CAP Consultation on General Data Protection Regulation
Individual responses

1 – Boots UK Ltd

As the statutory Regulator for data protection matters, we would argue the ICO should be the foremost body dealing with data protection, privacy and GDPR related matters and would question whether this should be removed from the CAP code altogether.

If CAP are to retain elements of data protection within marketing, we would respond as below to the specific questions.

5.1.1 Agree, the ICO is the most appropriate body to deal with such matters

5.1.2 Agree, the ICO is the most appropriate body to deal with such matters

5.1.3 Agree

5.1.5 Agree, the ICO is the most appropriate body to deal with such matters

5.1.6 Agree, the ICO is the most appropriate body to deal with such matters

5.2.1 Agree, this is consistent with GDPR

5.2.2 Agree, this is consistent with GDPR

5.2.3 Agree, this is proportionate

5.2.4 Agree, this is consistent with GDPR

5.2.5 Agree, this is consistent with GDPR

5.2.6 Agree, consistent with Unfair commercial Practices Directive and Consumer Protection from Unfair Trading Regulations 2008.

5.3.2 Agree, this is consistent with GDPR

5.3.3 Agree, this is consistent with GDPR

5.3.4 Agree, this is consistent with GDPR

5.3.5 Agree, however if PECR changes before being enacted this may lead to conflict or necessitate further consultation to amend CAP code

5.3.6 Agree, this is consistent with GDPR

5.3.7 Agree, in line with existing CAP code requirements

5.3.8 Agree, in line with existing CAP code requirements

5.3.9 Agree, this is consistent with GDPR

5.3.10 Agree, this is consistent with GDPR

5.3.11 Agree, however if PECR changes before being enacted this may lead to conflict or necessitate further consultation to amend CAP code. It must also be consistent with ICO guidance

5.3.12 Agree, this is consistent with GDPR

2 – Direct Marketing Association UK Ltd (DMA)

About the DMA

The DMA is the trade body for the data and marketing industry. We represent over 1,000 organisations – encompassing brands, agencies and marketing service companies. Please visit our website www.dma.org.uk for more information about us.

Introduction

The DMA welcomes the opportunity to respond to this consultation issued by CAP. The CAP Code has an important role to play in ensuring organisations use data responsibly for their marketing activity and that there is consistency between regulators and other self-regulatory bodies. Using the Direct Marketing Commission (DMC) as an expert panel will help achieve these goals.

Section 4.3 pre-consultation work and guidance

Direct Marketing Commission (DMC)

The consultation document posits that the DMC could take on an advisory role to the CAP executive, ASA executive and ASA Council in complex cases involving personal data covered by section 10 rules in the CAP Code.

Organisations are still grappling with GDPR compliance in relation to direct marketing. There is not a widespread consensus over which legal ground is appropriate in certain circumstances. The use of legitimate interest, in particular, has been problematic because of its subjective nature. Organisations must carry out a legitimate interest assessment (LIA) and decide for themselves whether they believe they have a valid case for using legitimate interest. In the absence of case law businesses will be tentative when deciding whether to use legitimate interest as a legal ground for direct marketing.

Individuals can challenge an organisation's legitimate interest assessment. Ultimately, it is up to the ICO to decide whether it is valid or not. However, the ASA may well receive complaints about the use of legitimate interest. The lack of case law may mean these cases are often ambiguous and complex. Therefore, the ASA would benefit from the expertise of the DMC, which is responsible for enforcing compliance with the DMA Code in relation to DMA members. The Code is strongly aligned with the key principals of GDPR and supported by a series of GDPR Guidance documents which have been created in collaboration with the ICO, ISBA and the Data Protection Network.

Working with the DMC will ensure a consistent approach to GDPR across self-regulatory bodies which is essential for marketers to develop consensus on their approach to legitimate interest and other issues. Consistency will reduce the risk for marketing departments and give businesses confidence to invest and plan for the long-term. The DMC is comprised of 5 commissioners. All of them have a background in the regulation, data or marketing - from diverse roles in government to PWC and advertising agencies. They are experts in data protection and marketing.

DMA GDPR Guidance

To counter any concerns around consistency with the ICO's approach, the DMA would advocate that CAP takes on board the DMA/cross-industry GDPR guidance as referenced above when ruling on any data/GDPR related complaints.

The guidance focuses on; the essentials, accountability, consent and legitimate interest and profiling. The DMA accepted all substantive amendments suggested by the ICO. Information Commissioner, Elizabeth Denham, wrote the foreword for each of the documents. The guidance is freely available to all marketers. The ASA can help build consistency in GDPR approaches by sharing the DMA's guidance, which is already widely used.

Section 10 rules

Personal data is fuelling growth in Europe and allowing marketers to form a comprehensive view of their customers. In the UK, BCG estimates that the internet economy accounts for over 10% of GDP and growing at 32% a year. Nesta estimates that Digital Technology contributes £160 billion to the UK economy through 1.56 million jobs, of which 12% are in data management and analytics solutions.

The CAP Code will play a vital role educating marketers around the responsible use of personal data and ensure that businesses receive a coherent message. One of the main problems in the run up to GDPR was the plethora of different groups giving contradictory data protection advice. By consulting with the ICO and working with the DMC, CAP call help align regulatory and self-regulatory bodies.

Overall, the DMA agrees with the proposed changes to section 10 but has reservations regarding three changes.

Removal of rule 10.4

The DMA agrees that the first sentence of the rule should be retained as a new rule 10.1. The DMA is not convinced the rule in 10.4.3 is necessary but have no objection to it being retained as a separate rule 10.11.

Rule 10.5

The DMA would like to see this rule end at the end of the first sentence. The rest of the rule deals in more detail with legitimate interests which is unnecessary here. If this was to stay, there should be some clarification on consent as well. Unintentionally, it is suggesting that legitimate interests is "second tier" to consent, which is not the case. All six legal bases for processing personal data are equally valid as there is no hierarchy. It is up to businesses under the accountability responsibility to decide on their legal basis for processing.

Rule 10.16

The DMA agrees with the first part of the rule in terms of providing information in a form that children will understand. However, the reference to avoiding using personal data of a child for personality or user profiles goes beyond Recital 38, which states special protection should apply to this but not that it cannot happen. This would seem to go beyond the GDPR provisions. In addition there is no mention in Recital 71 about children, so as children are treated as data subjects like anyone else, there should not be added restrictions placed on processing their data beyond the provisions of the GDPR. The DMA would suggest the rule should be:

When collecting personal data from a child, marketers must ensure that the information provided in Rule 10.2 is intelligible to a child (or their parents if relying on Rule 10.15).

