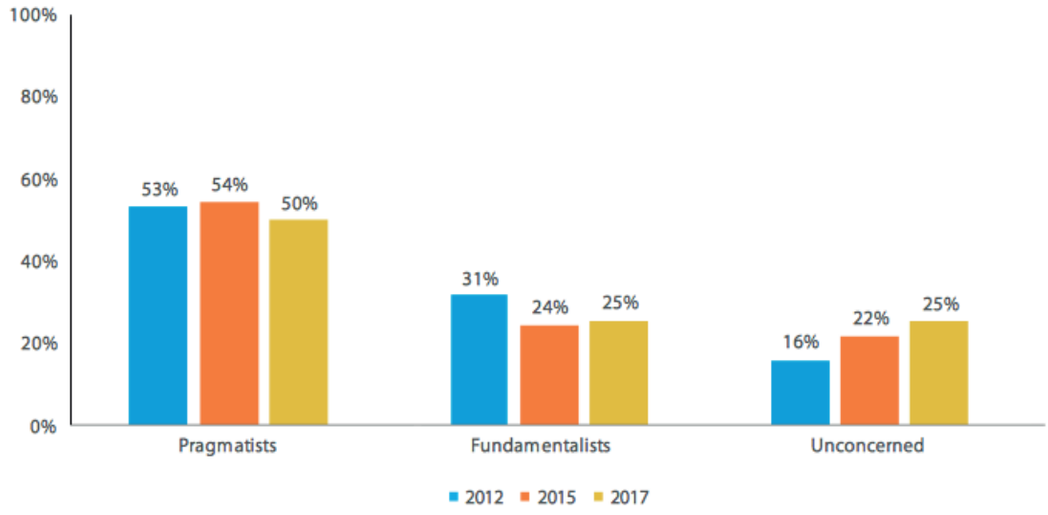
Essentially, attitudes towards data may be evolving, but trust remains the constant and key factor when it comes to understanding what people feel is most important about data.

Under the GDPR, the default position is that the individual is the owner of their data, so the default position is to give the individual choice and control over how their data is used. Brands that fail to take responsibility lose customers, goodwill and ultimately shareholder value.

Those that can demonstrate good data governance will find customers trusting them more and sharing their data, which should lead to better revenues.



Full segmentation of attitudes towards privacy in the UK (2012-2017)*



*from the DMA and Foresight Factory report Data privacy: What the consumer really thinks, 2018

Life after Brexit?

The UK will be exiting the EU and therefore will not be subject to EU legislation.

However, any future trade deal must protect the free flow of data between Europe and the UK. As such, the UK must achieve adequacy status (equivalent data protection standard) or a similar bespoke deal to ensure UK companies continue to be able to trade successfully in the digital single market. The UK Government has said it would like to achieve a bespoke agreement, the so-called 'Adequacy Plus', based on the UK's unique relationship with the EU.

Adequacy is a status granted by the EU to non-member nations, which certifies that the country in question offers "essentially equivalent" data protection safeguards. Once granted adequacy, a country can exchange personal data freely with other EU member states.

As a prerequisite for adequacy status, the government intends to adopt the GDPR irrespective of this.

The government has proposed the Data Protection Bill, currently being discussed in Parliament, which will implement much of the GDPR, such as the various derogations. The EU Withdrawal Bill will also bring the GDPR into UK when we leave the EU.

What is the scope of the GDPR?

The processing of any personal data belonging to EU citizens or others resident in the EU will be subject to the GDPR rules no matter where the data is stored or processed – this is known as the territorial scope.

This means organisations processing personal data about customers resident in the EU will need to abide by the law, and if a non-EU based organisation is offering goods or services to individuals in the EU or monitoring the behaviour of individuals residing in the EU then the law applies to them, too.

Article 3 territorial scope

"This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

Examples of the wider application of the GDPR

Scenario	Directive applies	GDPR applies
US company without any EU subsidiaries offering free social media services via a website hosted in the US to individuals in the EU	x	✓
Singaporean hotel booking business using cookies to track past customers' (including EU-based customers) browsing in order to target specific hotel adverts to them	x	✓
Chinese flower delivery company allowing data subjects in the EU to make orders for fulfilment only in China	x	✓
Australian retailer with a website for orders/deliveries. The website is accessible to individuals in the EU in English. The currency is the Australian dollar and the address fields only allow Australian addresses	x	x

Credit: Slaughter and May

The GDPR is already law, but will come into force in each individual EU Member State on 25 May 2018.

