

Data: A New Direction – Consultation Response

November 2021

Responsible Marketing

DM
Data &
Marketing
Association **A**

/ Contents

Data and Marketing Association.....	03
Approach to the Consultation.....	04
1. Chapter 1.4: Availability and use of legitimate interests	05
2. Chapter 1.5: AI and Machine learning.....	07
3. Chapter 1: Innovative Data Sharing Solutions.....	07
4. Chapter 2: Reform of the Accountability Framework.....	09
5. Chapter 2: Subject Access Requests.....	10
6. Chapter 2: Privacy and Electronic Communications	10
7. Chapter 2: Sectoral Codes.....	13
8. Chapter 2: Use of personal data for democratic engagement.....	15
9. Chapter 3: Boosting trade and reducing barriers to data flows.....	15
10. Chapter 5: Reform of the Information Commissioner's Office.....	16
11. Supplemental topic: Notification requirements under Article 14 of UK GDPR.....	19
12. Supplemental topic: simplifying the legislative framework.....	21
Appendix 1: DMA Code.....	22
Appendix 2: GDMA Global Principles	28

/ Data and Marketing Association

The Data & Marketing Association (DMA) is Europe's largest trade body in the data and marketing industry, representing over 1,000 data-driven organisations across the UK. The DMA played a major role in the shaping of the GDPR data protection laws in the UK and the EU and led the implementation in our industry, working closely with the ICO, as the trusted source for industry advice and guidance. The DMA has almost a century of experience in data protection legislation, pioneering ethical approaches to customer engagement throughout our history.

The Data and Marketing Association is UK's most customer focussed business community led by a Code of ethics. All corporate members must pass a compliance audit to ensure they are compliant with our Code before they are accepted into membership. Through our wholly owned Institute of Data and Marketing we drive for marketing excellence through development and learning opportunities. DMA Talent's range of initiatives is inspiring a new and more diverse generation into the data and marketing industry to help meet the needs of today and tomorrow.

From the classroom to the boardroom, the DMA is driving the force of intelligent marketing, moving the data and marketing industry forward ethically and responsibly. Our classroom to boardroom journey supports 750 student members, almost 1,000 individual members and most significantly over 1,000 corporate members ranging from large multinational brands to SMEs.

/ Approach to the Consultation

Attracting and retaining customers is the essential business activity that drives growth in every business and in the economy. Data-driven marketing and customer engagement drives every aspect of an organisation's relationship with a customer. The most profitable of these relationships are underpinned by trust – where marketing is an exchange of value between businesses looking to prosper and customers looking to benefit – as exemplified in the DMA Code (Appendix 1).

The DMA's commitment to high standards of personal data protection is led by our customer first principles enshrined in the DMA Code and best practice guides. Putting the customer first informs our overall approach, ensuring that data is used as a force for good for both the economy and society more broadly

The topics covered in our consultation response are those which will have a direct impact on building successful customer relationships, both in terms of greater certainty around customer acquisition or retention and safeguards for customers to ensure trust is earned and maintained over time. In exploring these areas our questions will primarily focus on:

1. Legitimate Interests (chapter 1.4, pages 21-23)
2. AI and Machine Learning (chapter 1.5, pages 24-44)
3. Innovative Data Sharing Solutions (chapter 1.7, pages 47-52)
4. Chapter 2: Reform of the Accountability Framework (pages 53-68)
5. Chapter 2: Subject Access Requests (pages 69-72)
6. Chapter 2: Privacy and Electronic Communication (pages 72-84)
7. Chapter 2: Sectoral Codes (clause 201 and Q2.4.5)
8. Chapter 2: Use of personal data for democratic engagement (clauses 219-228)
9. Chapter 3: Boosting trade and reducing barriers to data flows
10. Chapter 5: Reform of the Information Commissioner's Office
11. Supplemental topic: Notification requirements under Article 14 of UK GDPR
12. Supplemental topic: simplifying the legislative framework

Overall, the DMA agrees that there is a lot of untapped value in data being held in the private and public sectors that if unlocked could have a transformative impact on the UK's economy and society. Moreover, UK citizens will benefit from better use of personal data, which will deliver a stronger economy, more efficient and effective public services, and greater innovation in science and technology.

This aim is completely consistent with both EU GDPR and UK GDPR. Recital 4 in both texts states very clearly the overall aims and ambitions of a balanced data protection regime: **“The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights** and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, **freedom to conduct a business**, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.”

Internationally the DMA are strong advocates for harmonisation of worldwide data protection legislative regimes based on a set of common principles to facilitate free flows of data internationally. The Global Data and Marketing Alliance, representing over forty individual DMAs on four continents has agreed to a set of Global Privacy Principles designed to create consistency globally and recognise the rich variety of cultural and legal systems in different countries. The GDMA Global Privacy Principles establish a worldwide framework for customer communication that should underpin all legal and commercial approaches. They are designed as an instrument of best practice and are intended as a guide for self-regulation and legislation. These principles should sit at the heart of future UK adequacy decisions.

In summary, new technologies and the use of personal data provide humanity with the opportunity to live better, consume better, and be more sustainable. Data has an ever-increasing role to play for business innovation, scientific research, medical research and economic growth. The benefits of data for society and the economy can only be achieved through its ethical use and by generating trust between individuals and organisations. Privacy and data protection rules both contribute to the creation of trust, while providing a framework for responsible flows of information. The DMA welcomes the government’s approach in maintaining a high level of data protection and support some of the suggestions that will create greater clarity and certainty for organisations and people.

1. Chapter 1.4: Availability and use of legitimate interests

(consultation pages 21 – 23, Q1.4.1, 1.4.2, 1.4.3, 1.4.4)

DMA members strongly support the consultation hypothesis that “uncertainty may have caused an over-reliance on consent” and agreed that many companies had shied away from using legitimate interests where appropriate because “using legitimate interests for lawful processing is more complicated and riskier than other grounds”. Members shared examples where uncertainty has caused activity to be cancelled thus reducing revenue opportunities and innovation.

In some circumstances asking customers for consent (which must be specific and informed) could be a burden on consumers requiring the average person to review

and understand complex data processing activity without specific understanding or knowledge. The alternative of using legitimate interests in appropriate circumstances ensures that the controller takes greater responsibility for the way data is used and that the processing has reasoning documented behind it. Using their legal right to object maintains consumer control over what communication they receive, whether that be specifically using an email unsubscribe, notifying the company, or registering with an industry level opt-out file such as the Mailing Preference Service and the Telephone Preference Service.

The need for every business to conduct an LIA balancing test for processing that is standard across every company and where the risk of harm to customers is minimal consumes resources when the balancing tests could be conducted at an industry level on behalf of all organisations. Much of the behind-the-scenes processing that is necessary to run a business effectively are standard practice whether that be normal data hygiene to ensure data is up to date or cross-referencing bereavement files, Mailing Preference Service files or Telephone Preference Service files.

The granular specificity required for consent as a basis of processing means that many different consents would be required simply to ensure a company was communicating about products and services that were relevant to each of their customers. Our research into consumer attitudes to privacy consistently shows that receiving offers for products that are relevant is the preferred experience for customers. Using legitimate interests lets people know what their data will be used for while keeping the responsibility and onus of proportionate data processing on the shoulders of the data controller, because the controller must be able to justify the processing activities at all times. Customers retain an unfettered right to object to marketing messages at any time providing them a significant level of protection from harm.

For these reasons the DMA strongly supports the proposal to create a limited but exhaustive list defining where legitimate interests could be used and believes that in accordance with Recital 47 some direct marketing should be included. We believe strongly that Recital 47 must be one of the recitals that is brought into the main text to give it greater legal effect.

If direct marketing is added to the limited but exhaustive list then the DMA would support language along the lines of the Singapore business improvement exception:

- To improve, enhance or develop goods or services provided by the organisation, or methods or processes for the operations of the organisation.
- To learn about and understand the behaviour and preferences of customers in relation to the goods services provided by the organisation or to identify goods or services provided by the organisation that may be suitable for the organisation's customers other than individual customers.

It is important to note that our members see using legitimate interests as ensuring companies take greater responsibility rather than less. As such, the proposals in clause 60 that say “without applying the balancing test” might be amended to “where a balancing test is discretionary” to ensure that companies continue to take responsibility for their decisions. When using legitimate interests a high degree of consumer protection is retained through legally required opportunities to object to marketing messages on a company specific and industry level. Many instances would remain in the legislation where consent is still required, and many companies will voluntarily choose consent even when it is not a legal requirement and may still choose to conduct discretionary balancing tests.