3 – Harbottle & Lewis LLP

Introduction

Harbottle & Lewis is a leading UK-based law firm with a reputation for our expertise in the Technology, Media and Entertainment sectors. We undertake the full spectrum of work in relation to data protection and privacy and, over recent years, have assisted a very large number of clients with their preparations for compliance with the GDPR. Our clients range from start-ups to multinationals across a diverse range of industries. In addition we have a strong marketing and advertising practice. We are involved in the latest industry trends and frequently advise clients on issues such as programmatic media buying, native advertising, and product placement. We have a particular interest in the intersection between advertising regulation and data protection, as this affects a significant proportion of our clients, whether they are brands, agencies, platforms or media companies.

Our submission draws on our experience of advising our clients about their obligations both under the GDPR (and associated privacy and data protection laws) and the CAP code (and associated advertising regulations).

General comments

We welcome the ASA's consultation on Section 10 and Appendix 3 of the CAP code, which we have considered for some time as confusing for our clients and their customers. Whilst our detailed response is provided below, our overall impression is that the proposal to remove rules in the CAP Code which relate to "pure data protection matters" is necessary and helpful. We consider that it will help promote simplicity and certainty for both marketers and consumes. This should foster greater compliance overall by enabling a consistent approach to data protection law and regulatory guidance lead by the most appropriate regulator.

In particular, we agree that it does not make sense for the CAP Code to include regulatory requirements which are not specifically related to marketing and advertising. Our view is that the CAP Code should only address a matter of privacy and data protection where either (i) privacy and data protection legislation (such as the GDPR, the UK Data Protection Act 2018 (DPA 2018) or the Privacy and Electronic Communications Regulations (PECR)) does not cover the point or (ii) the privacy and data protection legislation has left the matter open to interpretation. This is especially the case given the additional regulatory force that will be given to the ICO's direct marketing guidance which will take the form of a direct marketing code (pursuant to s.122 DPA 2018).

Responses to the specific proposals for change

5.1 Removal of rules from section 10

5.1.1 Removal of rules 10.1 and 10.2: data security and transfer outside EEA

1. We agree with this proposal as rules 10.1 and 10.2 should remain within the ICO's sole jurisdiction. As mentioned above, the overlap between (i) privacy and data protection matters in the CAP Code and (ii) privacy and data protection law (and associated ICO guidance) is confusing to both businesses and consumers and creates uncertainty as to which regulator has oversight over the applicable requirements.

2. In addition, the greater the overlap, the greater scope there is for discrepancies as the law and regulatory guidance evolve. This places an additional burden on both

CAP and the ICO to ensure their respective approaches are aligned in a time when regulators are experiencing extreme resource constraints (in particular due to the implementation of the GDPR).

3. We also note that the enforcement options available to the ASA are clearly very different to those of the ICO. There is a benefit to marketers and advertisers for there to be flexibility in the regulatory enforcement regime. However, in the event consumers were to complain to the ASA about a matter of 'pure' data protection law under the CAP Code (such as the rules regarding data security and extra-EEA transfers), there is a significant risk that data subjects' rights would be diminished if the matter were handled purely by the ASA with its limited enforcement powers (when compared to the ICO).

5.1.2 Removal of rule 10.3: access to data

1. We agree with this proposal. This rule is not exclusively related to advertising or marketing and is properly and much more substantially covered by Chapter 3 of the GDPR (together with the applicable exemptions under the DPA 2018). In particular, we consider that Rule 10.3 does not adequately reflect the scope of the data subject access right under Article 15 of the GDPR. There is a risk that advertisers and marketers (if solely relying on the CAP Code) would not appreciate the scope of the data subject access right as a result.

2. In addition to the overlap with data subject access rights we note the overlap with the obligation for data controllers to inform data subjects of certain information about the processing of their personal data and their rights in relation to their personal data at the time (or shortly after) such data is collected under Articles 13 and 14 of the GDPR.

3. We also consider that if this rule were to remain (which we do not think is advisable) it would require significant additions to adequately match the conditions of Article 12 GDPR which concern how the data controller should facilitate the exercise of data subjects' rights.

5.1.3 Removal/amendment of rule 10.4: persistent and unwanted marketing communications

1. We note that Rule 10.4 (or 10.1 as it will become) is derived from Schedule 1 of the Consumer Protection from Unfair Trading Regulations 2008 ("**CPRs**") which lists the commercial practices which are in all circumstances considered unfair. Paragraph 26 of Schedule 1 of the CPRs states:

   "Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified to enforce a contractual obligation."

2. There are clearly some differences between Paragraph 26, Schedule 1 of the CPRs and the equivalent rule in the CAP Code:

   a) Rule 10.4/10.1 applies specifically to *"marketing communications"* as opposed to *"solicitations"* under the CPRs. We consider this distinction is sensible given that the CAP Code is, of course, specifically focused on advertising and marketing, whereas the CPRs apply more broadly to trading between businesses and consumers;

b) Paragraph 26, Schedule 1 of the CPRs also includes an exception to the prohibition against persistent and unwanted solicitations, *"in circumstances and to the extent justified to enforce a contractual obligation".* Rule 10.1 does not however include this (or even a similar) exception. This is appropriate given that there will never be a situation where a marketer could justify persistent or unwanted marketing to enforce a contractual obligation.

c) We note that the reference to "other remote media" is consistent with the terminology used in the equivalent rule in the CPRs. However, we consider that this terminology is perhaps unclear and out of date. For instance, it could be helpful to include a reference to SMS and/or perhaps more simply to marketing communications by "any other means". An alternative approach would be for the definitions of direct marketing to be aligned in the CAP Code with the definition of direct marketing under s.122(5)DPA 2018: ""direct marketing" means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals."

d) We understand the intention of Rule 10.1 to prohibit persistent and unwanted marketing communications. However, in practice there is still the potential for this to overlap with privacy and data protection law. In particular, the most common lawful basis (under data protection law) that a marketer will rely on in order to process personal data for marketing purposes is either (i) consent or (ii) legitimate interest. Marketing communications may therefore be "unwanted" if the consumer has withdrawn his/her consent (as one is entitled to do at any time under Article 7 GDPR) or objected to marketing (Article 21(2) GDPR). Marketing communications could also be considered "persistent" where the marketing is outside the consumer's reasonable expectation as per the balancing test required for legitimate interest under Recital 47 GDPR which requires that the data controller must weigh up the proposed legitimate interest with the interests and fundamental rights of the data subject*: "The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing".* It is therefore unclear what is (if anything) Rule 10.1 of the CAP Code adds by prohibiting 'unwanted' and 'persistent' marketing to the extent such activity would already breach privacy and data protection law.

