

IAB UK response to the ICO's
'Update report into adtech and real time bidding'

December 2019



Table of Contents

1. Executive summary

2. Introduction

About the IAB

Background

3. Approach to IAB UK's response

Context

What IAB UK can do

Process

Timing

The role of the Transparency and Consent Framework

Next steps

4. Understanding RTB

The OpenRTB protocol

The Content Taxonomy

The IAB Europe Transparency and Consent Framework

5. Commentary on specific topics

Context-related information and special category data

Data sharing

Legitimate interests as a legal basis for processing personal data

6. IAB UK's response

Action taken

Detailed future action plan

A: Use of organisational/technical measures to secure data in transit and at rest, appropriate safeguards for international transfers and appropriate data minimisation and retention controls

B: Processing of special category data (SCD)

C: Reliance on legitimate interests (LI) for storage/access (cookies and similar technologies)

D: Legitimate interests legal basis

E: Data Protection Impact Assessment (DPIA) requirements

F: Transparency and fairness (information provided to consumers)

Further areas to explore

Next steps

7. Conclusion

1. Executive summary

- This paper responds to the Information Commissioner's Office (ICO) *'Update report into adtech and real time bidding'* published in June 2019.
- The ICO's message was clear: the digital advertising industry needs to improve its GDPR and ePrivacy compliance. All those involved in real-time bidding (RTB), including advertisers, intermediaries and media owners, need to understand and meet their data protection and privacy compliance obligations in practice.
- In this paper, we outline the process that IAB UK has undertaken to respond to the 'Update report', set out the actions that IAB UK and its members have committed to take, and identify areas where we believe further discussion is needed before a clearer position and consensus can be reached.
- IAB UK shares the ICO's goal of protecting personal data. We firmly believe that digital advertising and content are valuable economic drivers with major societal benefits – including underpinning the ad-supported internet – and that digital advertising and content can be delivered in ways that not only respect the law but also give users confidence and trust in how their data is being used. Based on our experience, we believe that most companies operating in the UK RTB market are responsible companies who take their compliance obligations seriously.
- As the trade body for digital advertising, we see our role as being to work with our members to provide responsible companies in our remit with standards and tools to facilitate legal compliance, responsible data use, and to ensure accountability.
- IAB UK and its members, along with IAB Europe and IAB Tech Lab (where appropriate), will work together and with other parts of the industry to deliver realistic, meaningful and collective change, and to demonstrate responsibility as an industry.
- When the ICO published its report, it committed to “a measured and iterative approach, so that we act decisively and transparently, but also in ways in which we can observe the market's reaction and adapt our approach accordingly”. IAB UK welcomes the ICO's careful consideration of the complex issues involved and its acknowledgement that third-party digital advertising is an ecosystem comprising multiple players contracting to support other important ecosystems, like news media.
- The ICO's process and approach allows for the necessary debate and discussion to inform the development of a realistic response. We have been very pleased that the ICO has been willing to engage with and work with the industry. Since the publication of the 'Update report', IAB UK and its members have been in dialogue with the ICO which, in our view, has been constructive and informative on both sides and has enabled the IAB to develop its realistic and meaningful proposals for change. We look forward to further dialogue and collaborative working with the ICO in 2020 as we continue to discuss a number of important issues and further develop our response.

- Maintaining a successful and sustainable industry that operates compliantly requires everyone to be willing to take action and to invest in making changes where necessary, within their own organisations and as part of the IAB. We are committed to playing our role in helping this to happen, and the industry needs to be too.



2. Introduction

This paper responds to the Information Commissioner's Office (ICO) *'Update report into adtech and real time bidding'* (referred to hereafter as the 'Update report') published in June 2019. It should be read in conjunction with that report.¹

The paper outlines the process that IAB UK has undertaken to respond to the 'Update report', sets out the actions that IAB UK and its members have committed to take, and identifies areas where we believe further discussion is needed before a clearer position and consensus can be reached.

Our response addresses the ICO's report in so far as it relates to general practices, and to the OpenRTB Protocol in particular. It does not address Google's proprietary Authorised Buyers protocol.

About the IAB

IAB UK (the IAB) is the trade association for digital advertising in the UK, with over 1,200 members comprised of the UK's leading media owners, technology providers agencies and brands, and a board comprised of 24 leading businesses in the sector. Our purpose is to build a sustainable future for digital advertising, a market that was worth £13.4bn in the UK in 2018.