2. Chapter 1.5: AI and Machine learning

(pages 37 to 41 of the consultation)

AI and machine learning are used by marketers to gain insight into their customers and make suggestions for products or services that are relevant to their interests. This takes many forms from Netflix recommending which film you might like to watch, to retailers recommending products that are similar to products that you have purchased previously, to grocery stores offering savings on foods and household items a customer buys frequently, to airlines offering airmiles that can be redeemed for free trips. All these examples could not be managed effectively and efficiently for the benefit of customers without the use of AI to analyse information and make suggestions in a timely manner. It is therefore crucial that throughout this section the government makes clear the distinction between activities that benefit citizens in making day to day decisions on what to buy from those decisions that have a significant legal effect.

This is particularly true when considering Article 22 in Q1.5.14, 1.5.15, 1.5.16 and 1.5.17. The DMA does not support removing Article 22 completely, but it is extremely important to have greater clarity on what becomes a “legal effects or similarly significant effects”. Members distinguished clearly between understanding customer preferences to offer appropriate products and services, which does not create a legal effect and has a low risk of causing harm, from automated decisions such as a mortgage loan approval which could have a legal effect and for which we support the right to a human review.

The DMA is also extremely supportive of all suggestions to ensure fairness and eliminating bias in algorithms. We therefore support the suggestions in Q1.5.10, 1.5.11 and 1.5.12 but with appropriate safeguards to ensure that the usage is limited to bias monitoring only.

3. Chapter 1: Innovative Data Sharing Solutions

(chapter 1.7, pages 47-52)

Personal Data Mobility (PDM) will play a critical role unlocking data’s value. The UK can make PDM a reality for millions of citizens in the same way centralised services made the digital world accessible 20 years ago with proper engagement, oversight, shared standards and legitimate intermediaries. This will bring an economic stimulus at least equivalent, and likely to surpass the last age of the web in scale. By its own research commissioned through CTRL Shift, DCMS has recognised data mobility as an opportunity to realise productivity and competition benefits it estimates would add £27 Billion to UK GDP.

However, while GDPR established individual data portability rights and created a firm legal basis, it did not create the structures necessary to support a New Data Economy based on value generation from personal data. This creates a space for innovative data sharing solutions which replace individual responsibility (and risk) with collective agency and bargaining power.

The DMA believes practical data stewardship in the form of trusts or unions such as Pool Foundation, together with a lightweight data licensing framework, upgrading of access rights and continuing education can meet the needs of all stakeholders, accelerate the UK's National Data Strategy and unlock the potential of current regulations such as GDPR and DPA 2018.

With regards to Q1.71, GDPR establishes data portability rights of the individual over their personal data but did not create the structures to support mobility and value generation from its use. Leaving it to the market to create solutions has led to lack of adoption for new entrants, while relying on market leaders risks further centralisation of data, power and revenue, with associated risk and competition issues.

Gaining the engagement and trust of all key stakeholders will play a critical role in creating new data intermediaries and the development of Personal Data Mobility. We believe this requires strong coordination and support from the government, in line with similar initiatives and funding seen in the US and Europe.

The needs of data intermediaries in this area can be summarised as follows:

1. Education and promotion as part of digital literacy initiatives
2. Regulation, standards and certification
3. Light touch, proportionate licencing for data
4. Funding & Tech resources (sandboxes, API's)

The DMA believe this is best achieved through an alliance of intermediaries, external tech providers and representation from data buyers.

While the analogy of open banking is useful, this needs to remain inclusive; previous schemes such as the Information Commissioner's Office (ICO) sandbox had a narrow technical remit, focused on a small ecosystem of suppliers helping large data controllers meet their regulatory obligations.

A sandbox is part of a successful Personal Data Mobility strategy but needs to be integrated with a ground-up, accessible set of standards and open access to existing and nascent intermediaries such as data unions, if current silos are to be broken down.

Similarly, there needs to be a focus not just on preservation of rights but an upgrading of data portability rules in the form of a practical code around which data intermediaries can build their own services, and API access privileges to data in real time.

In answer to Q1.72 the DMA believe that in the context of direct marketing, where automated profiling of data relating to an individual does not lead to significant/legal effects, this should be added to the cases where legitimate interests are used as legal basis for processing by Data Unions and other intermediaries.

Similarly, in the context just outlined, the DMA recommend there should be no requirements to apply a legitimate interest balancing test, though this could be built

into the process design for other use cases. This would lend itself well to automation, and an audit trail created using smart contracts and other blockchain technologies.

Combined with a Code of Conduct to which intermediaries such as Data Unions contribute and adhere to (similar to the DMA Code and Responsible Marketing Policy), the following outcomes could be achieved.

- Individuals who wish to join a Data Union have a clear understanding of the terms under which their data is processed.
- Data Union Operators can sign up individuals and offer ‘data clearing services’ as outlined in section 129 of the DCMS document, using legitimate interests as the default legal basis.
- Responsible Data Union Operators can create both products for buyers and a raw layer of data for data scientists to query.

In this context the Personal Data Vault has a dual purpose; master record of an individual’s data, preferences and union memberships over which they wield sovereign control, and a more granular, informed successor to the web cookie model by which digital services are still largely accessed today.

4. Chapter 2: Reform of the Accountability Framework

(pages 53 to 72 of the consultation, Q2.2.1 to Q2.3.5)

The DMA does **not** support the government proposals to replace the current accountability framework with a new Privacy Management Programme. Members believe strongly that the overall effect of the current regime and the new proposals are essentially similar, describing the proposals as “replacing apples with apples”. The change to the current accountability regime would therefore create unnecessary confusion and uncertainty for little benefit.

In considering clauses 160 to 164 members could understand that the proposed changes to the need for independence of DPOs could be useful for SMEs, but broadly **support maintaining DPOs**. The current role of DPOs is considered appropriate and useful.

In considering clauses 165 to 169 and 174 to 176, our members believe strongly that **DPIAs and Records of Processing Activity (RoPA) are essential tools** that improve business outcomes, although they feel that flexibility around what these looked like would be useful.

Members did not see the point of removing the need for **prior consultation** with the ICO prior to undertaking risky activity as proposed in clauses 170 to 173, but nor did they really see the point of maintaining it. The view was that if the appropriate balancing tests were implemented by an organisation, such as Privacy by Design and DPIAs then mitigation would take place to reduce the risk without the need to consult the ICO, including the possibility that the activity would be shelved

altogether if the assessments identified considerable risk to customers. In short, members do not see the current obligations as an onerous burden because they were unlikely to use it.

Regarding clauses 178 to 183 changing the threshold for **breach reporting** members did feel that greater clarity would be useful, especially for SMEs. They believed that larger organisations that deal with the ICO regularly are usually only reporting when a significant threshold is achieved.

5. Chapter 2: Subject Access Requests

(Pages 69-72)

Members did not support implementing a fee for **subject access requests** as proposed in clauses 185 to 189. They believed that if a company has implemented an appropriate privacy by design regime and a complete commitment to the accountability framework then responding to SARs should be considered part of the customer experience.

6. Chapter 2: Privacy and Electronic Communications

(pages 72 to 84 covering Q2.4.1 to Q2.4.18)

The DMA agrees with almost all of the proposals in this section. In considering our response it is important to note that members clearly distinguish between first party cookies which govern a website's own interactions (whether that is strictly necessary, analytics or serving existing customer) and cookies that enable third party data sharing or cross website tracking which inherently reduce the control and security of the data. Our members support those changes which recognise an organisation's legitimate interests in creating a top-quality customer experience and understanding their existing customers to serve them better. Our overall approach extends from our response to the issues of cookies, email soft opt-in and telephone proposals.

Regarding clauses 194 to 205 concerning the use of cookies, members strongly support the proposals to permit organisations to use analytics and strictly necessary cookies without consent but with legitimate interests as a basis. In this regard, we agree with clause 199 and the French example which limits the scope to first party relationships such as single website or application. As noted, this may enable some understanding of preferences in clusters that would help meet the consumer's expectations of relevance and recommendations. All research in the arena of customer attitudes to privacy validates that consumers appreciate recommendations for products and services based on their purchase history with a single organisation, whether that be recommendations of films to watch from Netflix, recommendations for offers on food purchases, recommendations for opportunities to use air miles and other loyalty points, and personalisation of pages on the website and even reminders that potential purchases remain in the shopping cart. In a first party relationship an organisation becomes more knowledgeable about its long-term

customers over time to serve them better. They achieve this through observing purchase history as well as individual behaviour on the organisation's own website.

In a first party relationship an organisation becomes more knowledgeable about its long-term customers over time to serve them better. They achieve this through observing purchase history as well as individual behaviour on the organisation's own website. First party cookies in which the data is only ever used by the company who has the relationship with the customer, and is never shared outside the organisation, should be able to be used in this context in a similar way to analytics and strictly necessary cookies. The only purpose of first party cookies is to improve the customer's experience by making its own website pages more relevant. First party tracking can be differentiated from 3rd party tracking by the degree of control that the website owner has over the use of the data that is being collected. With first party tracking, the website owner is the controller of the data and therefore, is bound by law to be responsible for the security of any personal information as well as being able to protect an individual's privacy rights. This recommendation would make it possible for organisations who use this type of "controlled" tracking, to remove the "cookie" consent banners from websites, but still use low risk personal information, to make the website users experience more relevant and enjoyable.