3. In relation to the proposals regarding the sub-rules under current Rules 10.4.1 – 10.4.5, our comments are as follows:

a) Rule 10.4.1:

We agree that this sub-rule should be deleted for the reasons cited in the proposal. The sub-rule is already dealt with by various other rules. We also note that 'persistency' under new Rule 10.1 primarily relates to the 'frequency' of the marketing communication and arguably not the 'suitability' of its contents. We also consider that there is a difference between requiring marketers to assess the *suitability* of the communication as opposed to whether it is *wanted* or *unwanted*. This sub-rule arguably confuses these issues.

b) Rule 10.4.2:

We agree with this deletion (please also see our comments on proposal 5.3.4). Our view is that the CAP Code does not need to cover rules or guidance about 'consent' which has been covered (at length) by regulatory guidance in the

context of privacy and data protection law. We also note the reference to 'explicit' consent in this sub-rule is unhelpful as neither the GDPR nor PECR require 'explicit' consent for marketing.

c) Rule 10.4.3:

We agree with the proposal to retain this rule as a new Rule 10.11. This is a good example of a rule which should be retained and covered by the CAP Code because there is no overlap with data protection law – the deceased are specifically outside the scope of the GDPR (and data protection generally) as provided in Recital 27 GDPR and s.3(3) DPA 2018.

d) Rule 10.4.4:

We agree with the proposal as per our comments in relation to Rule 10.4.2 above.

e) Rule 10.5.5:

We agree with the proposal to remove this sub-rule due to the overlap with pure protection matters. We note in particular, the inconsistency with the data subject right to rectification under Article 16 GDPR which provides that such rectification should take place “without undue delay” which we consider conflicts with the 60 day timeframe under this sub-rule.

5.1.5 Removal of rule 10.8: publically available information *[We assume the omission of 5.1.4 from the proposal was a typo]*

1. We agree with the proposal to remove this rule for the reasons cited in the proposal. Please also see our comments in relation to proposal 5.3.4.

2. It is broadly correct that marketers need either consent or a legitimate interest in order to use generally available personal data for marketing purposes. However, even if there is a legitimate interest in the marketing, there are still further considerations which have to be considered as part of a *legitimate interest assessment* (see ICO guidance on legitimate interests).

3. Aside from the data protection issues (i.e. the need to ensure there is a lawful basis for processing in the first place), we also suggest that this rule is perhaps somewhat misleading from an intellectual property given that there may be IP issues beyond merely 'database rights' as referenced in the Rule which affect whether 'published information' can be used. Rule 10.8 does not define ‘published information’, nor does it indicate how such information can be used and what it can be used for. The rule is therefore quite vague and we consider there are potentially broader issues at stake such as copyright, trade mark rights, and passing off in relation to the use of ‘published information’.

5.1.6 Removal of rules 10.10 and 10.11: nature of personal information and retention

1. We agree with the proposal to remove these rules which clearly overlap with the data protection principles in Article 5 of the GDPR.

Additional comments on removal of section 10 rules:

Rule 10.5: We note the current Rule 10 will be included as a new Rule 10.10. We consider that this rule should remain in the CAP Code. However, we suggest that it could be helpful for the rule to include further guidance regarding the significance of maintaining a suppression file from a data protection perspective. For instance, the Rule could states that, in order to comply with the consumers' entitlement to have their personal information suppressed (or their right to object to direct marketing generally), marketers must retain a suppression files and, in particular, retention of such a suppression file will constitute a legitimate interest. In our experience, marketers have been confused as to whether they are entitled to retain data on a suppression file if someone objects to marketing under Article 21(2) GDPR, or even more so if someone makes an 'erasure request' under Article 17 of the GDPR. If the marketer's entitlement to retain data on a suppression file is expressly stated in the CAP Code as constituting a legitimate interests we consider this would help marketers in an area of much confusion (and provide helpful guidance to any marketers who are conducting a legitimate interest assessment on this point). See our comments at 5.3.7 below.

Rule 10.6: We note that there is no proposal to amend existing Rule 10.6 (which will be included as a new Rule 10.7). However, we do not consider that this rule is required in the CAP Code as it is already adequately covered by Regulation 23 of PECR which covers the use of email for direct marketing purposes where the identity or address of the sender is concealed.

5.2 Addition of/amendments to definitions in section 10

5.2.1 Consent

We agree with this definition. The definition of consent should align with the statutory one provided under the GDPR and DPA 2018.

5.2.2 Personal data

We agree with the proposal for the same reasons as 5.2.1 above.

5.2.3 Marketers

1. We do not agree with this proposed definition for the following reasons:

2. Firstly, much of the statutory regulation around direct marketing falls under PECR which does not operate on the basis of a controller/processor distinction. For example, the email marketing provision in Regulation 22(2) PECR applies to the person transmitting or instigating the transmission and does draw a distinction between whether that person is a controller or a processor.

3. Secondly, we consider that compliance with the CAP Code should not require an assessment as to whether a marketer is a controller or processor (this distinction is also a difficult one in a digital marketing context). The very requirement to make that distinction indicates that data protection law is involved.

4. Finally, it is unclear how this proposed definition relates to the "Scope" provision in III(g) of the CAP Code. We consider that this presents an opportunity for CAP to provide a more industry specific position as to whether they intend the CAP Code to apply to the brand/advertiser only and not its agency (e.g. a direct marketing agency).

5.2.4 Controllers

1. We do not agree with this proposed definition.

2. We do not think it is helpful to include a definition of 'controller' in the CAP Code. It is a very difficult definition conceptually and arguably one that falls within the realm of 'pure data protection law'. We consider that the purpose of the CAP Code should be to provide clear and industry specific guidance for advertisers/marketers.

5.2.5 Special categories of personal data

We query why it is relevant to include a definition of Special Categories of Personal Data as we consider this is a ‘pure data protection point’. See our further comments below regarding the new Rule 10.9.

5.3 New section 10 rules

5.3.1 Rule 10.1: persistent and unwanted marketing communications

1. Please see our comments in relation to proposal 5.1.3

2. In addition, as a more general comment we query the general prohibition against ‘persistent’ and ‘unwanted’ marketing provided under this rule as these terms are not clearly defined.

    a) For instance, it is not clear what constitutes ‘persistent’. If someone consents to weekly emails, then that marketing is persistent, but a marketer who has obtained consent of the consumer, would be entitled to send it.

    b) It is also not clear what ‘unwanted’ means. If a person consents to marketing, they could argue that they do not 'want' the marketing but the marketer is still entitled to send it until the person withdraws their consent. Similarly, if a marketer is entitled to market on the basis of the soft opt-in under PECR, or for postal marketing where consent is not required, a person could argue that they do not ‘want’ the marketing, but again the marketer would not have been in breach when sending the marketing in the first instance.

    c) We assume that the intention of this rule is to refer to situations where a person has either withdrawn their consent or exercised their right to object to direct marketing under Article 21(2) GDPR. In such circumstances, the marketer would already be in breach of PECR and/or the GDPR. As such we query whether Rule 10.1 should be removed altogether on the basis that it is unclear as to the relationship and overlap with privacy and data protection laws.

5.3.2 Rules 10.2 and 10.3: transparency about data collection

1. We disagree with the proposal to include these new rules.

2. We note that the purpose of this consultation is to remove ‘pure data protection matters’ from the CAP Code and the ASA’s jurisdiction. These new rules clearly overlap with the information obligations under Articles 13 and 14 of the GDPR. We are concerned that the inclusion of this Rule in the CAP Code will foster confusion amongst marketers (and potential consumers).