The IAB is actively engaged in working towards the optimal policy and regulatory environment to support a sustainable future for digital advertising. We work with our members to develop and promote good practice to ensure a responsible medium. IAB UK is one of the 25 European national IABs that are members of IAB Europe, and one of the 41 national IABs that are members of IAB Tech Lab. These three bodies all work to support the digital advertising industries in the UK and beyond, and to develop standards and good practices across these markets.

IAB Europe brings together a European network of 25 national IABs, including IAB UK, which together represent roughly 5,000 companies from across the digital advertising and media ecosystem.

The IAB Technology Laboratory, Inc. (IAB Tech Lab) is a not-for-profit organisation that engages IAB member companies globally to develop and promulgate technical standards, software and services to support growth of an effective and sustainable global digital media ecosystem. Comprised of digital publishers and ad technology firms, as well as marketers, agencies, and other companies involved in interactive marketing, Tech Lab focuses on solutions that set industry standards on brand

¹ <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>

safety and ad fraud; consumer identity, data, and privacy; advertising experiences and measurement; and programmatic advertising. Importantly, for the ICO's purpose, Tech Lab is the organisation responsible for promulgating OpenRTB as a global protocol and developing the Content Taxonomy.

Background

In June 2019, the ICO in the UK published the 'Update report', which summarised the findings of its review of the use of personal data in the real-time bidding (RTB) process. In its report the ICO set out its observations about the processing of personal data in RTB with respect to the relevant provisions of the General Data Protection Regulation (GDPR)² (enacted in the UK as the Data Protection Act 2018) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). The 'Update report' focuses on, amongst others, six³ key points:

- Inadequate approaches to data security and managing the associated risks (including when sharing data with third parties), and the reliance on contracts for this purpose
- Processing of special category data without the requirement for obtaining explicit consent being met
- The use of legitimate interests for placing and/or reading a cookie or other similar technology (rather than obtaining the consent that PECR requires)
- Levels of awareness of the requirements for reliance on legitimate interest as a legal basis for processing personal data; specifically, the requirement to have properly carried out a legitimate interest assessment and implemented appropriate safeguards
- Levels of awareness of the need for the Data Protection Impact Assessment requirements in the GDPR (and specifically with regard to the ICO's Article 35(4) list of processing operations that would trigger a DPIA requirement) and the need to fully assess and mitigate privacy risks associated with RTB
- Information provided to individuals about data processing, particularly with respect to the transparency and fairness requirements of PECR and the GDPR

When the ICO published its report, it set out clear expectations about where the digital advertising industry needed to change, based on the areas listed above, in order to improve standards of compliance. At the same time, the ICO committed to take "a measured and iterative approach, so that we act decisively and transparently, but also in ways in which we can observe the market's reaction and

² Throughout this document we refer to GDPR, rather than the DPA, for simplicity.

³ While nine issues are summarised at the end of the 'Update report', they fall within the same six key areas.

adapt our approach accordingly”.⁴ This was in recognition of the complexity of the market, the number and variety of organisations and technologies involved, and the “importance of advertising to participants in this commercially sensitive ecosystem”.⁵

As part of that approach, the ICO announced a further six month period of industry engagement to “continue to gather information and engage with the industry to further enhance our knowledge”.

IAB UK welcomes the ICO’s careful consideration of the complex issues involved and its acknowledgement that third-party digital advertising is an ecosystem comprising multiple players contracting to support other important ecosystems, like news media. The ICO has also recognised this is a highly interconnected market and challenged the digital ad ecosystem to work together on a response. IAB UK wants to ensure that next steps are designed so that companies operating in the RTB ecosystem cannot merely operate in compliance with GDPR and ePD, but can also compete fairly and thrive.

The GDPR’s legislative process provided few opportunities to surface the complexities of how ecosystems comply with GDPR, so we welcome the opportunity for that dialogue now. The ICO’s process and approach allows for the necessary debate and discussion to inform the development of a realistic response. We have been very pleased that the ICO has been willing to engage with and work with the industry. Since the publication of the ‘Update report’, IAB UK and its members have been in dialogue with the ICO to better understand the findings of its review process; to provide information and insight about some particular aspects of the RTB process and ecosystem, and how they work; to clarify our shared understanding of the salient issues; and to identify potential ways forward, involving IAB UK and/or IAB Europe and IAB Tech Lab, and member companies.