The DMA does believe that third party cookies for cross website tracking and retargeting of online advertising exposes the customer to a higher level of risk. Eventually a replacement for third party tracking cookies may be devised that would potentially use aggregated, anonymous clusters or contextual advertising solutions. The important experience for customers is that the advertising they see from companies they do not know should be relevant to their needs, wants and budgets. But the creation of relevance does not necessarily mean using personal data to do so. It is very possible that contextual solutions that use the content of web pages combined with publisher first party data could create an adequate level of understanding to make an advertising decision without using personal data. In other words, it might be possible to assume that all the people visiting a particular page of a website to access specific content would be interested in products related to that content.

The DMA strongly supports the proposal in clause 210 (Q2.4.9) to extend the soft opt-in for electronic communications to other organisations as a result of membership or subscription. It is clear the donors to a charity often have an extremely emotional connection to a cause they are supporting, whether that be saving children, animals, cancer care or a myriad of good causes. Maintaining a relationship between the charity and the individual would be valued by the individual provided that the communications met their reasonable expectations and that an opt-out was always available so the data subject could exercise their right to stop receiving communication.

Proposals regarding Nuisance and Fraudulent calls are made in clauses 212 to 215 and Q2.4.10 – Q2.4.18. The DMA brings extensive expertise to this section of the consultation through our role operating the Telephone Preference Service under contract with the ICO. The DMA has a long history of supporting investigations and prosecutions of rogue callers brought by the ICO, trading standards and other bodies, often acting as witnesses in court in addition to submitting written evidence.

As a result, we strongly support any measures that would provide citizens with greater protection from rogue callers and facilitate investigations and fines.

The DMA strongly supports Q2.4.10. The benefits of updating the ICO's enforcement powers so that they can take stronger action against organisations for the number of unsolicited direct marketing calls 'sent' are clear, the rogue companies ignoring the legislation would receive fines or enforcement action proportionate to the number of nuisance calls made. This would certainly act as a deterrent to making large volumes of calls and punish the worst offenders.

There is a risk that it might be difficult to accurately identify the number of calls 'connected' although this information may be available from the company making the calls as this information is often recorded in the system use for dialling the numbers and storing data (a dialler). This information could also be retrieved from the offending companies' communication service provider.

The DMA supports a duty to report in Q2.4.11. The organisations with the most information about the nature of calls being made on a network are the communication service providers. The DMA is aware of service providers that can easily identify suspicious activity on their networks but currently have no authority to do anything about it. The service providers are currently benefiting from the revenue made from all the nuisance calls that are connected, it is not unreasonable therefore to introduce a 'duty to report'. There is a small risk that legitimate businesses might be incorrectly identified as nuisance callers, but legitimate organisations should be able to respond quickly to the ICO before any action is taken or the communication provider suspends their service.

Regarding 2.4.12 and 2.4.13, more responsibility should be given to the communication service providers to prevent nuisance calls and texts. These organisations have wealth of information about the calls being made and can spot suspicious activity. They also benefit financially from all the nuisance calls and texts that are delivered. Currently there is not much incentive for them to prevent these from being made. With support from communications providers 'duty to report' there would be no requirement for further legislation.

Regarding 2.4.14, the benefits of mandating communications providers to do more to block calls and text messages at source are that the communications providers have access to real time information and the ability to identify suspicious activity. There is a small risk that legitimate businesses might be temporarily affected by the blocking.

Regarding 2.4.15, the technology to block incoming calls from numbers not on an 'allow list' is already available on certain telephone handsets and mobile phones. The benefit is that a person only receives calls from a trusted list of numbers. There is a risk that a person might not receive an important call from someone calling from a new or different phone, also some public bodies that offer personal or confidential services such as GP's and support services may not be able to get through.

The DMA strongly agrees with Q2.4.16 that increasing fines that can be imposed under PECR so they are the same level as fines imposed under the UK GDPR. It seems sensible that fines for contravening data protection legislation should be the same whether it is UK GDR or PECR.

The DMA strongly agrees with allowing the ICO to impose assessment notices on organisations suspected of infringements of PECR to allow them to carry out audits of the organisation's processing activities as proposed in Q2.4.17. For many companies that handle and process large volumes of data audits are a common occurrence. ISO standards require onsite audits, and often clients will conduct their own audits of their processors. If a company cannot demonstrate to the ICO that their activity is compliant by any other means, then an on-site audit should be something that they can insist on.

Regarding 2.4.18, the requirement for the ICO to demonstrate 'significant damage or distress' was removed from PECR for calls and texts because each individual call was unable to reach this threshold. Since this was changed the ICO have been very effective in its PECR enforcement. However, this clause was not removed for Cookies and therefore it would be almost impossible to make a successful case against a company that was using cookies illegally. The 'significant damage or distress' clause should be removed from all aspects of PECR.

In addition to supporting the proposals in 2.4.16 to 2.4.18, the DMA believes that consolidating PECR, UK GDPR and Data Protection Act 2018 will remove inconsistencies and provide clarity across the three texts. This is covered later in this response as a supplemental issue.

7. Chapter 2: Sectoral Codes

(clause 201 and Q2.4.5)

The DMA **very strongly supports** sectoral codes of conduct under Article 40 and Industry Monitoring Bodies under clause 41 of UK GDPR. We have long been working with the ICO on a direct marketing code of conduct that would identify the legitimate interests of controllers and develop industry level mitigation to reduce risks to the customer, whether that be an opt-out service such as the Telephone Preference Service and Mail Preference Service or perhaps a registry of third party data providers who have been audited and proven to be compliant and safe. The process of Code approval is cumbersome, bureaucratic and process driven despite the ICO's public support of sector codes.

Article 40 specifies the role of Codes of Conduct as follows: **Associations and other bodies representing categories of controllers or processors may prepare codes of conduct for the purpose of specifying the application of this Regulation, such as with regard to:**

- a) fair and transparent processing;
- b) the legitimate interests pursued by controllers in specific contexts;
- c) the collection of personal data;

- d) the pseudonymisation of personal data;
- e) the information provided to the public and to data subjects;
- f) the exercise of the rights of data subjects;
- g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32
- i) the notification of personal data breaches to supervisory authorities the Commissioner and the communication of such personal data breaches to data subjects;
- j) the transfer of personal data to third countries or international organisations; or
- k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

The DMA believes that industry codes of conduct are a critical component of finding the right balance between innovation and privacy in a modern economy. It is only industry experts who understand the specific processing that takes place in a sector who can properly assess how those processes should be conducted to ensure maximum safety to people while organisations seeking innovation, growth and job creation can pursue their legitimate interests.

The role of an industry code of conduct should be focussed specifically to provide guidance on the application of legitimate interests in a sector, and to specify where consent or another basis are required. In every sector of the economy, similar data processing takes place that is common to all organisations operating in sectors with similar business models. Making greater use of industry codes for all sectors of the economy will provide certainty and clarity in support of the legislation. In particular, the DMA believes that sector codes of conduct should be a supplemental requirement to any activity that is added to the limited, but exhaustive list of legitimate interests that is proposed. The codes of conduct would mitigate any risks that might be created when a balancing test is not required for use of legitimate interests and in detail demonstrate how that legitimate interest should be carried out safely. Industry codes of conduct can provide industry level balancing tests where the processing is replicated by many companies, which would serve to give greater confidence to any activity included in the list.

Whereas UK GDPR specifies the expertise of industry experts and establishes a critical role for industry codes of conduct and industry monitoring bodies in Articles 40 and 41, the Data Protection Act of 2018 requires the ICO to produce industry codes of practice for sectors such as direct marketing in which they have little

8. Chapter 2: Use of personal data for democratic engagement

(clauses 219-228)

The DMA has always believed that data protection legislation should apply equally to all organisations that engage in direct communication with their audiences. We therefore believe strongly that PECR's rules of direct marketing should apply to political organisations in the same way that they apply to businesses. In principle we support the extension of the soft opt-in to all types of organisations as we have said in our previous response in terms of extending soft opt-in to other types of organisations (Q2.4.9).

However, we would draw attention to the requirements in UK GDPR around the use of sensitive personal data and note that political issues often cover areas of great passion and are very personal. The nature of some issues such as health and gender are protected characteristics. Political parties should take great care when they use characteristics that are sensitive and protected. Although paragraph 227 notes that an exception exists in the requirement of consent for processing sensitive data for political organisations, the DMA believes that political organisations should be very cautious when relying on this exception.

The DMA's general view remains that the rules of UK GDPR, PECR and UK Data Protection Act 2018 should generally apply equally to all types of organisation.