For organisations established in the EU, the GDPR will always apply. For those who are non-EU establishments, there are certain conditions for the GDPR to be triggered.

Processing activities must be related to:

- Offering goods or services, irrespective of whether a payment is required, to such individuals in the Union
- The monitoring of their behaviour, as far as their behaviour takes place within the Union. The GDPR will expand the scope of data protection legislation.

The previous legislation only applied to data controllers – usually the brands or agencies that have a relationship with the customer. Data processors now have obligations under the GDPR as well, those that may provide services for the brand or agency.

For example, an email service provider would be a data processor. They only process personal data in accordance with what their client tells them to do, but now they could have enforcement action taken against them if they commit a fundamental breach of the GDPR.
Under Data Protection Act 1998 (DPA 98) the email service provider's clients would have enforcement action taken against them. However, liability is now shared between both parties under the GDPR.

What is the definition of Personal Data and a Data Subject?

The definition of personal data under GDPR is broader than it is under the DPA 98. It explicitly references online identifiers such as IP addresses and social identities - such as Facebook or Snapchat profiles - if an individual can be identified directly or indirectly from that information. Indirect identification can include using any data you are likely to, or able to, obtain in the future.

What are special categories of data?

Categories of sensitive personal data are now referred to as "special categories". In most cases for marketers, these can only be processed with explicit consent. Great care needs to be taken to prevent unauthorised use.

Special categories of data are defined as data concerning:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Data concerning health or sex life
- Sexual orientation

Data regarding criminal records also requires special treatment under individual member state law (see articles 9 and 10 of the GDPR text for further information).

Who will enforce the GDPR?

There will be a supervisory authority for the GDPR in each EU member state, and there will be co-operation between supervisory authorities in cross-border disputes.

Current regulators will become supervisory authorities (for the UK this is the ICO).

The ICO will liaise with other supervisory authorities in instances where UK organisations are suspected of breaching the GDPR in other member states, and vice-versa.

(See Article 51 of the GDPR text for further information)

Accountability

What is the principle of accountability?

The principle of accountability under the GDPR is about being able to demonstrate compliance with all of the GDPR's principles. Carrying out a Data Protection Impact Assessment (DPIA) or employing a data protection officer (DPO) are tools you can use to evidence your compliance.

These measures are important to successfully implementing the regulation. The GDPR is principles based but much of it has a risk-based approach. Effective risk assessment is an important part of successful compliance.

The mitigations that you use must be appropriate to the risk to that data. There are a number of tools in GDPR that will help you ensure that privacy risks are mitigated as much as possible and ensure you're able to evidence your compliance. These include:

- Privacy by design
- Privacy Impact assessments
- Breach notification
- Data Protection Officers
- Data Security

(See Articles 5, 25, 30 and 35 of the GDPR text for further information).

Accountability is a core principle. The GDPR asks companies to be accountable for their own decisions on how they collect and use personal data, and be able to have records and evidence of the decisions they made and how they made them. Companies need to be clear about why they need the data, what they are going to use it for, how they are going to keep it secure and the legal basis they are using to process the data.

Accountability applies to everyone in the organisation. The company is responsible for what it does with its customers' data and has to consider the customer's right to privacy when developing new products, services or marketing campaigns. The notion of data protection by design and tools such as DPIAs should become standard business processes and will be required in certain circumstances.

Most importantly, accountability should be driven at board level – it's not just an issue for the lawyers. Ensuring an organisation builds a culture of accountability, transparency and trust is the responsibility of the CEO working closely with the data protection officer.

A DPO will be required if an organisation's core objectives consist of regular and systematic monitoring of large quantities of personal data as well as in other situations. They must also be independent and report to the highest level within the organisation.

The nature of the GDPR means that organisations will not be given fully comprehensive guidance telling them what to do in every scenario. In the absence of definitive answers, organisations will have to make their own risk-based decisions about how best to do things in a compliant way.

The DMA believes the risk-based approaches in the legislation could prove to be a positive for organisations, providing flexibility to make judgements on an approach to GDPR compliance. Given accountability is a key principle in the GDPR, it means that it is not enough for organisations simply to comply. They also have to demonstrate that they are complying.