3. The proposed rules are not sufficiently industry specific. We suggest that the ASA should only consider including rules on transparency and the right to be informed if there is any industry specific rules the ASA wishes to address. Otherwise we consider that the ASA does not have sufficient regulatory power to enforce against insufficient privacy notices. It should be clear to consumers that any complaints concerning transparency or their rights to be informed should be directed to the ICO.

5.3.3 Rule 10.4: further processing

1. We disagree with the proposal to include this new rule as we consider that it is a pure data protection issue.

2. Whilst it is correct that the proposed new rule broadly reflects the provisions in Articles 13(3)/14(4) of the GDPR, the position is much more complex – in particular merely providing a "further privacy notice" does not in and of itself entitle and justify the further processing.

3. We note that Article 6(4) of the GDPR also needs to be considered as to the appropriate lawful basis for the proposed further processing. There is a risk that including the new rule in its proposed form could mislead marketers into thinking that they are only required to provide another privacy notice rather than carry out the assessment under Article 6(4) to ensure they have an appropriate lawful basis for further processing.

5.3.4 Rule 10.5: lawful basis for processing

1. We disagree with the inclusion of this new rule. We consider that this rule is a matter for pure data protection law. In particular, it is not appropriate for the CAP Code (as a self-regulatory code) to make provisions about whether processing of personal data is done so under an appropriate lawful bases which is the remit of data protection law.

2. We also note that it is arguably not entirely accurate to state that the *"legitimate interest provision does not apply where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data".* Legitimate interests as a lawful basis can still apply in such circumstances but it would be subject to a balancing exercise (as provided in Recital 47 of the GDPR).

3. If this rule is included in its current form there is a risk that it will promote uncertainty and inconsistency in relation to this particular issue. However, we note that the availability of legitimate interests as a lawful basis for direct marketing (as per Recital 47 of the GDPR) has caused a considerable amount of confusion amongst marketers. We consider that there *could* be a role for the CAP Code to set out various types of direct marketing activity (conducted in certain ways) which do *not* require consent (and therefore **<u>may</u>** be justifiable on the basis of legitimate interests) - this could help marketers conduct their own legitimate interest assessment - the ICO has stated in its guidance on legitimate interests that industry codes can be used as a factor to consider whether legitimate interest is available as a lawful basis for any particular activity.

5.3.5 Rules 10.6, 10.7 and 10.8

We do not agree with the proposal to introduce these rules. In our view these rules are already covered by PECR (for example under Regulations 22 and 23).

5.3.6 Rule 10.9: special categories of personal data

We do not agree with the proposal to introduce this rule as it is clearly within the remit of the GDPR and DPA 2018 and subject to the ICO's jurisdiction.

5.3.7 Rule 10.10: suppression

1. Our view is that the first sentence of this new rule should be deleted. It is already covered by the right to withdraw consent and the right to object to direct marketing under the GDPR.

2. However, we consider that the second sentence should remain in the CAP Code as the obligation to specifically run checks against a suppression file is not provided in the GDPR (and in PECR it is limited to preference call lists and communications by fax).

3. However, we suggest that the drafting is reviewed as we do not think it is clear what a "suitable period" would mean. For instance, does it mean the checks against the suppression file must be run within the "suitable period" or that the suppression file itself must be created within a "suitable period". We note that in relation to checking against preference call lists, PECR prescribes a 28 day time frame and we are unclear how that is intended to fit with this new rule.

4. We consider that the final sentence of the new rule should remain in the CAP Code as it provides a specific positive obligation to maintain a suppression list which is not included in GDPR. This obligation can be used by marketers to demonstrate that the retention of their suppression list will be a legitimate interest as referred to above (or perhaps even necessity for compliance with a legal obligation under Article 6 GDPR).

5.3.8 Rule 10.11: contacting those notified as dead

We agree with this proposed rule (please see our comments in relation to proposal 5.1.3). There is value in including this specific obligation in the CAP Code as data relating to the deceased persons is not covered under UK data protection law.

5.3.9 Rule 10.12: withdrawal of consent

We do not agree that this new rule needs to be included. It arguably duplicates what is already covered in the GDPR and is therefore a matter of 'pure' data protection law.

5.3.10 Rule 10.13: right to object

1. We do not agree that this new rule needs to be included as it is a matter of 'pure' data protection law.

2. We also note that as currently drafted this rule is inconsistent with Article 21 of the GDPR because the right to object to direct marketing under Article 21(2) makes no reference to lawful basis.

5.3.11 Rule 10.14: marketing to corporate subscribers

We consider that, although much of this rule reflects the PECR corporate subscribers exemption, there is nevertheless value in including the reference to "named employees" within the exemption. In particular, this is an area of substantial confusion for many B2B marketers (i.e. whether they are able to market only to generic corporate email addresses

without consent or also to an employee work email address). There is therefore some value in having the position made absolute clear in the CAP Code (even if this duplicates the position in PECR).

5.3.12 Rules 10.15 and 10.16: marketing to and collecting data from children

1. It is not clear to us why the age of 12 has been chosen as the threshold for determining whether personal data may be collected from children (without verifiable consent of a parent/guardian). We note that the DPA 2018 (section 9) sets the threshold at aged 13 (in the context of 'information society services') and consider that consistency with the DPA 2018 will make it easier for marketers to comply.

2. As the rule is currently drafted it means that different age requirements will apply depending on whether the personal data is collected via an information society service for marketing purposes as opposed to an offline source. This is potentially confusing for marketers.

5.4 Removal of Appendix 3

1. We agree with the proposal to remove Appendix 3 of the CAP Code. We consider that Appendix 3 has long been problematic from a privacy and data protection perspective given that it (and the self-regulatory regime introduced by the European Advertising Standards Alliance (EASA) for OBA) fundamentally operates on an opt-out basis for OBA cookies.

2. This approach is inconsistent and conflicts with the prior consent requirements for cookies under Article 5(3) ePrivacy Directive (implemented under Regulation 6 PECR in the UK). This issue has been raised by European data protection regulators on many occasions for a number of years. For example in the Article 29 Working Party ("**WP29**") (now the European Data Protection Board / EDPB) letter addressed to the Online Behavioural Advertising (OBA) Industry regarding the self-regulatory Framework (3 August 2011) and the WP29 Opinion 16/2011 ("**WP188**") where the WP29 concluded that the EASA self-regulatory regime was not "per se" adequate to ensure legal compliance.

3. Whilst we do agree with the removal of Appendix 3, it is not clear to us how CAP intends to cover online interest-based advertising as a result, including how to address the tension between legislative and industry approaches as described above. Likewise, the self-regulatory approach to advertising cookies as "opt out" is likely to become even more untenable in the context of the GDPR – to this end we note the considerable work undertaken by the IAB in the context of its Transparency and Consent Framework.