⁴ <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-ico-adtech-update-report-published-following-industry-engagement/>

⁵ *ibid*

3. Approach to IAB UK's response

We believe that real time bidding can be conducted in a way that is compliant with GDPR and PECR. Based on our experience, we also believe that most companies operating in the UK RTB market are responsible companies who take their compliance obligations seriously. We recognise that there are limits to our sphere of influence, and also that there are some organisations who may choose not to acknowledge or respect their compliance obligations. These companies are not doing the marketplace any service, and ultimately, addressing this will require a combination of regulatory and self-regulatory measures.

IAB UK also recognise that due to the number and variety of companies operating in the UK digital advertising market, and their varying size, experience and functions, it is important to build a shared understanding among all companies of what is required by GDPR and PECR, and how to comply with these requirements in practice. Many companies operating in good faith have wrestled with questions about how to best meet their legal requirements, and how to operate in a distributed and interdependent marketplace where managing compliance in the full supply chain of their data is dependent on the cooperation of a wide range of partners and clients.

We believe that IAB UK has a role to play in addressing this disparity and meeting these challenges by helping to provide member companies with more specific guidance on how to interpret what the requirements of the principles-based GDPR mean in practice, in the context of their activities.

As part of our work to support members in preparing for GDPR implementation ahead of May 2018, IAB UK developed briefings and resources for members and ran educational workshops. Throughout that programme of education, we have consistently communicated that:

- PECR remains in effect alongside the GDPR, and requires consent (as defined by GDPR) for access to/storage of information on a device
- Reliance on Legitimate Interest as a legal basis is subject to carrying out a Legitimate Interest Assessment. IAB UK contributed to the DPN's guidance on LI and publicised it to members⁶
- Organisations will need to complete a Data Protection Impact Assessment (DPIA) if they process personal data using 'new technologies' or if the personal data processing is likely to present a 'high risk' to the user
- All relevant organisations should adopt the Transparency and Consent Framework (TCF) as a tool to support compliance with the GDPR and PECR

⁶ <https://www.iabuk.com/policy/iab-uk-supports-updated-dpn-guidance-legitimate-interests>

Context

One of the objectives of the GDPR was to create a harmonised data protection law across the EU, for the benefit of individuals and for data controllers and data processors, many of whom operate across multiple markets. The introduction of a single set of rules was the driver for the development of Europe-wide approaches to managing GDPR compliance through the Transparency and Consent Framework (TCF)⁷ launched in early 2018.

IAB UK, IAB Europe and IAB Tech Lab have a shared goal to develop industry approaches to data protection and privacy compliance that can be applied in a harmonised way at EEA level, to maintain the consistency envisaged by the GDPR. At the present time, there is fragmentation and competing interpretations of key elements of GDPR among national Data Protection Authorities (DPAs), which slows down and holds back standard-setting initiatives, especially in such a highly interconnected ecosystem as digital media and its supporting technologies.

IAB UK members are drawn from across Europe and globally. While the ICO is the lead DPA for some of our members, many have their lead DPA in other EU markets, and rely on the harmonisation principle of the GDPR being largely upheld in practice in order to be able to apply consistent, EEA-wide approaches to privacy compliance for their customers and within their businesses. We urge the ICO to, as far as possible, coordinate its activities with other DPAs who are actively undertaking work on digital advertising, and involve DPAs that are not currently focusing on this area. Harmonising regulatory approaches across the EEA will make it easier for companies to comply with the GDPR and to reduce non-compliance. Conversely, fragmentation will have the opposite effect and has the potential to be exploited by less scrupulous market participants.

What IAB UK can do

IAB UK shares the ICO's goal of protecting personal data. We firmly believe that digital advertising and content are valuable economic drivers with major societal benefits – including underpinning the ad-supported internet – and that digital advertising and content can be delivered in ways that not only respect the law but also give users confidence and trust in how their data is being used. Operating in the digital advertising market and respecting privacy are not incompatible.