To do this, organisations must put in place technical, organisational measures, as well as training programmes, policies and audits, to ensure they have the evidence to justify their actions. Besides this they can use tools such as data protection by design/default and DPIAs. Organisations will have to make a business-risk and policy decision about how they are going to implement marketing and data processing.

If organisations pursue minimal compliance with GDPR they're likely to lose customer trust and run the risk of enforcement action by the ICO.

For further information, please refer to the DMA's Guidance on Accountability.

Accountability and data security

The GDPR states:

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."

This can be done by using a number of methods. The regulation specifically cites "encryption or pseudonymisation" which effectively make the data unreadable without a secure key.

The regulation also requires the data to be protected in such a way that its integrity, confidentiality and availability is always ensured.

What is data protection by design?

One of the key requirements of GDPR is the concept of data protection by design.

This concept was first developed in Canada and has been adopted by the EU and endorsed by the ICO under the current law. It is the keystone for compliance for organisations.

It's based on seven foundational principles:

- Proactive not reactive
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – Positive sum, not zero sum
- End to end security – Full lifecycle protection
- Visibility and Transparency – Keep it open
- Respect for User Privacy – Keep it User Centric

Data protection by design is built in from the beginning of new product development or a marketing campaign.

Risks to people's privacy from the product or marketing campaign are considered, and where necessary those risks are mitigated - rather than marketers only thinking about privacy risks once they have created a campaign or after a new product is on the market.

This is a particularly important concept as technology evolves, connected devices proliferate, and we see more widespread use and adoption of augmented intelligence.

Data protection by default explained:

This entails new products and services having their privacy settings at the highest level when released.

For example, an app developer for smartphones would need to release a new product with default privacy settings at the highest possible level. It is then up to people to relax their privacy settings, if they want to.

At the moment, personal data must be kept securely by the data controller, who must ensure appropriate measures are taken to prevent a data breach.

(See Article 5 of the GDPR text for further information.)

Data protection for new products and services

The GDPR is a real opportunity for businesses to weave data protection and privacy together with innovation, and to think about how such data protection by design bolsters brand image, too.

Any data protection by default means that new products or services should have data protection settings at the highest level from launch. Measures to help deliver data protection by design and default are:

- Minimising the processing of personal data
- Pseudonymising personal data as soon as possible
- Transparently describing the functions and processing of personal data
- Enabling the data subject to monitor the data processing

(See Recital 78 of the GDPR text for further information).

The Data Protection Officer (DPO)

A DPO will be either an employee or an external person with responsibility for advising the business on GDPR compliance. The responsibility for compliance with the regulation is borne by the senior management of the business.

The DPO's work will focus around:

- Being the subject matter authority for their organisation on the requirements of the GDPR
- Consultation services during Data Protection Impact Assessments
- Acting as the central contact for data subjects and for when a business co-operates with national supervisory authorities (i.e. the ICO).)

DPOs will lead on data audit projects and co-ordinate the implementation of compliance tools across the business.

A DPO must not have a conflict of interest. For example, they must not determine the purpose of the data processing, but must have access to adequate resources, be independent and be able to report directly in at a boardroom level.

They can have a dual role, but it must not lead to a conflict of interest. This means that other roles such as Head of HR, COO, CTO CCO etc would have a conflicted interest.

The DPO in an organisation:

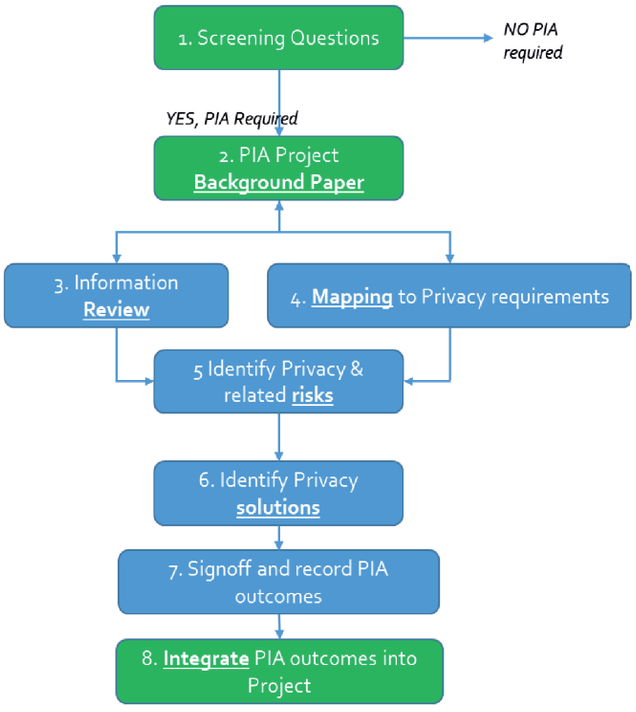
Meanwhile, the DPO's organisation must ensure the DPO is involved immediately with any projects, or attendant to any issues related to or arising from data protection compliance.