Additional comments on Annex A: new section 10 rules

Background

"In considering complaints under these rules, the ASA will have regard to the General Data Protection Regulation ("the GDPR", (EU) 2016/679) and the Data Protection Act 2018……"

Given that the purpose of the consultation is to separate the CAP Code from pure data protection matters, we are unclear as to why the ASA must/should have regard to the GDPR, DPA or PECR. In addition, the ASA is of course an advertising industry self-regulatory body which does not have jurisdiction over these pieces of legislation.

"Responsibility for complying with the database practice rules rests with marketers who are controllers of personal data and others responsible for marketing communications involving personal data (e.g. processors)"

We do not think it is helpful to refer to "database practice" as this is a very specific application of data in a direct marketing context. We consider the reference should be to the more general concept of "direct marketing".

We are also unclear what is mean by "and others" since this same paragraph provides that the amendments are made so that the rules only refer to marketers who are controllers – see our comment below regarding the definition of 'marketers'.

Definitions

"marketers" – the inclusion of "and/or" in this definition is confusing. It suggests that the definition covers a marketer and a controller, as well as a marketer who is not a controller. We do not think that is the intention.

"preference service" – we suggest that this definition refers to the **statutory definition under PECR** in order to ensure the obligations in the CAP Code do not apply in respect of any other preference service, including unofficial ones.

Additional comments on the new rules:

Rule 10.9 - In our view this Rule should not be included in the CAP Code. Our concern is that it does not state clearly that it applies only to processing for marketing purposes. If it applies more generally to any processing then the rule is a matter of pure data protection law and in any event is technically not correct as there are other lawful bases and exceptions which enable special category personal data to be processed for certain purposes.

Comments regarding rule 8.25.8

Finally, we note that this Consultation only relates to Section 10 of the CAP Code. However, in our view, Rule 8.25.8 is also relevant and should be considered by CAP as part of this Consultation.

Rule 8.28.5 specifies, amongst other things, that promoters must either publish or make available on request the details of major prizewinners except in circumstances where promoters are subject to a legal requirement never to publish such information. The Rule also states, amongst other things, that promoters must obtain consent to such publicity from all entrants at the time of entry.

We note that on the CAP website there is (as at the date of our submission) a statement adjacent to Rule 8.28.5 which refers to this Consultation. However, it is not clear whether CAP is intending any proposed amendments to Rule 8.28.5.

Rule 8.28.5 has long been the source of confusion amongst marketers and is likely to be even more so given the introduction of the GDPR. In particular, the obligation to publish details of winners on the one hand, but also obtain their consent on the other hand is arguably inconsistent and conflicts. This is on the basis that, under data protection law, consent can be withdrawn at any time. Therefore, if a winner withholds his/her consent, the promoter would be unable to publish the details and would on the face of it be in breach of the first sentence of Rule 8.28.5.

We understand that CAP interprets the "*legal requirement never to publish such information*" as only applying to NS&I (and not for example a situation where data protection law might prohibit publishing the individual's name). We also note that, in its 2015 guidance on promotional marketing, CAP stated that the ASA made it clear that it considered that (a) promoters' responsibilities under the Data Protection Act 1998 were not incompatible with the requirement to disclose the details of prize winners and that (b) including the information on how the data will be made available in the T&Cs of the promotion is likely to be considered an acceptable way to obtain consent. However, we would recommend that CAP reconsiders this position in light of the GDPR on the basis that the requirements for consent are clearer and stricter under the GDPR (in particular the basis on which consent can be included in terms and conditions and made a condition of performance etc). Similarly, it may be that there are other lawful bases available (such as legitimate interests) to enable the promoter to publish the details of the prize winner without needing to obtain the individual's consent.

4 – IPA

Introduction

The IPA is the professional body for advertising, media and marketing communications agencies based in the United Kingdom. We have approximately 300 agency brands within our membership.

As a not-for-profit membership body, incorporated by Royal Charter, the IPA's role is two-fold: (i) to provide essential core support services to its corporate members who are key players in the industry; and (ii) to act as the industry spokesman.

The IPA supports the fundamental purpose of the GDPR: the protection of natural persons with regard to the processing of their personal data, and the role of the Information Commissioner's Office (ICO) in the regulation of data protection matters in the UK. We also recognise the importance of the advertising industry, including agencies, in protecting people's personal data.

The IPA is a member of CAP and BCAP.

Responses to consultation questions – general

The IPA supports the proposal to remove section 10 CAP Code rules relating to "pure data protection matters". We would, however, suggest that several of the rules proposed to be introduced by CAP as having a "marketing dimension" also relate to "pure data protection matters".

We note that the Background section confirms that the rules are intended to relate only to data used for direct marketing purposes.

Responses to consultation questions – specific

5.1 Removal of rules from section 10

We agree with the proposals.

5.2 Addition of/amendments to definitions in section 10

We agree with the proposals.

5.3 New section 10 rules

5.3.1/rule 10.1 – agree.

5.3.2/rules 10.2 & 10.3 – under Art 13 GDPR, where personal data relating to a data subject are collected from the data subject, the controller must, at the time when the personal data are obtained, provide the data subject with information listed under that Article. (Similar rules apply under Art 14 GDPR where personal data are obtained other than from the data subject.) These proposed new rules seem to have general application rather than specific relevance to marketing. Further, we question the need to copy out Art 13 rather than incorporating it by reference.

Proposed rule 10.2.6 does not seem to make sense or accurately reflect Art 13.1(f) GDPR.

We would ask whether proposed rule 10.2.12 should be amended so that, in the second line, "other" is replaced by "similarly" (to more accurately reflect Art 22.1 GDPR).

5.3.3/rule 10.4 – we suggest removing "the" from "the marketers" in the first line.

5.3.4/rule 10.5 – we question the need for the wording after the semi-colon at the end of the proposed new rule. That wording seems intended to reflect the rules under the Privacy and Electronic Communications Regulations (PECR). Those Regulations deal with sending unsolicited electronic direct marketing messages rather than the processing of personal data.

5.3.5/Rules 10.6, 10.7 & 10.8 – agree, although since the proposed new rules are intended to reflect the requirements of PECR, we suggest the inclusion of wording in proposed rule 10.6 to make clear that it applies only to unsolicited electronic marketing messages.

5.3.6/Rule 10.9 – Art 9.2 GDPR provides that the prohibition on the processing of special category data under Art 9.1 does not apply if any of the exemptions listed under Art 9.2 apply. For example, in addition to the data subject having given explicit consent under Art 9.2(a), processing may also take place if it relates to personal data which are manifestly made public by the data subject under Art 9.2(e). We would suggest that the proposed new rule 10.9 makes reference to these exemptions so that they will apply if appropriate under the circumstances.

5.3.7/Rule 10.10 – agree, although, whilst the Background section makes clear that the rules relate only to data used for direct marketing purposes, we would ask whether proposed rule 10.10 should be amended to expressly refer to the type of marketing it is intended to cover (unsolicited electronic direct marketing messages, for example).

