May 2023

Dear Committee Members,

As CEO of the DMA, it has been my privilege to chair the Secretary of State's Business Advisory Group for the DPDI Bill. In this group, we discussed a wide range of topics with a focus on enabling growth and innovation while maintaining high standards of data protection for citizens in the UK. The DMA believes the proposed bill achieves this balance while also maintaining adequacy with the EU.

DMA members have, for some years, navigated a rapidly changing technological environment and complex data protection framework. While we hoped this legislation may have brought all current data protection legislation under one roof, we are content that this additional piece of legislation can make positive amendments to the range of current rules and regulations.

This document first outlines aspects of the legislation that our members strongly support and why. These include amendments to legitimate interests in Article 6 (1)(f) of GDPR, an extension of the soft opt-in for email marketing in PECR to non-commercial organisations, additional exemptions to consent for cookies in PECR, and reductions in the administrative burdens on smaller organisations.

Beneath that, I offer thoughts on where the DMA believes that additional amendments could provide economic, environmental or consumer benefit. These suggestions are supported by an annexe that includes a more in-depth analysis and recommendations pertaining to Article 14 GDPR.

The DMA is UK's most customer focussed business community and the only industry representative body that runs a consumer protection division through our Telephone Preference Service and Mail Preference Service products. The customer experience and building trust are central to successful organisations that prioritise long-term, loyal relationships with customers and donors. Innovation and growth must be balanced with respect for privacy for citizens to trust the data-driven digital economy.

I look forward to discussing our point of view with the Committee on May 10th when I will be giving evidence.

Best regards,

Chris Combemale | CEO, DMA
Chris.combemale@dma.org.uk

The DMA is supportive of the following components of the Bill:

Issue 1: Clarification of Legitimate Interests as a basis for data processing in Article 6(1)(f) UK GDOPR

At present, processing for "legitimate interests" is one of the six equal lawful bases for processing personal data. When relying on legitimate interests as a lawful basis, organisations must demonstrate that the processing is necessary for the legitimate interest and carry out a "balancing test" to document how their legitimate interests are balanced with the rights of data subjects.

Clauses 5(9) and 5(10) of the DPDI Bill provide greater certainty to the scope of Legitimate Interests and includes three specific examples which are drawn from Recitals 47, 48 and 49 of GDPR. The DMA strongly supports this amendment as it provides clarity in the main text that is consistent with the original Recitals.

GDPR is risk-based and proportionate. For example, Recital 4 states clearly that Privacy is a fundamental right, not an absolute right, and must be balanced with other rights such as the right to conduct a business. There is nothing more fundamental to the right to conduct a business than finding new customers and retaining existing customers. A business would not exist without customers nor a charity without donors. Direct marketing is specifically recognised as a Legitimate interest in Recital 47 of UK GDPR because it is the essential activity of finding new customers/donors and retaining them over time.

However, since the implementation of GDPR, many lawyers and Data Protection Officers have created uncertainty by advising companies that consent was "safer" even though LI and consent are equal in the text. In fact, it has become widely believed across society that GDPR requires consent even for legitimate local community activities. This has limited growth at a critical time in economic recovery without providing any additional protections to individuals. As an example, in just one direct marketing channel, the DMA estimates that £250 million of direct spend in the print production sector has been lost as a result of this lack of certainty, equating to £1.5 billion of GDP using the Advertising Association's calculator that £1 of advertising spend equates to £6 of GDP.

Establishing legal certainty around LI for direct marketing as established in Recital 47 is our number one priority, including ensuring the interpretation of LI across the UK reflects that any legal interest could be a legitimate interest subject to necessity and proportionality. In advocating for this position, it is critical to remember that individuals would always retain an unfettered right to object to marketing and are further protected by consumer protection services such as Mailing Preference Service (MPS) and Telephone Preference Service (TPS), both of which the DMA runs.

In short, we strongly support the amendments in clauses 5 (9) and 5(10.

Issue 2: Cookies

Cookies and similar technologies track information about people who access a website or other electronic service. The Privacy and Electronic Communications Regulation sets out rules on the use of cookies and similar tracking technologies and on the confidentiality of terminal equipment. Clause 79(2)a-d of the DPDI Bill would extend the circumstances under which cookies or other technologies could be used to store or access information on people's devices without their express consent.

We support the Bill's proposed expansion of the range of exemptions to consent for cookies which will reduce consent banners, especially for e-commerce websites that do not take advertising. Exemptions include collecting statistical information which should cover audience measurement, and enabling the way a website appears or functions, for necessary security updates. Taken together, we believe these exemptions will mean that e-commerce and B2B websites that do not take advertising and who do not share their first-party cookie data outside the organisation should be exempt from cookie banners, freeing consumers from significant numbers of meaningless consent box-ticking and freeing many businesses from bureaucracy.