As the trade body for digital advertising, we see our role (and that of IAB Europe) as being to work with our members to provide responsible companies in our remit with standards and tools to facilitate legal compliance, responsible data use, and to ensure accountability, i.e. by setting out examples of what may be appropriate legal

⁷ <https://iabeurope.eu/transparency-consent-framework/>

and technical approaches to achieving compliance with GDPR and ePrivacy legislation (while recognising that individuals companies remain accountable for deciding what approaches they should take in practice). This has been the foundation of our engagement and dialogue with the ICO.

Process

IAB UK established an ICO Working Group comprised of board member representatives to inform and agree our approach to responding to the ICO's report, and to engage in detailed discussions internally, and with the ICO. This group has worked closely with the equivalent Working Group, which was established by IAB Europe to respond to the aspects of the 'Update report' that relate to the TCF. IAB UK has supported the work of these groups through technical meetings and discussions with our wider membership, and by engaging external experts in ad tech and privacy to provide legal and technical expertise and help guide our response.

The IAB UK and IAB Europe Working Groups have jointly engaged in dialogue with the ICO through a series of in-depth meetings and discussions over the last six months, covering the topics identified in the 'Update report', along with others that have arisen during those conversations (such as cookie walls). In our view, this dialogue has been constructive and informative on both sides and has enabled the IAB to develop its realistic and meaningful proposals for change. We look forward to further dialogue and collaborative working with the ICO in 2020 as we continue to discuss a number of important issues and further develop our response.

During the last six months we have issued regular updates to our membership at large and in November 2019 we consulted them on our proposed actions set out in section 6. Our members have been supportive of our approach and our proposals. We also hosted two member events, one of which the ICO spoke at, to talk about the details of the ICO's report; explain our approach and proposed response; seek members' feedback; and answer members' questions and concerns. We will continue this communication and engagement in 2020.

It is important that there is a collective industry response to the ICO's concerns, which have implications for all participants in the RTB ecosystem, from advertisers to media owners and everyone in between. We also want to ensure that, where possible, responses from different parts of that ecosystem are coherent and aligned. We have therefore also engaged with other trade bodies as they develop their responses to the ICO report, including the Advertising Association (via its Digital Advertising Working Group), ISBA and the DMA, the AOP, and the IPA, and look forward to continuing to work together in 2020 on areas of joint interest as we take forward our actions.

Timing

Through this response to the 'Update report' we are committing to taking a number of steps to address the ICO's concerns, in order to both enhance industry participants' knowledge and understanding of the law and its practical application in relation to RTB, and to improve standards of compliance.

The responses we are putting forward are designed to deliver change across the whole industry, through a phased approach comprised of both short term priorities and longer term workstreams. In the short term, our areas of focus are broadly: data security; special category data; the consent requirements in PECR and the GDPR relating to storage of, or access to, information stored on a device (i.e. cookies and similar technologies - i.e. issues A, B and C detailed in section 6).

We have developed a phased approach in order to be able to take action in the short term to address priority areas, while allowing the necessary time to develop appropriate and sustainable solutions to the more complex issues. It is also important that we work to a timetable that allows for meaningful change to be designed and implemented effectively by companies in the industry. IAB UK will support members to deliver the changes proposed in this paper through, for example, providing education and training to complement guidance and standards.

The role of the Transparency and Consent Framework

Throughout our dialogue with the ICO we have been clear that the Transparency and Consent Framework, as an EU/EEA-wide industry standard built on the requirements of GDPR and the ePrivacy Directive (ePD), has a critical role to play in addressing the issues raised in the 'Update report'.

TCF version 2.0 was released to the market in August 2019 and contains a number of improvements that address many of the ICO's observations and will benefit individuals as well as those companies that are using the TCF. These are detailed in section 6. The TCF has always been designed to be an evolving, iterative standard and TCF policies and specifications could be adapted to address other areas of data protection and privacy issues as the common interpretation of GDPR evolves. Companies are currently in the process of investing significant resource and engineering commitments required to implement version 2.0 of the TCF, due to go live by the end of April 2020.

Next steps

We believe that the constructive proposals we have developed demonstrate the UK digital advertising industry's commitment to compliance, addressing issues of critical importance to our users and regulators. We are committed to working with

relevant members to deliver the actions set out in section 6 of this report.

Our work during the last six months, including our engagement with the ICO, has identified some issues where more information and discussion is needed before a clearer position and consensus can be reached. These include the use of legitimate interest as a legal basis for processing personal data under GDPR where consent has been gained for access and storage prior to such processing, and some aspects of the discussions around special category data, along with the question of conditionality of access to content ('cookie walls'). We will continue to engage with the ICO on these topics in 2020.