Further, we would ask whether, with regard to the third sentence, it should be made clear to whom no other marketing communications should be sent (for example, to consumers who have opted out of receiving marketing messages/communications).

5.3.8/Rule 10.11 – agree.

5.3.9/Rule 10.12 – agree.

5.3.10/Rule 10.13 – agree.

5.3.11/Rule 10.14 – agree.

5.3.12/Rule 10.15 – agree.

5.3.12/Rule 10.16 – the beginning of proposed rule 10.16 does not seem to accurately reflect Art 12.1 GDPR. Rather than requiring the controller to "ensure that the information provided….is intelligible", Art 12.1 requires the controller to "take appropriate measures to provide any information….in an intelligible….form."

5.4 Removal of Appendix 3

We agree with the proposal.

5 – More Partnership Ltd

This submission to the CAP is made on behalf of the Council for Advancement and Support of Education (Europe)'s (CASE) working group on GDPR and Fundraising Regulation.

Background

CASE is an international charity, headquartered in Washington, DC, USA and with a European base in London. It is the leading professional body internationally for those involved with Fundraising, Supporter Relations and Marketing in higher education. It also has a significant number of members from the secondary schools sector and from cultural organisations.

Its working group comprises volunteers from a wide range of member organisations, together with a representative from Universities UK and a number of consultants who work extensively in the sector. The author of this response – which has been agreed by the group – is one of those consultants.

Consultation response – rule 10.3

We have just one submission to make in respect of your consultation.

The proposed Rule 10.3 reiterates the requirements of GDPR Article 14 in respect of the provision of privacy information to a data subject whose data has been obtained other than from the data subject – i.e. from third parties.

We believe that, in incorporating the main thrust of Article 14, CAP has not taken into account two factors.

We believe the proposed wording needs nuancing insofar as the timing of the provision of the notice is concerned. We also believe that, since GDPR contains four exemptions to this provision, these exemptions should be referred to in Rule 10.3. It would be unfortunate if a Code of Practice removes the possibility of using exemptions which have been placed in legislation for good reasons.

Timing

Firstly, Article 14.3 contains three "triggers" in respect of the timing for the provision of the privacy information to the data subject. The first requires that data is provided within one month having regard to circumstances, the second that it is provided at the time of first communication with the data subject and the third if disclosure to another controller is envisaged. It is consistent with the remainder of the text of GDPR to read these three triggers as being of equal weight with none having priority over another. In other words, to read 14.3 as requiring a) OR b) OR c). The Article 29 Working Party guidance reads this section differently, as has your draft rule 10.3. Instead of "a) OR b) OR c)" you have proposed "a) AND [b) OR c)]" We believe the Article 29 WP reading may be an extension of the requirements of GDPR beyond that which is stated by the law.

This may appear a very minor change, but it matters. It matters when building a small list of potential donors in respect of whom an appropriate approach on a personal basis at an appropriate time is the best way to initiate communication between them and the charity. Sometimes the appropriate time does not occur within one month. If the notice MUST be provided within one month in all circumstances, then this has been liked to "walking up to someone you have not yet met and telling them that when the moment was right you were intending inviting them out on a date." This is not normal human behaviour.

Thus we believe that Article 14.3 need re-reading and the requirement with respect to the timing of the provision of a privacy notice included in the proposed CAP 10.3 should be more nuanced.

Exemptions

Article 14.5 provides four circumstances in which paragraphs 1 to 4 of Article 14 do not apply.

Some of these circumstances, in particular those referred to in 14.5 a) and 14.5 b), may apply to a small range of fundraising interactions, particularly those with high net worth individuals. The latter could easily apply if the “one month” provision of 14.3 a) were regarded as mandatory.

For these reasons we believe it is important that the code recognises and refers to Article 14.5 in order to allow Data Controllers to avail themselves of the exemptions which GDPR provides if they are needed in specific circumstances.

6 – SuperAwesome Trading Ltd

We understand that the purpose of this consultation is primarily technical, i.e. to ensure alignment of the CAP Code's provisions on data protection with the GDPR. This is welcome, and we have just one comment—detailed further below.

We would, however, like to take this opportunity to highlight to the Committee that there are material uncertainties around the practical impact of the GDPR on digital marketing practice, in particular when it comes to children. We hope that—soon after the May 25th deadline—the CAP will tackle these issues and work with the industry and the ICO to provide critical clarifications and practical implementation guidance, including:

- The definition of a "service offered to a child', as this has a direct impact on which websites or apps are in scope of your new rules 10.15 and 10.16.

- Guidance to advertisers on what marketing practices may be conducted under the Legitimate Interest legal basis when it comes to children, taking account of recitals 38 and 75 (that children deserve special protection).

We strongly encourage the ASA and the CAP Committee to engage with us and industry to fill the gaps remaining after the ICO's consultation on GDPR and Children from earlier this year.

The consultation

Regarding the current Consultation, we are in favour of all the proposed changes to the CAP Code, with one comment:

5.3.12 Rules 10.15 and 10.16: marketing to and collecting data from children

10.15 "Marketers must not knowingly collect from children under 12 personal data about those children for marketing purposes…" (emphasis added)

As you know, the age of digital consent under Article 8 of the GDPR is 16, unless individual EU member states choose to lower the age but in any case no lower than 13. The current draft of the UK's Data Protection Bill proposes to lower the age to 13 (not 12).

Given that in this consultation you are seeking to harmonise the CAP Code with the GDPR in all material respects, we think the age threshold for applying the protections of rules 10.15 and 10.16 should also be aligned with the GDPR.

Our recommendation is that this clause should read: *"Marketers must not knowingly collect from children under 16 (or such age as the UK determines in relation to Article 8 of the GDPR, but in any case no lower than 13) personal data about those children for marketing purposes…"*

The reasoning is (a) to avoid confusion for marketers who are trying to comply with the GDPR as well as the CAP Code, and (b) to align with the CAP Code's own definition of children, which —under Section 5—is anyone under the age of 16.

We hope you will take our comment in the spirit of constructive collaboration, and we continue to make ourselves available to work with you on this, or any other initiative in relation to marketing to children.

SuperAwesome background

By way of context, SuperAwesome is the leading provider of 'kidtech', technology and services used by companies worldwide to enable safe, compliant (COPPA, GDPR) digital engagement with children. We have over 200 customers who use our technology across industries including toy, film, entertainment and video games. From our London headquarters, our team of 130+ employees, including more than 35 software engineers, are developing and rolling out Privacy by Design technology focused on the needs of the childrens' digital media ecosystem.

Our technology is used by content owners (websites, apps), brands and agencies to comply with children's data privacy rules and appropriate content standards in each territory. In particular we serve advertisers and publishers who want to deliver advertising without collecting any personal data, and who wish to comply with COPPA in the US and GDPR in Europe when it comes to offering services to children.