Issue 3: Extension of the soft opt-in for email to non-commercial organisations such as charities

The term "soft opt-in" describes the rule about commercial organisations sending electronic marketing communications (e.g. emails or texts) to existing customers, using data they gathered when that customer either bought or expressed interest in their products or services. There are certain criteria which need to be met to rely on this rule.

Marketing communications with an existing customer or engaged prospect must be in relation to similar goods and services. The existing customer must also be offered a simple means of opting out of receiving further communications. Currently, the soft opt-in rule does not apply to non-commercial promotions, for example, charity fundraising or political campaigning. However, if enacted, clause 82(3) of the Bill would add a new subsection (3A) to PEC regulation 22 to permit organisations which have charitable, political or non-commercial objectives to send electronic marketing communications for the purposes of furthering their objectives.

As part of the PECR, this issue has been critical for our charity members for many years in order to grow charitable donations. They will now be able to communicate with donors using email marketing in the same way as commercial organisations communicate with customers. This is a positive development which we encourage the Committee to support.

Issue 4: Accountability Framework

The DMA welcomes the recognition that Accountability Frameworks can place a significant administrative burden on companies, particularly SMEs. We are, therefore, supportive of the Bill's intention to implement a more flexible and risk-based accountability framework based on privacy management programmes.

Indeed, there are a number of changes to the Accountability framework that will reduce administrative burdens on smaller businesses such as requirements to have a DPO, conduct DPIA's and so on. The bill replaces them with similar concepts such as Senior Responsible Individuals, or Assessment of High-Risk Processing. The critical change is that smaller companies who do not conduct high-risk processing will be exempt from the duty to keep records and to have an SRI (previously DPO) which the DMA supports.

Critically, many of our members, especially our larger members, have customers in Europe so will need to maintain the accountability frameworks under GDPR. DPDI (No2) accepts this is appropriate despite the changes, essentially meaning organisations can maintain the solutions they put into place for GDPR in 2018 should they wish and remain compliant with the new legislation.

Issue 5: Enforcement and fines

The DMA believes those who flaunt the rules damage the industry's reputation, put customers at risk and harm the economy. We fully support the proposals to expand enforcement powers in PECR to match GDPR. Having run the TPS and MPS, the DMA understands the necessity of stronger reprimands for breaking marketing rules.

Issue 6: Encouraging research and investment in the commercial sphere

The Bill proposes to make improvements to facilitate research and development in the commercial sphere. Among other things, the proposals bring together research-specific

provisions; create a statutory definition for scientific research; incorporate broader consent for scientific research into legislation; extend the "disproportionate effort" exemption on information provision requirements for further processing for research purposes of personal data collected directly from the data subject.

These proposals will all be effective in reducing compliance costs in the sector, particularly, the incorporation of 'scientific research carried out as a commercial activity" into the definition of scientific research. Above all, it will bring clarity and legal certainty to researchers in the commercial sector that they can benefit from the privileges the regime affords to research.

Issue 7: Subject Access Requests (SARs) and the definition of 'vexatious requests'

The DMA supports the proposed amendments in DPDI regarding the treatment of subject access requests, and in particular, proposals that mitigate misuse of this important consumer right where it may be malicious, excessive or where such requests are co-ordinated on a large scale. It is an unfortunate complaint many DMA members and external organisations have voiced and struggled to contend with since 2018.

We support amendments to replace "manifestly unfounded" with "vexatious and excessive" and the improved clarity by way of non-exhaustive examples as to what may help our members determine whether a request is vexatious or excessive in the legislative text itself, such as "intended to cause distress", "not made in good faith" and "an abuse of process". These amendments will ensure that SARs are rightly limited to individuals pursuing their rights and will prevent abuse of the legislation by individuals or groups seeking to use the right in a targeted and purposefully harmful way.

The DMA also supports proposals to allow controllers to charge a reasonable fee for vexatious or excessive SARs should they wish to offset the administrative costs associated with such requests. Many DMA members have indicated that they consider responding to SARs a legitimate cost of business and will not charge fees, others have indicated that deterring vexatious or excessive requests is imperative as SARs have been weaponised in some instances with the intent of causing harm to businesses.

DMA proposes the following changes to the Bill

Article 40 inclusion of PECR & DPA 2018

Under the UK GDPR, trade associations and other representative bodies may draw up codes of conduct intended to contribute to the proper application of GDPR taking into account the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

As such, the DMA is developing a GDPR Code of Conduct for Direct Marketing and the specific processing of personal data that is essential to attracting and retaining customers or donors. However, the specific way Article 40 is drafted could limit the scope of a Code of Conduct only to issues contained within GDPR, whereas the overall data protection framework in the UK also includes the Privacy and Electronic Regulations and Data Protection Act 2018.