9. Chapter 3: Boosting trade and reducing barriers to data flows

The DMA are strong advocates for harmonisation of data protection legislative regimes worldwide based on common principles to facilitate free flows of data internationally. The Global Data and Marketing Alliance, representing over forty individual DMAs on four continents, has agreed a set of Global Privacy Principles (Appendix 2) designed to create consistency despite the rich variety of cultural and legal systems that exist globally.

The GDMA Global Privacy Principles establish a worldwide framework for customer communication that should underpin all legal and commercial approaches. They are designed as an instrument of best practice and are intended as a guide for both self-regulation and legislation. These principles should sit at the heart of future UK adequacy decisions and for this reason the DMA strongly supports Q3.21 that UK's future approach to adequacy decisions should be risk-based and focussed on outcomes. The DMA also strongly supports Q3.22 and Q3.23 for the same reasons.

In magnitude of importance, international data transfers with the EU governed by reciprocal EU/UK adequacy decisions are the most critical to DMA members both from the perspective of data transfers and market access. If adequacy with the EU is lost larger organisations would most likely be able to work around it with Standard

Contract Clauses and Binding Corporate Rules but SMEs would be greatly disadvantaged.

All of the proposals that the DMA supports in this consultation are not viewed as being a risk to data adequacy. In particular, the proposals that relate to legitimate interests should not pose a risk to adequacy given the long history of support for legitimate interests in the EU including Court of Justice rulings in cases such as Fashion ID.

Some of the proposals that the DMA does not support, such as removal of Data Protection Impact Assessments from the accountability framework, removing Article 22 completely and reducing the ICO's independence could be triggers for the EU to review adequacy.

Regarding the additional proposals in Chapter 3, the DMA strongly supports 3.2.4, 3.3.1, 3.3.3, 3.3.4, 3.3.6, and 3.3.7.

Regarding certification schemes, the UK believes strongly in the role of sector codes of conduct under Articles 40 and 41 of GDPR and believe that an industry sector code of conduct would be the best way to ensure international certifications for a sector such as direct marketing. An industry association through its international network, such as the GDMA network, could provide an appropriate method for certifying overseas organisations as compliant through local audits and certifications. This is one of the critical roles envisaged in UK GDPR for industry sector codes of conduct. The DMA therefore supports the proposals in 3.4.1, 3.4.2, and 3.4.3.

10. Chapter 5: Reform of the Information Commissioner's Office

(pages 113-143)

5.2 Strategy, Objectives and Duties

The DMA supports the proposals in 5.2.1, 5.2.2, 5.2.3, 5.2.5, 5.2.6, 5.2.7, 5.2.10, 5.2.12, and 5.2.13.

The DMA strongly supports 5.2.4 and believes it is one of the most important proposals in the consultation.

On 5.2.7 the DMA agrees with the requirement to liaise with existing regulators but would recommend that the ICO's duty to cooperate and consult should also apply to self-regulators such as the Data and Marketing Commission, MRS and other relevant self-regulators such as the Advertising Standards Authority (ASA). The Data and Marketing Association has a strong existing relationship with the ICO, and we believe

it would be beneficial that non-statutory regulators are recognised to ensure that regulation is agile and supports the various sector self-regulatory systems which will apply data regulation to specific professions and disciplines.

5.3 Governance Model and Leadership

The DMA supports these proposals generally.

More specifically we support 5.3.1, 5.3.2, 5.3.3 and 5.3.4.

The DMA does not support Q5.3.5 as it removes some of the independence of the ICO and could create an outcome in which the ICO deferred to DCMS on critical issues to protect their compensation. However, we note that the ICO's salary should be competitive and appropriate for the level of skills that are required to perform a highly complex role.

5.4 Accountability and Transparency

The DMA supports greater accountability and transparency in the ICO's KPIs and therefore supports Q5.4.1, 5.4.2, and 5.4.3.

Some of the KPIs must be focussed on operational efficiency and especially the speed of response. Despite significant increases in manpower in recent years the ICO has become slower, more bureaucratic and less timely in all responses, whether that be investigations, approvals of codes of conduct, consultation discussions and generally speaking all matters. The slow response times undermine the ICO's credibility in a fast-moving digital economy and threaten natural justice due to delays. This is another very strong reason the DMA supports sector codes of conduct which would enable the ICO to pass significant numbers of complaints to industry monitoring bodies under a rigorous co-regulation process.

The DMA is concerned that the proposals in Q5.4.6 would reduce the ICO's independence from political oversight and are concerned this would pose a risk to data adequacy with the EU

5.5 Codes of Practice and Guidance

The DMA have concerns about the role of industry codes of practice as specified in UK Data Protection Act 2018 which create confusion because the requirement for a direct marketing code of practice does not exist in UK GDPR. Rather, UK GDPR specifies the important role that sector codes of conduct play in the implementation of GDPR across various sectors of the economy and give authority to the role of trade associations to interpret the legitimate interests for their sector. As stated in our response to Q 2.4.5 the DMA believes strongly that industry codes of conduct are essential to bring specific industry expertise to implementation of UK GDPR.

The proposals made concerning chapter 5 section 5.5 clearly recognise that the ICO does not have the required sector expertise to produce industry codes of practice

because they lack the specific industry knowledge required. Clause 378 states: “As the ICO is a cross-sector regulator, a broad and transparent consultation process could improve the ICO’s understanding of how legislation should apply to different sectors and data use cases”

Clause 379 proposes “to introduce a power for the DCMS Secretary of State to require the ICO to set up a panel of persons with relevant expertise when developing codes of practice, and complex or novel guidance”. These proposals recognise what has already been recognised in Articles 40 and 41 of GDPR: that sector specific interpretation should reside with the appropriate expertise of industry trade associations. Crucially, Article 40 states: “Associations and other bodies representing categories of controllers or processors may prepare codes of conduct for the purpose of specifying the application of this Regulation”

Although the DMA supports the recommendations in clauses 378 and 379, we do not believe they should be necessary. If industry codes of conduct were approved under the criteria established in UK GDPR there would be no need for the ICO to develop separate codes of practice under Data Protection Act 2018. A reconciliation of Data Protection Act 2018 with UK GDPR should remove the requirement for the ICO to develop a direct marketing code of practice and prioritise the development and approval of a direct marketing code of conduct and industry monitoring body as called for in Articles 40 and 41 of GDPR.

The legislation should mandate that the ICO accelerates approval of industry codes of conduct and works closely with industry practitioners to determine how UK GDPR should be applied in each sector of the economy.

5.6 Complaints

The DMA believes that the solution to the issues raised in section 5.6 is the approval of sector codes and industry monitoring bodies under Articles 40 and 41 of UK GDPR. This would free the ICO to focus its investigatory resources on the wider systemic issues that risk significant harms to large numbers of citizens. The appropriate solution is to encourage the ICO to accelerate the process of approving sector codes and to focus on the outcomes and policies contained in a sector code rather than creating delays driven by process and bureaucracy. We do not disagree with any of the proposals in 5.6.1, 5.6.2, 5.6.3 and 5.6.4 but we also believe they are unnecessary if the right energy and resources are allocated to establishing industry codes of conduct across many sectors.

5.7 Enforcement Powers

The DMA supports the proposals in this section generally and agrees with 5.7.1. We also have no objections to 5.7.2, 5.7.5, and 5.7.6.

A critical issue that our members raise regarding ICO investigations is that there is frequently no change between the Notice of Intent and Final Penalty Notice. The perception widely exists that the ICO investigators ignore the responses made by organisations. We therefore strongly support any changes that compel the ICO to

pay careful attention to written recommendations and oral representations. In some cases, a company may require more than 28 days to properly respond to a Notice of Intent and therefore we strongly support 5.7.7, 5.7.8 and 5.7.9

11. Supplemental topic: Notification requirements under Article 14 of UK GDPR

Article 14 of GDPR specifies “Information to be provided where personal data have not been obtained from the data subject”.

This generally applies to publicly available data sources such as Companies House, Edited Electoral Roll, and Bereavement files which are used by organisations for purposes such as data hygiene, address verification, debt collection, fraud prevention and removing people who have passed away from marketing messages. This data is often used to supplement or verify first party data held by organisations about their customers, members, or donors to deliver more accurate and relevant communications and to make better business decision. Better, more informed decisions contribute to innovation and growth.

The DMA supports the aims and ambitions of Article 14. While the DMA believes that a significant amount of processing that uses publicly available information is based for the legitimate interest of the business especially for operational processing required to fulfil data hygiene obligations and support debt collection, the same publicly available data may sometimes be used to inform marketing decisions and to send marketing messages. In these instances, the requirement for transparency is essential for the individual to exercise control of their data and their right to object to marketing messages.

However, the requirement to inform millions of people personally by post, telephone or email every time any company is planning to use data from publicly available sources results in two significant adverse effects, one on people and the other on organisations.