Our advertising platform is connected to online services (ISSs) that serve an aggregate of 72M children and teenagers across the EU. Every advertisement delivered by our technology is watermarked with our SafeAd logo, which signifies that the ad (1) is not collecting any personal data (including persistent identifiers), and (2) has been reviewed by a human for age appropriateness.

In addition, our Kidaware education programme is used extensively by brands and agencies to train their employees in children's data privacy laws and advertising standards—we educated well over 150 UK digital media professionals in 2017.

Finally, we have been actively involved in working with the market and regulators in developing and implementing digital child safety policies, including:

- As board director of Mediasmart, where we design and distribute media literacy materials in schools.

- Contributing actively to earlier revisions of the CAP Code, in particular the April 2017 guidance on labelling and disclosure of native advertising aimed at children.

- Working closely with industry associations such as Toy Industries Europe (TIE), the World Federation of Advertisers, and the British Toy & Hobby Association (BTHA) to educate and advise their members on data privacy compliance.

- Submitting comments to Working Party 29 consultation on Profiling and Automated Processing, Transparency and Consent, and to the ICO consultation on Children and the GDPR earlier this year.

Our nearly 5 years of experience in building technology platforms for compliance gives us a unique insight into practical, technology-based solutions to the most difficult challenges, including age verification, parental consent, disclosure for kids, and assessing the relative risk of different tracking technologies.

SuperAwesome comments on ICO consultation: Children and the GDPR

Our comments address five areas of the consultation:

1. Definition of 'offered directly to a child'
2. When the Legitimate Interest basis may apply in relation to children
3. Parental consent verification methods

4. Reaffirmation of consents in the context of the Data Minimisation principle
5. Age verification solutions

When is an ISS (online service) 'offered directly to a child'?

The definition of child-directed service will determine which websites and apps are in scope of the law's provisions relating to children. Your guidance proposes a very broad interpretation, that any site accessible to children is in scope unless it makes clear efforts to prevent children using it.

We believe this is too broad and may have the unintended consequence of reducing protections for children. This interpretation would oblige nearly every website and app operator to implement age gates, or to seek ways of blocking child users. We believe this is counter-productive, for three primary reasons:

1. If the rule applies so broadly, it will be widely ignored or flouted by sites that are not relevant to children (and which are unlikely to be investigated). As a result, sites that have a mixed audience of children and adults (such as casual games websites for example) will be less inclined to comply, citing the many examples of non-compliance without consequence.

2. Children will come across an ever larger number of age-walls to visit any part of the web. As a result, they are likely to become accustomed (and trained) to circumvent them. We've seen this play out widely on social media platforms, whose age verification methods are routinely side-stepped by millions of under-13s.

3. It would lead to the majority of online services that are not harmful to children being closed off for children in a way that is likely to contravene their fundamental human rights, as expressed in articles, 12, 13 and 14 of the UNCRC and the Council of Europe's Guide to Human Rights for Internet Users. Such restrictions would also potentially mean the child suffers a detriment within the meaning of the GDPR.

In addition, these measures to block children would lead to the collection of additional and unnecessary data, including the ages of children, going against the data minimisation principle. These unintended consequences can be avoided with a definition that applies to fewer services, but with significantly less ambiguity.

The fact is the vast majority of digital services that are not for children are also of no interest to children. So there is little benefit from explicitly policing such services in the same way as we do sites where children (a) want to go and (b) face real risks of inappropriate data collection. We would therefore amend the definition of an ISS 'offered directly to a child' to mean a service that is both:

(a) accessible to children, and

(b) either appealing to children, or marketed to children.

This will capture nearly all services children are likely to use, either because they were drawn to them by their content, or because they were targeted in their promotion.

It also means that services that appeal to both adults and children, eg what we would call **'mixed audience'** sites, will have to decide whether they (a) are primarily child-directed and should treat all visitors as children, or (b) segregate their audiences by use of an age gate so

that they can provide differentiated services to children and adults whilst respecting the equal access principle.

Encouraging the concept of mixed-audience sites that age gate their users into two separate streams would enable, for example:

1. A casual game mobile app to age gate its site into over- and under-13s (in the UK), and to allow it to generate revenue compliantly from each audience segment by applying the appropriate monetisation method, eg traditional data-driven advertising to over-13s, vs zero-data, contextual advertising to the under-13s.

2. A toy company's product website to offer different sections for a visitor to navigate, such as a Kids page with content appealing to children, and a Parents' page that is age-gated and leads to product information and ecommerce functionality.

Legitimate interest

Much of the focus in relation to children is on Article 8 and the Consent basis for processing. We feel strongly that the market would benefit from clarification on how recitals 38 and 75 are to be interpreted when conducting a balancing test where children are the data subjects.

There should be very few scenarios where Legitimate Interest can be used as the basis for processing children's data. But there are clearly some that are legitimate - even necessary - activities of content owners, taking into account the risk of processing and the rights of the child (including their right to equivalent service from an ISS), for example:

Data type	Purpose	Examples	Risk	Legal basis
IP address or device ID or other technical identifier	Personalisation	Site remembers games scores, or user choice of background colour	Low	Legitimate Interest
IP address or device ID or other technical identifier	Analytics, security, internal operations	Pseudonymised (and often aggregated) data used by ISS to improve service, enable auto-scaling, provide business analytics internally	Low	Legitimate Interest
IP address or device ID or other technical identifier	To verify a user's age by checking the device against an ID database	A site not for children that wishes to confirm a user is over or under the age of consent	Low	Legal Obligation

IP address or device ID or other technical identifier	To serve advertising based on context of the site; to frequency-cap such advertising within the domain	An app or websites that funds itself primarily through advertising but does not collect PI from children.	Low	Legitimate Interest

You may recognise some of these scenarios, as they are similar to those called out by the U,S. Federal Trade Commission as specific exemptions under COPPA. Making it clear that these data processing activities can be considered Legitimate Interest or Legal Obligation even taking into account recital 38 would dispel many kids' publishers' serious concerns about how to comply. We would urge the ICO to provide further guidance with examples in a form similar to the above.

Parental consent

Where the legal basis is consent and the data subject a child:

> *you must make reasonable efforts, taking into consideration available technology, to verify that the person providing parental consent does, in fact, hold parental responsibility for the child. A reasonable effort [...] might therefore entail simply asking for a declaration that the user is old enough to provide their own consent, or a declaration of parental consent and responsibility, via a tick box or email confirmation.*

The Guidelines on Consent under Regulation 2016/679 (wp259) also recommend a "proportionate approach" when (a) confirming that a data subject is over the age of digital consent; (b) seeking parental consent; and (c) establishing the parental authority of the consent provider. This is to ensure sufficient verification whilst minimising the collection of personal data.

The GDPR's risk-based approach to verification is welcome. It echoes the US experience with proportionality under COPPA. In order to facilitate implementation, we strongly encourage you to provide specific examples of matching appropriate levels of verification to the actual risk of the data processing. This is particularly important in light of the GDPR's data minimisation requirement.