To properly cover the processing in a sector of the economy a GDPR Code of Conduct should cover all direct marketing channels including email, text messaging, and telephone calls which have specific requirements covered in PECR.

Our proposals are to amend Article 40 of GDPR to ensure a sector Code of Conduct applies to data protection legislation as a whole and not just GDPR by specifically referencing PECR and DPA2018.

"Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation **and the Privacy and Electronic Communications Regulation and the Data Protection Act 2018**, such as with regard to……"

Direct marketing for the purposes of democratic engagement

Overall, we do not support the inclusion of a new exemption for direct marketing provisions used for the purposes of democratic engagement. There have been a number of instances of political parties not following the current data protection requirements (see: the ICO website: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2020/11/uk-political-parties-must-improve-data-protection-practices/).

The DMA are concerned that the option for the Secretary of State to offer such an exemption will result in an increase in poor practice. One of our members, the Market Research Society,

has rules prohibiting such poor practices referred to colloquially as "plugging" which is political lobbying under the guise of research. For example, a telephone call which seeks an individual's political opinions and then urges support, invites contact, provides promotional material or uses that data to identify those people likely to support the political party or campaigner at a future date, in order to send them marketing material.

Therefore, we would recommend the removal of Clause 83. If that is not possible, we suggest embedding ICO guidance in the legislative text.

(see: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-for-the-use-of-personal-data-in-political-campaigning-1/)

Definitions established by the Privacy & Electronic Communications Regulations (PECR)

PECR is the key legislation that protects the confidentiality of communications and applies to all "electronic communication networks". However, Government has proposed to narrow the scope of exceptions to "information society services" (ISS) only.

This is significant as an information society service would include a service like Gmail, but ironically an email being sent using Gmail likely would not be. Additionally, services such as the 'Live TV' section on BBC iPlayer would not fall under an ISS and would require consent for audience measurement cookies but 'VOD sections' of BBC iPlayer would not have to obtain consent for the same cookies. The original scope of "electronic communications networks" should apply here.

Centralised cookie controls.

One of the stated aims of the Bill is to reduce consent fatigue and Clause 79 (6B) attempts to legislate for the automated signalling of pre-determined consent or objection to the use of cookies. We have previously expressed our concerns about legislating for alternative consent management mechanisms in this Bill.

Specifically, the power provided for in new Reg 6B is not linked to a corresponding change to consent requirements, i.e., exercising the power under new Reg 6A to create an 'opt-out' regime for cookies. Therefore, it is possible for centralised cookie controls to be introduced, and services required to respect the signals they send, while an opt-in regime exists for some cookies.

This creates risks that:

- services dependent on the use of cookies that are subject to consent will not be able to function if users choose not to opt-in via those centralised controls.
- any other personal data processing that is dependent on consented cookies (e.g., for advertising purposes) cannot take place.
- any 'consent' given by automated signals would have to meet the standard for consent set out in the UK GDPR (specific, informed, etc.).

The DPDI (No 2) Bill gives the Secretary of State the power to approve such mechanisms but does not specifically require consultation with the CMA/DMU on aspects of competition and leaves this question open-ended. This is important as centralised cookie controls incorporated in browsers (such as Safari, Google Chrome, Edge etc.) or other access-enabling technology could effectively create a new set of gatekeepers. By this, we mean creating the ability to (a) conflict with or override existing consent preferences expressed by the user to individual publishers; or (b) prompt users to authorise the technology to act as a first party in the publisher/user relationship.

As the underlying legal framework would remain unchanged, this also raises serious legal questions about liability for obtaining valid consent for processing and what should happen if consent obtained by a third party is ever legally challenged. The direct relationship between publishers and end users should be paramount and any consent expressed by users directly to publishers should not be overridden by alternative consent management platforms.

Article 14 proposals

The use of publicly available—or open source—data is important for the data and marketing sector as it enables improved analysis and insight that is used by marketers to offer relevant products and services to customers and prospects. Greater relevance improves productivity and creates economic benefits, consumer benefits and environmental benefits without creating harm.

In the case of all publicly available data sources, the scope of use is clearly established by law and transparent notification is provided. In its current form, Article 14 requires thresholds of transparency that would be too costly or impossible to achieve.

The attached annexe contains the full text of article 14. The government has already proposed amendments to Article 14 to address these concerns which are highlighted in green in the annex. The DMA's further proposed amendments are highlighted in purple. We hope the inclusion of the full text plus explanations of our proposals will help the committee to consider the matter fully.