The negative impact on people will be significant. Under the requirements of Article 14 it is possible that every person will receive hundreds of messages from companies they have no relationship with letting them know they have acquired their personal data from a specific publicly available source. This would create a situation for individuals that is more intrusive and harmful than cookie banners, with a barrage of messages for each data source and every organisation using the data.

For organisations the notification requirement creates disproportionate effort and cost which could render use of the data unviable economically or even encourage organisations to bypass the notification process using the exception in Article 14.5.b. As such, consumers would either not be able to exercise their rights or significant amounts of data that support innovation and growth would cease to flow through the economy.

Industry level solutions to fulfilling the transparency requirements for sending marketing messages have been developed by industry trade associations and approved by Data Protection Authorities across the EU, solutions that would enable individuals to exercise their data protection rights and avoid receiving a bombardment of notification messages. Examples are contained within the DMVOE Code of Conduct in Austria, the SMB Code of Conduct in Poland and the ANCIC Code of Conduct in Italy, all of which have been approved by their respective Data Protection Authority as compliant with EU GDPR. There is no reason similar solutions would not be compliant with UK GDPR.

These DPA approved solutions set out best practice for using publicly available data combined with an audit process conducted by the industry monitoring body to verify that the data provider is fully compliant with the code of conduct requirements, resulting in issuing a seal of approval. The Code owner then compiles and manages a list of all approved data providers including the complete information required in Article 14.1 and 14.2. This registry is then made available to individuals via the code owner website to research how, when and why their personal data has been collected. Critically, if they object to the use of their data by the data provider they register opt-out from the data provider's list.

The DMVOE Code of Conduct in Austria goes further: the DMVOE assigns a number to each audited data provider and requires this number to be included in any marketing communication that uses personal data provided by that data owner. A simple statement within each marketing message would say "you are receiving this message as a result of data provided by yyy company". The individual receiving the marketing message is then able to go to the code owner website, look up data provider yyy and register their objection if they wished to opt out from any future marketing messages.

The use of this type of system provides the transparency and control that enables individuals to exercise their rights without being bombarded with hundreds of messages notifying them their data is being used. Importantly, the notification takes place in the context of a specific marketing message making the notification relevant and giving individuals an easy method to exercise their right to object. Additionally, such a system provides a proportionate and cost-effective way for data providers to fulfil their obligations.

The DMA is therefore proposing an amendment to the text of Article 14 to specify clearly that such a system, developed and run under the auspices of an approved sector Code of Conduct and Industry Monitoring body, would adequately fulfil the requirements of Article 14 in the context of marketing messages. The DMA proposes that adding a new clause 'd' to Article 14.3 stating "The notification may take place through a publicly available registry of verified data providers via a public website operated by the code owner of an industry code of conduct as specified in Articles 40 of UK GDPR. Such a code of conduct must be reviewed and approved by the ICO as specified in the legislation. Such approval must not be unreasonably withheld or delayed by the ICO"

The DMA further proposes amending Article 14.4 to remove the word "prior"

12. Supplemental topic: simplifying the legislative framework

As previously discussed, the confusion created between industry codes of conduct specified in UK GDPR and ICO codes of practice specified in Data Protection Act 2018 is just one example of confusion created by having multiple legislative vehicles for the same subject.

In the consultation document the government refers variously to at least three different legislative vehicles, all of which are long and complicated: UK GDPR, Data Protection Act 2018 and Privacy and Electronic Communications Regulation (PECR).

This preponderance of legislation covering the same or similar topics is extremely confusing and time consuming for all organisations, especially when there are contradictions between the texts. Even the largest organisations with significant manpower and resources in their legal and compliance teams struggle with the confusion and contradictions involved. SMEs have no chance whatsoever to navigate this legislative complexity.

The DMA therefore suggests that the government strongly consider consolidating the various texts into a single Data Protection Act 2022 which reconciles contradictions, simplifies and shortens the legislation. This is critical if the aims of unleashing innovation and reducing burdens on business are to be achieved.

/ Appendix 1: DMA Code



/ Introduction

The DMA Code sets the standard of conduct for the industry and is the code to which all DMA members must adhere, in addition to all legal requirements.

But the Code is much, much greater than just a rulebook: It stands as an agreement between you, the DMA and your fellow members to serve each customer with fairness and respect and, in consequence, to cultivate a profitable and successful commercial ecosystem.

Under the hero principle **Put your customer first**, the Code promotes the evolution of marketing as an exchange of value between your business, looking to prosper, and your customer, looking to benefit.

The DMA is committed to helping you put your customer at the heart of everything you do, in order that your business can prosperously grow to be enjoyed, prized and ultimately sustained by your market.

Putting your customer first



Data & Marketing Association

4

/ Putting your customer first

Value your customer, understand their needs and offer relevant products and services

Outcomes

Customers receive a positive and transparent experience throughout their association with a company.

Customers receive marketing information that is relevant to them and reflects their preferences.

Customers receive prompt, efficient and courteous service.

- / Respect privacy
- / Be honest and fair
- / Be diligent with data
- / Take responsibility

Data & Marketing Association

5

Respect privacy



Data & Marketing Association

6

/ Respect privacy

Act in accordance with your customer's expectations

Outcomes

Customers have a clear understanding of the value exchange when sharing personal information.

Companies are open, honest and transparent upfront about why they are collecting data and how they intend to use it.

Companies are sensitive to their customers and avoid marketing that is intrusive or excessive.

Companies recognise vulnerable customers and market to them responsibly.

Rules

- | | |
|---|---|
| <p>1.1 Members must not send or instigate the sending of direct marketing or process personal data for marketing, unless they comply with the Data Protection Act 2018 and all other associated legislation.</p> <p>1.2 Members must operate and maintain an in-house suppression file –including the least amount of contact detail to identify consumers who have indicated they do not wish to receive commercial communications via all or particular channels.</p> <p>This includes receivers of third-party communications who have indicated at the first contact that they do not want to receive further communications.</p> <p>1.3 Members must ensure that lists containing names and contact details are not used for marketing purposes unless the list has been cleaned against the relevant preference services – TPS, MPS, CTPS, BMPS, Facsimile Preference Service, Fundraising Preference Service and Your Choice.</p> | <p>1.4 Members must take all reasonable steps to ensure consumers do not receive commercial telephone calls or SMS messages at times considered to be antisocial.</p> <p>Members must consider their target audience when scheduling the delivery of commercial communications.</p> <p>1.5 Members must screen data to remove files of deceased people so that they are not used for marketing.</p> <p>1.6 Members must not undertake random number or sequential dialling, whether manually or by computer, or any number scanning activities (any activity designed to establish the validity of telephone numbers).</p> |
|---|---|

Data & Marketing Association

7



Be honest and fair

/ Be honest and fair

Be honest, fair and transparent throughout your business

Outcomes

Companies are clear, open and transparent.

Companies explain in plain terms what data they are collecting, why it is useful to them, the benefit to the customer of providing their personal data and how the company will be a good steward of that data while it is in their control.

Rules

2.1 Companies must not mislead customers, whether through omission, exaggeration or other means; companies must be clear and transparent.

2.2 Members must not exploit the credulity, lack of knowledge or inexperience of any consumer – and take particular care when dealing with children and other vulnerable consumers.

2.3 Members must clearly identify the advertiser on any one-to-one marketing communication that they send or instigate

Members must provide caller line identification, to which a return call can be made, whenever they undertake any outbound calls either directly or through an outsourced supplier.

Members must provide a valid address on any marketing communication, through which the consumer can opt-out of future communications.

2.4 Members must not send goods or provide services for which payment is requested to any consumer without first having received an instruction to supply such goods or services.


Members must not demand that any consumer either pay for or return unsolicited products, except for substitute products.

2.5 Members must not misrepresent themselves as carrying out research or a survey when the real purpose of the contact is to sell goods or services, or to solicit donations.

When members collect personal information for the purposes of research or a survey and also intend to use this information for any other purposes, such as to market to the consumer, they must make clear the purposes.

Members must not adopt high-pressure selling techniques in the course of any contact with any consumer or business.

Data & Marketing Association 8



Be diligent with data

/ Be diligent with data

Treat your customer's personal data with the utmost care and respect

Outcomes

Customers always know who is collecting their data, why it is being collected and what it will be used for.

All customer data held by companies is accurate, up to date and not held longer than necessary.

Companies always hold customers' data safely and securely.

Rules

3.1 When collecting personal data for marketing purposes, members must provide all the information required by the Data Protection Act 2018 and all other associated legislation, which includes their identity and details of the person ultimately responsible for customer data within their organisation and the basis under which the data will be processed.

3.2 Personal data should be:

- processed lawfully, fairly and in a transparent manner.
- collected for specific, explicit and legitimate purposes.
- adequate, relevant and limited to what is necessary for the purpose for which it has been collected.
- accurate and up to date and should not be kept for longer than necessary for the purpose for which it has been collected.
- processed in accordance with the rights of the consumer.
- protected using appropriate technical and organisational measures to ensure data is not processed unlawfully or without authority and is protected from accidental loss, destruction or damage.