What a DPO does

A DPO is required to:

- Monitor business compliance with the GDPR
- Advise the business on all data protection issues and challenges
- Carry out data protection impact assessments ("DPIAs)
- Ensure the business takes a risk-based approach to assessing processing activities. While not a GDPR requirement, this is highly recommended. DPIAs are an integral part of data protection by design as they can help to identify possible risks to an individual's privacy, allowing an organisation to take action to mitigate those risks or cease the processing.

The Privacy Impact Assessment Process



PIA Decision.
Project owner to complete form (1) for Compliance review. PIA decision.

Preliminary Phase
Project owner to complete form (2) for Compliance review

Analysis Phase
Compliance to discuss project details with project owner, completing templates (3) and (4).
Compliance to then identify related privacy risks (5)

Solutions Phase
Compliance to consider all actions that can reduce the privacy risks. This should be a collaborative process with the project owner.

Documentation Phase
Compliance to document agreed outcomes

Project Integration Phase
Compliance to document; Project owner to integrate

Data breaches

When do you have to provide notification of a data breach?

In the case of a personal data breach, the organisation should without undue delay or within 72 hours report it to the ICO. Where a high risk is posed to people from a data breach, they must also be informed and also, where feasible, within 72 hours. For example, if personal health information was breached, this could constitute a high risk.

(See Article 33 and 34 of the GDPR text for further information.)

The data controller must notify the supervisory authority of a breach within 72 hours or without undue delay. The notification must cover the following elements:

- Nature of the breach
- Number of data subjects
- Categories of personal data
- Proposed mitigation
- The possible consequences of the data breach
- Contact details of the DPO

Notification of a breach is mandatory, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Communicating with data subjects following a breach

If the risks posed to the freedoms and rights of data subjects are high, the data controller must also inform all data subjects affected by the breach without undue delay.

The notification should explain in clear language:

- The nature of the personal data breach
- The likely consequences
- The name of the data protection officer (as a minimum)
- The actions the data subjects can take to mitigate any risks

Letters to data subjects must be carefully drafted to mitigate negative reputational impact and you must also take into account advice from other authorities, such as the police. The letter should also be clear, concise and understandable for the data subject.

Data controllers will also need to manage reactions by briefing customer service operators, and monitoring commentary on social networks and blogs.

Experience from the US, where breach notification has been required for some time, suggests that apologies should be backed up with practical advice about how the individual can take action to protect themselves in the event of a breach.

What are the penalties under the GDPR?

The GDPR gives regulators significant new powers, including the ability to issue much higher monetary fines.

For the ICO and its European counterparts, when data controllers (and now data processors) infringe specifically identified sections of the GDPR, or present risks to individuals, they can issue fines up to €20m or 4% of annual worldwide turnover, whichever is greater.

For further details about the sanctions read Article 83 (4) and (5) of the GDPR.

This compares to a maximum fine of £500,000 under the current UK Data Protection Act 1998. However, conspiracy theories abound about the ICO's approach to fines and penalties:

"The ICO is bound to fine a (insert business sector here) company in May next year" or "They are going to hit one or two companies with some big fines to scare people into being compliant".

The Information Commissioner has told us that the GDPR is not about seeking to issue as many fines as possible. For them, GDPR and its implementation is about putting the consumer and citizen first. Focusing on big fines makes for great headlines, but thinking that GDPR is about crippling financial punishment misses the point.