Annexe

Article 14 Proposals: **this annexe contains the full text of Article 14. DPDI2 amendments are shown in green. DMA and DMA member amendments are shown in purple.**	**Rationale**
1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: a) the identity and contact details of the controller and, where applicable, of the controller's representative; b) the contact details of the data protection officer, where applicable; c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; d) the categories of personal data concerned; e) the recipients or categories of recipients of the personal data, if any; f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available. 2. In addition to the information referred to in paragraph 1, the controller shall provide the data	The proposed amendments to Article 14 of the UK GDPR intend to build practical solutions and clarity on the responsibilities of data controllers towards information provision to data subjects where a data controller has not obtained personal information directly from a data subject. The currently proposed amendments to Article 14 are welcomed by the data, marketing, and advertising sectors within our membership. However, filling in gaps of understanding and practical application requires greater provision to ensure sound compliance and consistency within these industries. Our membership is represented by hundreds of brands, agencies, data centres, and data brokers. These members, together with their partners, process personal information to optimise marketing material to consumers and prospects with the aim of limiting untargeted and ill-informed marketing material which is of little or no interest to individuals. Reducing practical and commercial burdens on business whilst ensuring a clear and workable privacy and data protection framework which protects individuals and their personal data is no small task, but we believe this is achievable and will

subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; e) the right to lodge a complaint with a supervisory authority; f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	lead to greater innovation in the marketplace and position the UK as a leader in data marketing compliance and innovation in the data economy.

3. The controller shall provide the information referred to in paragraphs 1 and 2: a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed. 4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. 5. Paragraphs 1 to 4 ~~shall not apply where and insofar as~~ do not apply to the extent that: a) the data subject already has the information; ~~b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the~~	

~~controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;~~ c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; ~~or~~ d)~~where~~ the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy; e) providing the information is impossible or would involve a disproportionate effort; f) the obligation referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of the processing for which the personal data are intended; or g) the controller has obtained the personal data from any of the following public registers: (i) the Electoral Register (ii) the Register of Judgments, Orders and Fines (iii) the Register of Companies (iv) the Land Register (v) the Food Standards Agency Register The Secretary of State may by regulations amend paragraph 5(g) by	The addition of paragraph 5(g) cements and reinforces the already existing understanding that publicly available data is processed for public interest and legitimate commercial purposes. Individuals are told that their details on the electoral register, for example, can be used by organisations for any purpose and are given the choice to opt out from having their details included in the open electoral register. Navigating the current Article 14 requirements is not easy. The function of setting out a specific exemption in law where data is obtained from publicly available registers would provide clear

(i)adding to or varying the list of public registers, or (ii)omitting provisions added by regulations made under this paragraph.	understandings to data controllers. Additionally, it would reduce unnecessary and wasteful notifications to individuals which are likely to cause confusion and alarm.
6. For the purposes of paragraph 5(a), the data subject will be deemed to have the information where they have been provided with a hyperlink to that information by a third party.	The addition of paragraph 6 proposes the use of hyperlinks to provide privacy information. Such a simple proposal would help reduce the practical and commercial burdens on data controllers. It is routine practice for data controllers to conduct their due diligence on suppliers and processors to make sure that they are UK GDPR and PECR compliant. Enabling controllers to rely on their third parties to provide their privacy information minimises the significant additional costs and emphasises a culture of building greater transparency and commitment to ensuring compliance with the law. Providing clarity and instruction in legislation for all controllers and their third parties will also mitigate any commercial disadvantages to smaller resourced organisations operating within this industry, creating an equal footing for all. An additional benefit would be the reduction in wasteful postal notifications being sent to millions of individuals which increases environmental concerns, as well as lessening confusion to individuals, and significant costs to organisations.
7. For the purposes of paragraph 5(e), whether providing the information would involve a disproportionate effort depends on, among other things, the cost and effort of compliance, the	The proposed amendments to paragraph 7 add further clarificatory criteria that should be considered when assessing whether the provision of

number of data subjects, the age of the personal data, the damage and distress to the data subjects, any appropriate safeguards applied to the processing, and the information having been collected and made publicly available by a public body. 8. A controller relying on paragraph 5(e) or (f) must take appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including by making the information available publicly. 9. For the purposes of paragraphs 7 and 8, an appropriate safeguard or measure might be a risk assessment, including limiting the extent and purpose of the processing for which the data might be used.	privacy information constitutes a disproportionate effort. In support of the proposals being made for Article 14, the recent FTT judgement highlighted the point that individuals are unlikely to be harmed or distressed by not receiving notification information where disproportionate effort is relied on, but also that there is a concern of overwhelming individuals which itself could create, at best, annoyance and, at worse, distress where they are overloaded with notification information. The addition of paragraph 9 offers clarity as to what an appropriate safeguard might be - a risk assessment. This maintains the focus on organisations taking responsibility to plan and think about their processing activities, consider their resources in the current economic climate, and ensure data subject rights and protection are properly accounted for.