3.3 Members must not use special category data for marketing purposes without the explicit consent of the consumer concerned.

3.4 When buying or renting personal data, members must carry out due diligence to satisfy themselves that the data has been properly sourced, permissioned and cleaned.

3.5 All processing undertaken by/for a third party (whether a data controller, data processor, or data sub processor), must be the subject of written instructions. The data controller must ensure that sufficient contractual protection is in place with all data processors and data sub-processors. Those contracts must protect the rights and freedoms of the data subjects concerned.

Data & Marketing Association 10



Take responsibility

/ Take responsibility

Act responsibly at all times and honour your accountability

Outcomes

Companies have the resources and systems in place to carry out agreed contracts.

Companies take responsibility for the entire customer experience, whether provided in-house or outsourced to a third party.

Companies take responsibility for their commitments and fix things if they go wrong.

Rules

4.1 Members must act decently, fairly and reasonably, fulfilling their contractual obligations at all times.

4.2 Members must ensure that they do nothing that could bring into disrepute the public image of one-to-one marketing or the DMA.

4.3 Members must accept that in the context of this Code they are normally responsible and accountable for any action (including the content of commercial communications) taken on their behalf by their staff, sales agents, agencies, marketing suppliers, sub-processors and others.

4.4 Members acting as an agency or supplier for a non-member's one-to-one marketing activity must advise the non-member to act within the Code. If the non-member client does not take that advice, the member must insist as a condition of acting for the non-member that the Code is followed in respect of all relevant work.

4.5 Where members sub-contract work to non-DMA members, they must ensure that the contractor complies with the Code in respect of the sub-contracted work – and must accept responsibility for the consequences of non-compliance by the contractor.

4.6 Members must maintain adequate records to demonstrate compliance with the Code – and must maintain an adequate system of monitoring and audit.

4.7 Members must ensure that they market in an environmentally sustainable way – and must have a documented environmental policy in place.

4.8 Members must at all times give prompt, efficient and courteous service to customers – and must ensure they have in place adequate administrative procedures and resources to achieve this.

4.9 Members must accept the jurisdiction of the Data & Marketing Commission (DMC) and co-operate fully with their investigations or enquiries.

Members must comply with any conclusion reached by the DMC, including any decision to take disciplinary action resulting from a breach of the Code.

4.10 Members must accept the right of the DMA to monitor compliance with the Code through an audit scheme, mystery shopping exercises or other activity – and to accept compliance visits.

As a result of these activities, the DMA may raise compliance issues with the member and take appropriate recommendations to prevent a possible breach of the Code.

Failure to accept such recommendations may result in a referral to the DMC for adjudication and, where such adjudication is negative, to sanctions for a breach of the Code.

Legislation and codes

Principal rules affecting data driven marketing

/ Legislation and codes

A number of laws and regulations must be followed when carrying out one-to-one marketing activities in the UK.

You can find up-to-date documents on legislation at www.legislation.gov.uk

<p>Core</p> <p>Business Protection from Misleading Marketing Regulations 2008</p> <p>Communications Act 2003</p> <p>Data Protection Act 2018</p> <p>Disability Discrimination Act 2005</p> <p>Electronic Communications Act 2000</p> <p>Electronic Commerce (EC Directive) Regulations 2002</p> <p>Gambling Act 2005</p> <p>Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended 2011)</p> <p>Representation of the People Act 2000</p> <p>Representation of the People (England and Wales) (Amendment) Regulations 2002</p> <p>Representation of the People (England and Wales) (Amendment) Regulations 2006</p> <p>Representation of the People (England and Wales) (Amendment) Regulations 2015</p> <p>Representation of the People (England and Wales) (Description of Electoral Registers and Amendment) Regulations 2013</p> <p>Charity</p> <p>Charities Act 1992</p> <p>Charities Act 2006</p> <p>Charities Act 2011</p> <p>Charities (Protection and Social Investment) Act 2016</p> <p>Consumer</p> <p>The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013</p> <p>Consumer Protection Act 1987</p>	<p>The Consumer Protection (Amendment) Regulations 2014</p> <p>Consumer Protection from Unfair Trading Regulations 2008</p> <p>The Consumer Rights Act 2015</p> <p>Consumer Rights (Payment Surcharges) Regulations 2012</p> <p>Enterprise Act 2002</p> <p>Fair Trading Act 1973</p> <p>Price Marking Order 2004</p> <p>Sale and Supply of Goods Act 1994</p> <p>Sale of Goods Act 1979</p> <p>Supply of Goods and Services Act 1982</p> <p>Trade Descriptions Act 1968</p> <p>Unfair Contract Terms Act 1977</p> <p>Unsolicited Goods and Services Act 1971</p> <p>Employment</p> <p>Conduct of Employment Agencies and Employment Business Regulations 2003 (as amended)</p> <p>National Minimum Wages Regulations 1999 (as amended)</p> <p>Working Time Regulations 1998 (as amended)</p> <p>Financial services</p> <p>Consumer Credit Act 1974 (as amended by the Consumer Credit Act 2006)</p> <p>Consumer Credit (Advertisement) Regulations 2010</p> <p>Consumer Credit (Agreements) Regulations 2010</p> <p>Consumer Credit (Amendment) Regulations 2010</p> <p>Industry codes of practice</p> <p>There are also several codes of practice that must be adhered to, the most important of which are:</p> <p>BCAP Code</p> <p>The UK Code of Broadcast Advertising</p> <p>CAP Code</p> <p>The UK Code of Non-broadcast Advertising and Direct & Promotional Marketing</p>	<p>Consumer Credit (Amendment) Regulations 2011</p> <p>Consumer Credit (Early Settlement) Regulations 2004 (as amended by Consumer Credit (Early Settlement) Regulations 2010)</p> <p>Consumer Credit (Disclosure of Information) Regulations 2010</p> <p>Consumer Credit (EU Directive) Regulations 2010</p> <p>Consumer Credit (Disclosure of Information) Regulations 2010</p> <p>Consumer Credit (Total Charge for Credit) Regulations 2010</p> <p>Consumer Credit (Total Charge for Credit) (Amendment) Regulations 2012</p> <p>Financial Services and Markets Act 2000</p> <p>Financial Services (Distance Marketing) Regulations 2004</p> <p>Intellectual property</p> <p>Copyright and Related Rights Regulations 2003</p> <p>Copyright Designs and Patents Act 1988</p> <p>Trademarks Act 1994</p> <p>Specialist</p> <p>Offensive Weapons Act 1996</p> <p>Theft Act 1978</p> <p>Telecommunications</p> <p>Regulation of Investigatory Powers Act 2000</p> <p>Telecommunications Act 1984</p> <p>Telecommunications Lawful Business Practice (Interception of Communications) Regulations 2000</p> <p>Regulators</p> <p>The regulators who enforce compliance with the DPA and PECR are:</p> <p>ICO</p> <p>The Information Commissioner's Office</p> <p>Ofcom</p> <p>The Office of Communications</p>
---	---	---

Copyright / DMA (2021)

25

Glossary

Data & Marketing Association

16

/ Glossary

Advertiser

Any person or company that initiates a commercial communication to promote its products, services or aims

BMPS

The Baby Mailing Preference Service

Client

An advertiser, or agency acting on the advertiser's behalf

The Code

This "Code" or "the Code" is the DMA Code of Practice 4th Edition

Commercial communication

Any communication that carries a marketing message including sales promotions, fundraising and all advertising

The Commission / DMC

The Data & Marketing Commission

Consumer

The potential or actual end user of a product or service

CTPS

The Corporate Telephone Preference Service

Customer

An individual who has made a purchase or who has entered into negotiations to purchase a product or service

Data

Information gathered or stored for analytical, decision-making or marketing purposes

Controller

A person or organisation involved in deciding how data is processed, stored or used

Processor

A person or organisation who collects, stores or deals with personal data on behalf of a data controller (including a list broker/manager)

Data processing

Collecting, storing, processing or using information including its destruction, transmission, sharing or other use

Direct marketing

Any marketing communication to an identified individual

DMA

Data & Marketing Association (UK) Ltd

European Economic Area (EEA)

The member states of the EU plus Norway, Iceland and Liechtenstein

FPS

The Facsimile Preference Service

Identifiable natural person

Someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Member

A company or organisation that has been accepted into, remains within and is bound by the terms and conditions of the DMA

MPS

The Mailing Preference Service
Number scanning activities
Any activity designed to establish the validity of telephone numbers

One-to-one marketing

Any marketing communication to an identified individual

PECR

Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended

Personal data

Information relating to an identified or identifiable natural person

Random number dialling

Randomly dialling to find valid phone numbers

Recipient

Any natural or legal person, including a sole trader or a partnership, who receives a commercial communication

Special categories of personal data

Personal data relating to 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.