The ICO policy has always been one of proportionality: it would much rather educate an organisation and see it correct bad practice before even talking about fines. Even with its current enforcement powers, the ICO has never issued the maximum fine of £500,000.

The size of the organisation, the impact of the breach and whether or not sufficient policies and procedures are in place to justify action (accountability) will all be taken into account.

Legitimate interests

During a parliamentary debate, the DMA advocated that a business' legitimate interests were recognised alongside the customer's right to privacy. Communicating to prospects and customers is the essential lifeblood of commercial success so direct marketing is recognised specifically in the text as a legitimate interest in Recital 47.

Marketers have always been able to rely on the legitimate interests condition as an alternative to consent under DP 98, in cases where the Privacy and Electronic Communications Regulations (PECR) – which preceded DP 98 - wasn't applicable. However, this legal basis was not stated as explicitly in DP 98 as it is in the GDPR.

Legitimate interests is one of six legal grounds in the new law that allows the processing of personal data. All of these legal bases are equally valid.

The specific information needed for valid consent are rigorous, which can make it problematic to use for direct marketing activities. The DMA expects legitimate interests to be a widely used lawful basis for processing, particularly given the high level of flexibility given to organisations in explaining and documenting their rationale for processing activity.

The GDPR says:

"The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest" (see Recital 47 of the GDPR text for further information).

In addition, the GDPR says that processing is lawful if it is:

"Necessary for the purposes of the legitimate interests pursued by the controller or by a third-party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal information, in particular where the individual is a child" (see Article 6.1(f) of the GDPR text for further information).

When can legitimate interests be used to justify marketing?

Organisations may be able to rely on legitimate interests for data processing for:

- Postal marketing
- Email to existing customers using the soft opt-in option
- Telephone marketing to individuals who have not previously objected to you, or numbers which are not listed on the Telephone Preference Service (TPS).

Remember, your organisation must also be compliant with PECR in these circumstances.

When an organisation uses legitimate interests as the basis for processing, it is subject to appropriate balancing tests such as a Legitimate Interest Impact Assessment (LIA). The use of segmentation, targeting, profiling and analysis can also be covered by legitimate interests, providing that the LIA rules in favour of the proposed processing. If profiling is automated and therefore covered by Article 22 (1) of the GDPR then consent must be sought.

There are two conditions that must be met:

- The processing must relate to the legitimate interests of your business or a specified third party, providing that the interests or fundamental rights of the data subject do not override the business' legitimate interest. For example, a mail order clothing company may wish to keep its customers updated by sending them regular catalogues. Alternatively, an online retailer may use consent for email marketing communication but use legitimate interests for its customer profiling
- The processing must be necessary to achieve the legitimate interests of the organisation.

The DMA has collaborated on the industry guidance on Legitimate Interests 1.0 in tandem with other partners, including the DPN, ISBA and Bristows. Version 2.0 will follow.

You can read more about this guidance here.

Consent

There are six equal legal grounds for processing personal data in the GDPR but marketers are most likely to use legitimate interests or consent.

Depending on the context, a marketer may need to use the legal basis of consent.

The DMA has consistently informed the marketing community that the six bases of data processing are equal. To paraphrase George Orwell: some consent is not more equal than others.

What is Consent?
The definition of consent was very contentious as the GDPR text was being written. Finally, the word "explicit" was removed from the definition and the word "unambiguous" replaced it.

The GDPR says:

"Consent of the data subject 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" (see Article 4 of the GDPR text for further information).

The need for clear, affirmative action to agree to the processing of personal data is a new consideration and presents a new challenge in obtaining consent.

It is important to note what doesn't count as consent.

For example, marketers often use the phrase "opt-out consent" - but this will no longer exist under the GDPR.

Any form of passive or implied consent will not be valid. The regulation specifically rules out the use of pre-ticked boxes, which are still commonly used online. .

In a marketing context, consent may not preferable as it might be difficult to obtain. In some instances, marketers will be required to ask for consent, such as for cold business-to-consumer email marketing. However, where consent is not required, marketers could consider using legitimate interests as their legal basis for marketing.