Based on our experience of working with thousands of children's online services, as well as building Verified Parental Consent workflows and technology for COPPA compliance, we propose the following practical framework as a guideline for any online service 'offered directly to a child', whether aimed at mixed or general audiences:

Type of data being collected	**Sensitivity**	**Examples of sites or apps**	**Appropriate method to verify user is <u>over</u> age of consent**	**If not, parental consent required?** **Appropriate verification method**
Sensitive Personal Information (health, ethnicity, tied to a name or ID number, etc)	Very high	Ancestry or healthcare service that stores user profiles with identity information and demographic/ ethnic/health data.	Neutral age gate, plus Database check against national registry, or Copy of photo ID submitted	**Identity-Verified Parental Consent (<u>w/</u> database)** 1. Parent provides consent 2. Statement by parent that he is the holder of parental responsibility; 3. Parent identity checked against national ID database, or by submitting copy of photo ID
Identifiable personal information, eg full name, address, national ID number; image/video uploads; free text content. Combination of online identifiers and profile information that can be used to identify a natural person	High	Social media app that allows use of real names, connections with strangers, free-text chat rooms Virtual assistant that records voice & stores it in cloud, builds useage profiles.	Double confirmation, eg Neutral age gate, plus Reconfirmation of birthyear; or, Two-factor confirmation, eg Neutral age gate plus Confirmation provided by email or text message	**Identity-Verified parental consent (<u>no</u> database)** 1. Parent provides consent 2. Statement by parent that he is the holder of parental responsibility; 3. Identity is confirmed by requesting credit card details and matching them against information provided (no transaction). Credit card information is then immediately deleted.
Technical online identifiers that cannot easily be resolved to a natural person, but are (a) shared with third parties, and/or (b) used for behavioural advertising & profiling,	Medium	Websites that allow behavioral or profile-based advertising. Virtual world, or games app that includes username registration,	Double confirmation, eg Neutral age gate, plus Reconfirmation of birthyear;	**Verified Parental Consent** 1. Parent provides consent; 2. Statement by parent that he is the holder of parental responsibility.

including geo-location Creation of a unique username (not PII)		leaderboards	or, Two-factor confirmation, eg Neutral age gate plus Confirmation provided by email or text message	
Enabling of notifications (eg, push) City-level geo-location information	Low	Apps that request permission to send push notifications; provide services based on city location (eg transport)	Confirmation that subject is over age of consent, via a simple, neutral age gate	**Direct Notice**. Opt-in, and direct notice sent to parent, stating type and purpose of collection and linking to Privacy Policy. No further verification of parental holder of responsibility
Technical online identifiers used for internal operations purposes only (analytics, contextual advertising, personalisation, security) Country-level geo-location information	Low	Casual games site with no registration, only contextual advertising	Processing on **Legitimate Interest** basis. No age check required.	Processing on **Legitimate Interest** basis. Parental consent not required. n/a
No data collection	None	Corporate website for marketing purposes, no advertising, no trackers	No age check required.	Parental consent not required. n/a

All of the above is of course subject to the prerequisite that the ISS fully discloses, and the data subject fully understands, the relevant data collection practices in compliance with the Transparency requirements of the GDPR, in particular when it comes to notices children can understand.

Example 1: educational website that finances itself primarily through advertising.
If advertising is delivered only contextually and no cross-domain tracking is allowed, then this represents Low sensitivity and would not require age verification or parental consent.

Publisher would have to ensure all technology and advertising partners are aware of child-directed nature of site and is responsible for guaranteeing that they are not collecting technical online identifiers that could be used to profile users. Social media plugins would not be allowed.

Example 2: mobile social application that enables chat, connecting with friends, sharing content under real names.
Use of real names, open text chat and the ability to connect with strangers make this High Sensitivity, eg a service that requires age verification and/or verified parental consent.

Example 3: virtual world that allows interactions between anonymous avatars.
Provided measures are in place to prevent disclosure of personal information (eg filtering out real names or phone numbers in unmoderated channels or chat rooms), then this represents Low sensitivity, with no verification or parental consent required.

Example 4: voice-based virtual assistant, or Internet-connected toy.
Given that audio files are likely to be stored and analysed in the cloud, and it is not technically feasible to filter out personal information in moderation, this represents High sensitivity and should require both age verification and Verified Parental Consent.

If the service provider can demonstrate that it is using any collected audio files solely for purposes of transcribing a command, and immediately deletes the audio files thereafter, we may consider this case Medium sensitivity, requiring only a simple opt-in + Direct Notice to parents.

Reaffirmation of consents

Your guidance describes the need for ISSs to obtain a direct consent from the user when a child reaches the age of digital consent. We are concerned that - if applied at all levels of risk of data processing - this would force service providers to collect more data than necessary, effectively contravening both the principle of data minimisation as well as the guidance on data retention.

For example, a toy company website or a virtual world that allows children to register anonymously, but does not collect any other personal information, would have to process a date of birth and contact information for the child when it comes of age, potentially even identity documents to verify that age. This hugely increases the amount of personal data collected, and the associated processing risk - surely not the intention of the regulation.

We recommend clarifying that a pragmatic approach is acceptable here: there should be no change to the validity of the already given (and parent-verified) consent until such time that a consent needs to be refreshed, or a new consent is requested, or the parent or child wishes to change or withdraw a consent. At that point a new age check would be conducted and - if the child is over the age of consent - the direct consent mechanism can take over.

Age verification

Your guidance introduces an additional age verification requirement, whereby service providers are obliged to check whether someone providing consent is legally old enough to do so. As you rightly point out, there are no easy technical solutions for this, in particular when we take into account:

1. The fact that 13-17 year olds lack many of the identity documents one might use for such verification; and,

2. The need to respect the GDPR's data minimisation principle, which speaks against collecting more 'hard identifiers' from young users in particular.

Furthermore,

> *You should be wary of mechanisms which involve detailed collection and retention of any individual's personal data as this raises further data protection concerns. It is preferable to use 'attribute' systems which offer a yes/no response when asked if an individual is over a given age, or if this person holds parental responsibility over the child.*

Please see our **Double Confirmation** approach in the table above for a method of implementing an 'attribute' system for Medium and High levels of data processing risk. However, we believe service providers would benefit from a clear statement from the ICO and the WP29 on (a) what types of processing would be permissible under such a confirmation, (b) whether there are situations that would require a more stringent type of age verification, and (c) under what circumstances the data minimisation principle is subsumed to the verification obligation.

Finally, the guidance makes reference to *"**Trusted third party verification services** [which] may offer solutions which minimise the amount of personal data the controller has to process itself."* Our company currently provide child-directed online services with much of the infrastructure needed to operate in compliance with data privacy laws, including third party verification services.

We would welcome a dialogue with the ICO together with other technology or service providers you may have identified to explore common industry standards for such trusted verification services.