Sequential dialling

Calling digits in numerical order to find valid phone numbers

SMS

Communication sent via a mobile handset using text, picture or video messaging

Suppression file

A list of individuals who have opted-out of all future marketing communications

Third party

Any person or organisation other than the advertiser (with the exception of data processors). This includes associated and/or affiliated companies

TPS

The Telephone Preference Service

Unsolicited commercial communication

Marketing to a consumer with whom the sender does not have an ongoing commercial or contractual relationship or where such direct marketing is otherwise uninvited

Vulnerable consumers

Includes, but not limited to, the elderly, people with disabilities and those for whom English is not their first language

Your Choice

A DMA scheme through which householders can register their wish to not receive unsolicited items to their home address from DMA members

Data & Marketing Association

17

The Data & Marketing Commission

Enforcing higher industry standards

Data & Marketing Association

18

/ The Data & Marketing Commission

About

The Data & Marketing Commission (DMC) is the body that oversees and enforces the DMA Code.

The DMC investigates and adjudicates on reported breaches of the Code by DMA members.

The DMC can also pass comment and recommendation to the DMA regarding particular aspects of the Code and the promotion of compliance.

The DMC may consult consumer enforcement and advisory services to ensure the relevance and effectiveness of the Code, as well as to help identify emerging consumer issues.

The DMC produces a public annual report of its work.

More information about the DMC:
www.dmc.commission.com

Complaints considered

The DMC will investigate any complaint made against a DMA member that relates to direct marketing activity and falls under the scope of the Code.

A complaint can either be received directly or referred from the DMA or from a statutory, advisory, self-regulatory or enforcement body.

The DMC can also open an investigation on its own initiative if it sees an issue, involving a member company.

The DMC will investigate a complaint against a non-DMA member if the Code is binding on that party by any regulatory, licensing or other condition.

Complaints not considered

Where a complaint is of a contractual nature and does not involve a serious breach of the Code that would affect other parties, then the disputing parties may be advised to use an alternative mechanism to reach resolution.

If a complaint is not covered by the Code, or involves a company not in DMA membership, it will be referred to another relevant organisation or enforcement body.

The DMC may look at and express a view on the conduct of non-members in exceptional circumstances, where this is in the best interests of customers and members in the marketplace, but will not seek to enforce the Code or the procedures set out here.

More information about the complaints process:
www.dmc.commission.com/make-a-complaint/

Receipt of complaints

A complaint can be made in writing or online at www.dmc.commission.com

The DMC aims to acknowledge a complaint within two working days and to complete a case involving investigation and adjudication within three months, but expects an informally-resolved case to be closed in a shorter timeframe.

The DMC can only act on a complaint if there is enough information to identify that there is an issue in relation to the Code and a party over which the DMC has jurisdiction.

A complaint should be accompanied by all available supporting material, such as correspondence or a copy of the relevant commercial communication.

Gathering evidence

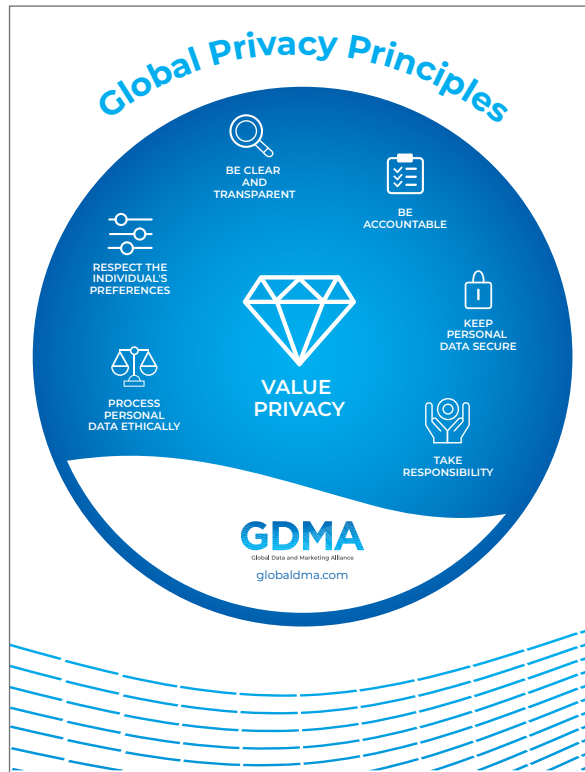
Upon receipt of a complaint, the Secretariat will raise the matter directly with the member. The member must respond to this request within 10 working days of receipt.

Data & Marketing Association

19

<p>If the member fails to respond to any request for information from the Secretariat, this may in itself constitute a breach of the Code and result in disciplinary action.</p> <p>The Secretariat may also request that the member responds directly to the complainant, with a copy of any response sent to the DMC.</p> <p>The DMC may ask the DMA to compile additional information to inform investigation into any complaints.</p> <p>Investigation process</p> <p>The DMC exercises judgment in deciding whether a complaint or a number of related complaints appear to require a substantive investigation and a formal adjudication or whether the matter can be resolved informally.</p> <p>It is the responsibility of the DMC, and the chief commissioner in particular, to ensure complaints are treated in a proportionate and appropriate manner.</p> <p>Informal resolution</p> <p>Where there appears to have been a minor breach of the Code and where there is no evidence of wider harm or risk, the Secretariat may close the matter with a formal reminder of the member's obligations under the Code.</p> <p>Where a complaint can be answered by the Secretariat without reference to the member, a copy of any correspondence will be sent to the member for information.</p> <p>In a case where an informal resolution is being considered, the DMC retains the right to revert to a formal investigation in the light of evidence of more serious or widespread harm.</p> <p>If a complaint is not resolved to the satisfaction of the DMC, or it appears that there is a serious or ongoing breach of the Code, it will be referred to the DMC Board for consideration and possible adjudication under the provisions of the Code.</p> <p>Formal investigation</p> <p>If a complaint is referred to the DMC Board, the Secretary will inform the member and request any information or comment. Members must respond to the request within 10 working days.</p> <p>The Secretariat may revert to the member, either through meetings or correspondence, if this is necessary to bring together the information needed to reach an informed adjudication.</p> <p>The Secretariat will then submit a report to the DMC, including any material that either party has specifically requested be brought to attention. The DMC Board will then consider the complaint, requesting any further information as necessary.</p> <p>The DMC may invite the member to meet with them in advance of their deliberations if it is thought that it would be helpful for the member to explain their business model and the events in question informally.</p> <p>In the case of a formal investigation, member representations may be made as part of the evidence-gathering process and just prior to adjudication.</p> <p>Adjudication meetings generally involve only Commissioners and the Secretariat.</p> <p>The Secretariat may end a formal investigation during the process and close the case, or reach an informal resolution if it becomes clear the case did not merit a substantive process and formal adjudication.</p> <p>The decision of the DMC will be recorded and communicated in writing to the member company.</p> <p>A summary of the adjudication is placed on the DMC website as soon as possible in all cases following a formal investigation, whether or not breaches have been upheld. A summary is NOT posted if the DMC declines to adjudicate on the grounds that there is no case to answer.</p>	<p>The DMC may refer a case back to the Secretariat with a request that the Secretariat look further at resolving the matter through informal procedures.</p> <p>More information about adjudications: www.dmccommission.com/adjudications</p> <p>Sanctions</p> <p>If a complaint is upheld following adjudication, the DMC has a range of sanctions that it will apply proportionately, depending on the seriousness of the issue or complaint.</p> <p>These include:</p> <ul style="list-style-type: none"> • A formal recommendation to the DMA • A formal visit to the member by the DMA • A formal undertaking from the member to comply with the standards set out in the Code • An undertaking by the member to carry out specific changes in processes, procedures, management or other arrangements to ensure an end to the problem <p>The DMC may make a recommendation to the DMA that a member be suspended from DMA membership or have their membership cancelled in cases where the DMC thinks this is necessary and proportionate.</p> <p>The DMC may refer a member to relevant law enforcement and consumer protection bodies when this appears necessary.</p> <p>The DMC may make its adjudications and files available to these bodies as required.</p> <p>More information about the sanctions: www.dmccommission.com/adjudications/appeals/sanctions/</p> <p>Appeal</p> <p>Where the DMC concludes that a member is in breach of the Code, the member is entitled to appeal against that ruling, as well as against any sanctions imposed by the DMC to the Independent Appeals Commissioner (IAC).</p> <p>On the application of the member, the DMC has the discretion to not implement any sanctions imposed until all appeal mechanisms have been exhausted.</p> <p>Members must submit an appeal in writing to the IAC within 14 days of the DMC communicating their decision.</p> <p>The IAC will only accept an appeal on one or more of the following grounds:</p> <ol style="list-style-type: none"> 1. The decision was based on a material error of fact 2. Substantial and material new evidence has emerged affecting the reliability of the original decision that was not available at the original adjudication. 3. The decision was reached following a material error in the DMC procedures, which has adversely affected the member's position. 4. The DMC has acted ultra vires (beyond its powers) 5. The sanction imposed is not proportionate. <p>Where the IAC agrees to consider an appeal, that decision will be communicated by notice to the member within 30 days of submission of the appeal. From this notice, the IAC then has a period of eight weeks in which to consider the appeal.</p> <p>Where the IAC finds in favour of the member, they will refer the decision back to the DMC and invite it to reconsider its findings or the sanction imposed.</p> <p>Where a decision by the DMC has been found to be perverse, the IAC will make their own decision. This will be final and binding on all parties.</p> <p>The DMC must consider a case redirected by the IAC within 30 days of his decision. Once the DMC has either confirmed or substituted its earlier decision, that decision shall be final and binding on all parties.</p> <p>More information about the appeals process: www.dmccommission.com/adjudications/appeals/sanctions/</p>
Data & Marketing Association 20	Data & Marketing Association 21