Obtaining consent
Under the GDPR, organisations will need to obtain clear and unambiguous indications of consent for marketing. Consent can be written, including electronic or an oral statement. Here are some pointers:

Consent includes:

- Ticking a box when visiting an website
- Choosing technical settings. For example, altering your privacy settings in your internet browser could be a valid consent mechanism, providing all the consent requirements were met
- By any other statement or conduct which clearly indicates acceptance

Consent does not include:

- Silence
- Pre-ticked boxes
- Inactivity

The wording below gains opt-in consent for updates, tells the individual that their information will be used to predict potential interest (i.e. profiling for direct marketing) and reminds them that they have the right to object.

This means that the requirements for consent to be "freely given, specific, informed and unambiguous" have been met.

Sample wording for valid consent:

At xxxxx, we have exciting offers and news about our products and services that we hope you'd like to hear about. We will use your information to predict what you might be interested in. We will treat your data with respect and you can find the details of our Contact Promise here.

☐ I'd like to receive email updates from xxxxx based on my details..

You can stop receiving by clicking here.

What proof of consent will be needed?

New GDPR requirements mean that an organisation must be able to demonstrate that an individual consented to the processing of their personal information.

- Your records should include who consented, when, what they were told, how that consent was given, by what mechanism and, if applicable, the timestamp
- You will need to retain copies of both on- and offline data collection forms for a reasonable period of time, including telephone scripts and notes of any changes made to these documents.
- Organisations must make sure that they can produce effective audit trails of how and when consent was given in order to give evidence of consent if challenged.
- The fact that consent has been withdrawn by the individual or is invalidated by a change of circumstances would also need to be recorded. Consent should be as easy to withdraw as it is to give.

Consult Article 7 of the GDPR text for further information.

The DMA's GDPR checklist has a consent section.

Effects on the database and records of processing

Database requirements

The act of consent, when it was given and the wording used must be recorded in the database. Meanwhile, the database will likely include a wide range of flags about consent, which must be carefully managed.

What other records of processing must be kept?

The GDPR requires data controllers and processors with more than 250 employees to keep detailed records of all processing activities (see Article 30 of the GDPR text for further information). Smaller businesses are exempt unless the processing carried out comes with a high privacy risk, involves special categories of personal data or is not occasional. At the time of this guide's publication the Article 29 Working Party had yet to define what "occasional " means in this context.

What information must be captured?

An organisation will be obliged to show processing records to the supervisory authority – in the UK, the ICO - on request. Maintaining accurate records allows an organisation to help demonstrate that it is compliant and has complied with the GDPR if the supervisory authority investigates.

For further information and case studies relating to consent, consult the DMA guidance on consent.

Right to be informed

GDPR offers organisations the opportunity to engage more directly with their customers about their personal information to build their trust and confidence.

Communicating changes in a clear and consistent way is vital.

The DMA advises a customer-centric approach as opposed to a GDPR-centric approach.

What information must you provide to data subjects?

When personal data is collected by an organisation, it has a duty to tell people how their personal data is going to be processed, amongst other things. This is done to make processing transparent and fair.

This applies for both the consent and legitimate interest legal grounds, and all the other legal grounds, too. The information you must display in your privacy notice includes:

- Name of organisation
- DPO contact details, where applicable
- Whether the data will be used for direct marketing
- Categories of personal data
- Purposes of the processing
- Categories of recipients of the data (who will get to see it)
- What legal ground the organisation is relying on
- Third parties the data will be shared with (this might be specifically named third parties or sectors – the ICO will publish formal guidance
- Countries outside the EU where personal data might be stored or processed
- How long the personal data will be kept
- Inform people of their rights and how they would exercise them
- A reminder that people can withdraw consent
- Inform people that they can complain to the ICO
- Information about automated decision-making, including profiling

This information must be displayed at a minimum in "clear and plain language", which must be relevant to the audience (see Article 12 of the GDPR text for further information). For example, if the retailer was marketing a product aimed at 14-year-olds, the messaging would need to be appropriate for that age. You can test statements to assess their suitability for your audience. Ideally, information should not deviate from a brand's tone of voice, meaning the creative teams are as important as the legal and compliance teams in crafting such notices.

The ICO issued guidance on children and the GDPR: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/children-and-the-gdpr-guidance/

Individuals' rights

What is the right to object?

The standalone right to object to processing personal information for direct marketing already exists under the 1995 Directive and Data Protection Act 1998. Individuals have a right to object to their personal data being used for direct marketing and to object to profiling for the purpose of direct marketing.