Appendix 2: GDMA Global Principles



PREAMBLE

New technologies and the use of personal data provides humanity with the opportunity to live better, consume better, and be more sustainable. Data has an ever increasing role in this quest for business, innovation, and economic growth. The benefits of data for society and the economy can only be achieved through its ethical use and the generating of trust between individuals and organisations. Privacy and data protection rules both contribute to the creation of trust, while providing a framework for responsible free flows of information across the world.

The GDMA Global Principles establishes a worldwide framework for customer communication that should underpin all legal and commercial approaches. They are designed as an instrument of best practice and they are intended to serve as a guide for self-regulation and legislation.

The GDMA Global Privacy Principles are aspirational commitments for organisations, governments, and people to cultivate a trusted and successful commercial ecosystem through serving each individual with fairness, transparency and respect for privacy. The guiding principle of respecting and valuing privacy engenders trust at the heart of customer communication as an exchange of value between an organisation, looking to prosper, and an individual, looking to benefit. These principles ensure that organisations across the globe put the individual at the heart of everything they do, so that organisations can be trusted, respected and ultimately sustained in all countries.

GDMA
Global Data and Marketing Alliance

PRINCIPLES

VALUE PRIVACY

Respecting and valuing individuals' privacy expectations is crucial in generating trust in the entire data and marketing ecosystem. Organisations must help individuals to feel confident and comfortable about marketing practices (for instance – when browsing the web, receiving an email, using a mobile app, or purchase online or offline) in order to generate benefits both for the individuals through trusted communication and for the organisation through worldwide value creation.

APPLICATION

- Organisations must make "Privacy" a core value through codes or policies, which must be approved by top management and communicated to all stakeholders.
- Organisations must take steps to ensure employees, partners and suppliers understand and are committed to the organisation's Privacy values.
- Organisations must train and commit employees to respect and value Privacy and ensure data security.
- Organisations should adopt a privacy by design approach.

BE CLEAR AND TRANSPARENT

Organisations must create trust by being clear and transparent with individuals about their personal data collection, use and disclosure practices.

APPLICATION

- When collecting personal data, organisations must provide (in privacy policies and beyond), timely, easily accessible and clear information about:
 - The identity of the organisation.
 - What personal data is collected and how they plan to use it.
 - The purpose of the personal data processing activities.
 - If they plan to share individuals' personal data, to what type of organisation and how.
- The right of the individual to access, rectify, update and suppress their personal data, according to local law, and how the individual can exercise these rights.
- Organisations must be clear about costs and processes that impact individuals.
- The sources of the data when not directly collected from the individual.

RESPECT THE INDIVIDUAL'S PREFERENCES

Organisations must respect individual's preference with regard to the use of their personal data for marketing communications, whenever legally and technically possible, as a way towards more efficient communication, benefiting both individuals and organisations.

APPLICATION

- Every marketer must provide an easy way for the individual to express his or her preference with respect to receiving communications from the organisation.
- The organisation must also respect opt-outs mandated by government and self-regulatory initiatives to which they are subject.
- Organisations must ensure individuals have a clear understanding of the preferences they have expressed and of any data processing resulting from their preferences.

PROCESS PERSONAL DATA ETHICALLY

The proper collection, storage, use and disclosure of personal data is essential to maintaining the integrity of the digital marketing ecosystem. Special care must be taken when dealing with sensitive data.

APPLICATION

- Organisations must limit the collection of personal data to what is necessary to fulfil their legitimate purpose.
- Organisations may not use or disclose personal information for purposes superfluous to the reason for which it was collected.
- Organisations should store personal information securely and for only as long as necessary to fulfil the informed purpose.
- Organisations should be particularly diligent when dealing with personal data that may cause harm to individuals if mishandled.
- When collecting personal data from children, organisations must ensure that all the information required is intelligible to the child and is provided by a parent or legal guardian.

TAKE RESPONSIBILITY

Organisations are responsible for the personal data they use to perform marketing activities even when it is transferred or assigned to third parties (processors).

APPLICATION

- Organisations must ensure that all their employees involved in personal data and marketing activities respect privacy and data protection practices.
- Every manager in the organisation is responsible for ensuring that personal data are used responsibly in all activities within their area of influence.
- Organisations should regularly conduct internal training on data protection for employees involved in processing personal data.
- Organisations must conduct regular audits of personal data practices and maintain records thereof.
- When commissioning third parties to process data, organisations must ensure that their personal data and marketing activities respect privacy and data protection practices.

KEEP PERSONAL DATA SECURE

Organisations must implement the necessary technical and procedural safeguards to protect personal data from unauthorised access, modification, misuse, disclosure, or loss.

APPLICATION

- Organisations must implement written information security policies and review them periodically, and conduct regular audits and testing of technical systems that house/manage personal information.
- Organisations must restrict access to their systems on a "need to know" basis. Each user should only have access to the personal data which they need to fulfil their tasks.

GDMA
Global Data and Marketing Alliance

GDMA
Global Data and Marketing Alliance

• Whenever possible, organisations should use encryption and/or pseudonymisation to safeguard the individual's personal data, especially during transfer or storage in a mobile/portable device.

• Organisations should take a Risk-Based Approach when deciding the security measures to implement, ensuring that potentially harmful personal information has higher level of security and further limitations on access.

• Organisation must promptly notify significant security breaches to enforcement or other relevant authorities as well as affected data subjects (when appropriate), and must ensure that personal information is re-secured and protected following a loss or unauthorised access or disclosure.

Organisations must demonstrate that they have adopted and implemented the necessary internal regulations, in accordance with these Principles, for the responsible use of the personal data they process.

BE ACCOUNTABLE

APPLICATION

In order to be accountable, organisations must:

- Have a comprehensive privacy management program.
- Have a clear and publicly available statement to demonstrate their commitment to compliance.
- Maintain adequate records to demonstrate compliance with these Principles.
- Implement an adequate system of monitoring and audit.
- Establish internal programs to ensure employees are held accountable according to established policy.
- Organisations must have a privacy management program in place and be prepared to demonstrate as appropriate, in particular at the request of a privacy enforcement authority.

DEFINITIONS

Encryption: is the process of converting information or data into a code to prevent unauthorised access. This is often applied to any text, messages, data, documents or images and to make the information unreadable to any person and/or organisation that does not have the decryption key.

Individual: refers to the data subject, that is an identifiable natural person who can be identified, directly or indirectly, through reasonable and appropriate efforts, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Organisation: refers to the legal/juristic person, company, partnership, trust, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Organisations may be supported by other organisations which process personal data on their behalf (e.g. cloud services, contact centers, organisation processors outsourcing).

Personal data: means any information relating to an identified or identifiable natural person (individual).

Personal data breach: an infringement of security that leads to the accidental or unlawful destruction, loss, theft, alteration, unauthorised access to or disclosure of personal data.

Personal data processing: any action done with personal data from its collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction through its erasure or destruction.

Privacy by design: is a principle which requires any organisation that is designing a data or marketing product, service or process to think about the privacy implications in advance. Thinking about privacy implications upfront and developing and integrating privacy solutions in the early phases of a project will help the organisation identify and address any potential problems at an early stage.

Privacy policy/ privacy notice: is the clear and comprehensive explanation to individuals about an organisation's data practices, including how it collects, uses, stores and shares data, and the individual's rights to have their data protected and information pertaining to how to proceed if an individual believes that their data have not been protected.

Sensitive personal data: personal data which if released without consent, could cause the individual to be marginalised and/or be harmful to the individual if it is accessed by non-authorised persons. For example: racial or ethnic origin, sexual orientation, political opinions, religious or philosophical beliefs or affiliations. Data relating to minors may also be sensitive.

GDMA
Global Data and Marketing Alliance

GDMA
Global Data and Marketing Alliance

Responsible Marketing