The right to object has been expanded under the GDPR, so that individuals must be told if profiling will be used for direct marketing and that they have the right to object to such profiling (see Article 21 of the GDPR text for further information).

A new requirement under the GDPR is that this right to object must be brought to the attention of the data subject clearly and explicitly at the time of collection of their data or in the first communication made to them.

A full list of rights is as follows:

- The right to be informed - to know what happens to their information
- The right of access - this is known as Subject Access Request (SAR)
- The right to rectification - data should be kept accurate
- The right to erasure - the right to have data deleted / to be forgotten
- The right to restrict processing - where the data subject believes the data is inaccurate or requires it for legal claims, or believes the processing is unlawful or is challenging the data controller's legitimate interests
- The right to data portability - to transfer data from one supplier to another
- The right to object - to stop data from being processed
- Rights in relation to automated decision making and profiling - not to be profiled or to have a human make automated decisions.

Individuals' rights

What specific rights do individuals have under the GDPR?

In addition to the right to object to direct marketing and profiling, individuals have some key rights under the GDPR.

These other rights are explained below:

- The right to erasure: also known as the right to be forgotten, this has caused a lot of debate but was included in the final text (see Article 17 of the GDPR text for further information). The European Court of Justice had already ruled that individuals had the right to request search engines to remove links, but this gives the individual the right to request that their data is erased by any data controller
- The right to data portability: principally to aid account switching, but will affect all data controllers (see Article 20 of the GDPR text for further information). An individual has the right to ask that data held on them is transferred to a new provider in electronic form. This only applies where the processing is based on consent or contract or explicit consent for special category data, and processing is by automated means
- The right to subject access: where the individual can demand access to what data is held about them will now be free of charge (see Article 15 of the GDPR text for further information).

More on the right to erasure (right to be forgotten)

The right to erasure allows data subjects to request that their personal data be erased without undue delay. This right is designed to protect people in the "new world" where lives are lived in public and on social media sites, but it is not limited to these data controllers.

There are exemptions. Individuals cannot use this right to avoid liabilities they have incurred with the data controller. Controllers must inform data processors of any erasure request(s) and take reasonable steps to tell other data controllers where data has been shared.

Someone may request that their data is deleted by an organisation,yet the organisation could still keep its personal data on an in-house marketing suppression file. Deleting all of the personal data would otherwise mean the organisation were unable to comply with the request not to receive marketing.

More on the right to data portability

The right to portability is a new right designed to make it easy for consumers to switch accounts.

The individual has the right to receive his or her personal data in a structured, commonly used and machine-readable format (see Article 20 of the GDPR text for further information).

This right applies when the processing is based on consent, or the data is necessary for the performance of a contract. The right also applies when the processing is carried out by automated means.

It does not apply when the processing is undertaken using any other grounds, such as legitimate interests.

Where technically feasible, the data subject has the right to ask for the data to be transferred directly from controller to controller.

Data controllers will be encouraged to develop interoperable formats for data portability, but the GDPR does not create an obligation for the controllers to adopt or maintain data processing systems which are technically compatible.

Profiling

How does the GDPR define profiling?

The previous Data Protection Directive did not have a definition of profiling.

The new GDPR distinguishes between different types of profiling and their impact.

For example, automated decision making that has a legal or similarly significant effect, and the type of normal day-to-day processing that marketers use for personalisation, segmentation, targeting and relevance.
An example of an automated decision with significant effect is a bank that runs an algorithm that analyses particular aspects of a person in order to decide whether their application for a loan is successful or not. This is an example of an automated decision and whether the person is granted the loan or not is an example of a legal effect.

A person can object to profiling for marketing at any time. Individuals also 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" him or her.

The full definition of profiling reads as follows in Article 4(4) of the General Data Protection Regulation (GDPR)

"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"

What are the key elements to profiling?

There are three:

- The processing has to be automated: profiling or decision making by a human being is not covered
- It must involve personal data. The use of non-personal data to make an automated decision is not covered. For example, analysing the number of households in a specific geographical area by reference to streets and street numbers does not count as profiling
- It must be used to evaluate certain personal aspects relating to an individual: personal aspects might include income, family composition or payment history of an identifiable individual.

The more extensive or intrusive the profiling for direct marketing, the more likely it is to infringe on the individual's rights and thus not fulfil the legitimate interests processing condition.

Marketing personalisation, such as age and interest segmentation, can be carried out using legitimate interests, providing the LIA you carry out authorises the processing. The Article 29 Working Party draft guidance on profiling references Recital 47 enables processing data for the legitimate interests of the organisation.

Marketing personalisation such as, age and interest segmentation can be carried out using legitimate interests. The Article 29 Working Party draft guidance on profiling references Recital 47 which enables processing data for the legitimate interests of the organisation.

Controllers are also required to provide fair processing information about solely automated decision making (including profiling). Under Article 22, organisations must make people aware of the following information:

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

However, Recital 63 notes that controllers are not required to divulge trade secrets or intellectual property.

What obligations do data processors have?

Firstly, let's look at the relationship between processor and controller:

- Processor - a body which processes personal data on behalf of the controller
- Controller - a body which, alone or jointly, determines the purposes and means of processing of personal data.

Examples would include a telemarketing bureau, an email broadcaster or a mailing house. Here are two simple illustrations:

The main change under the GDPR is that outsourced service providers will be liable for breaches of the GDPR in circumstances where they have initiated breaches or where they have acted outside the client's instructions which result in a breach.

As the outsourced service provider will now share liability for compensating damages resulting from breaches, they will have to prove their data protection compliance under the GDPR, and this will become a significant factor in the procurement of external processing services going forward.

Under previous legislation a data processor was immune to any investigation or regulatory action as they were 'just a processor acting on the instructions of the controller'.

Now that both are jointly liable, companies will expect their outsourcers to ask a lot of questions in order to carry out their due diligence about the source and accuracy of personal information they are being asked to process.

A processor now has the obligation to inform the data controller if any of the instructions that they are given, breach any data protection laws.

Conclusion

At first glance, the GDPR can be seen as a hindrance for marketing activities, but a closer examination of the regulation reveals that it gives marketers an opportunity to build more transparent and meaningful relationships with their customers.

The GDPR mirrors the DMA's long-held view about the need to place the customer at the heart of everything we do and echoes our commitment to a code that enshrines five key principles which 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.

Out of the six legal bases for which an organisation can process data of an individual, two closely apply to marketing activities: legitimate Interests, in certain circumstances, and consent.

Consent, the more obvious choice for marketing activity, gives the GDPR its poor reputation in our industry, but the DMA has established vital building blocks within the new regulations that will safeguard the interests of marketers. This has been made possible mainly by our advocacy for direct marketing to be carried out under legitimate interests, thus opening up more opportunities to build and strengthen relationships with customers.

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 – the ones who will be implementing the changes the GDPR requires – not just legal teams can fully understand the language used.

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

Consent: According to the GDPR, 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 interest (LI): A legal ground that can be used to process personal data for direct marketing in certain circumstances. 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 LI. 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, like 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: Data-protection-by-design is a new concept introduced by the GDPR, whereby an organisation considers what impact a particular campaign or product may have on privacy from the very start. In a marketing context this means identifying a campaign's risk for privacy and/or data protection, recording them and taking appropriate steps to mitigate them, thinking about 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 a good or service. For example, when a phone app goes to market it should have its privacy settings set to the highest level possible as the default setting. The user could then decide to lower the privacy settings, if they so wished.

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 their client tells them and this means they're a data processor.

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

Pseudonymisation: A method of making personal data no longer attributable to an individual, without further information, 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 its sensitive nature. The 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 the GDPR. The Information Commissioner's Office (ICO) are 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

A DMA membership will grow your business.

Our network of more than 1,000 UK companies access research, free legal advice, political lobbying and industry guidance. DMA members connect at regular events that inspire creativity; showcase innovation; examine and provide insights from award-winning campaign work; and grow our understanding of how responsible marketing and the GDPR will transform how we all work.

Membership of the DMA acts as a badge of accreditation and we provide expert-led guidance across channels, underpinned by a code that puts the customer at the heart of everything we do.

We represent a data-driven industry that leads in creativity and innovation: a sector that attracts the brightest minds, the individuals that will shape the future.

By sharing our knowledge, together, we'll make it vibrant.

To find out what we can do for you, email: membership@dma.org.uk

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 3000 brands across a range of sectors. Over a hundred 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