4. Understanding RTB

Real-time bidding (RTB) is industry architecture that allows for maximum economic value to participants within a distributed marketplace. Ad exchanges connect buyers with publishers, conducting a real-time auction for each ad impression. This system enables participation by buyers and sellers from the largest brands and publishers to more niche advertisers and content providers. OpenRTB is the most common protocol by which this economic activity occurs. A protocol is simply a standard set of technical parameters that allow for communication and interoperability.

OpenRTB, like most technology standards (including things like Bluetooth, WiFi or USB), is not in itself a processing activity. Rather, it is used to enable an organisation's processing activities (the purposes of which are determined by the organisation, if it is a data controller). It is the organisation's obligation to use such technology responsibly and in compliance with applicable law. That said, industry associations such as IAB UK can play a critical role in helping companies leverage standards, such as OpenRTB, in a legally-compliant and appropriate way.

The OpenRTB protocol

OpenRTB is a global technical protocol which is promulgated by the Tech Lab. It is comprised of a set of specification documents (i.e. OpenRTB 3.0 - a transactional specification, and AdCOM 1.0⁸ - a 'business object' specification) and allows implementing organisations to carry out the following objectives in a standardised and interoperable way:

- Transmitting of bid requests from supply-side sources (e.g., SSPs) to demand-side sources (e.g. DSPs)
- Collection of bids in response to such bid requests
- Sending of "win" notifications to winning bidders
- Transmission of advertisements for display to individuals

With the exception of a unique ID for the bid request (as opposed to a unique ID for the end user), OpenRTB requires very little specific bid request data. The protocol does not determine what data is transmitted, only how it is transmitted. The AdCOM specification, that can be used in conjunction with OpenRTB 3.0, expressly identifies where a data point is 'required'. Device data, geolocation data and other data categories referred to in the 'Update report' are not identified as 'required', as such

⁸ Advertising Common Object Model (AdCom). AdCOM defines the media to be transacted, to be used with a transactional specification like OpenRTB 3.0. AdCOM describes the ad, the creative, and the media channels that are traded over OpenRTB transactions and be used, for example, to give publishers control over the creative to be served on their page.

data does not relate to the minimal technical information needed to allow an RTB transaction to run.

OpenRTB can be used to send bid requests containing what could be considered under the GDPR to be personal data. However, decisions regarding what personal data to include within a bid request (if any), and to whom such personal data shall be shared or made available to, are made entirely by implementers of the protocol. These implementers can also use compliance mechanisms, such as IAB Europe's Transparency and Consent Framework, to help fulfil their jurisdiction-specific compliance obligations.

Implementers of OpenRTB can themselves determine whether and, if so, under which conditions particular fields are used to account for the jurisdictions in which they operate. This allows OpenRTB to be used in compliance with whichever laws are applicable to data controllers and processors using the standard. For example, if explicit consent is required before Content Taxonomy fields that may include or constitute special category data can be used in relation to users sitting in the European Union, and such explicit consent cannot be collected, organisations can deactivate these fields within bid requests with relative ease due to the flexibility of the protocol.

The Content Taxonomy

The 'Update report' raised some concerns about the IAB Tech Lab Content Taxonomy. The express purpose of this taxonomy is to provide publishers with a standardised way to tag and organise their page content, and has proven to be a helpful resource to save publishers the operational and technical resources of having to do this themselves. This taxonomy is included in the AdCOM/OpenRTB specifications and the ID values are sometimes used in OpenRTB bid requests from an SSP (on behalf of a publisher) to a DSP to inform the type of content where an ad might appear. However, most DSPs decide not to use this signal in the process of making bid decisions. Instead, most rely on external contextual targeting services that specialise in semantic analysis (this also helps to ensure consistency across SSPs). That said, the Content Taxonomy can be used for the following use cases:

- **Targeting:** In some cases, a smaller DSP might not have the resources to work with a specialised semantic analysis partner, or may have proprietary approaches to analyse/filter content taxonomy signals when used to target certain types of inventory
- **Brand safety:** Advertisers often seek to avoid illegal, offensive, or otherwise undesirable categories due to negative brand associations
- **Avoidance:** Advertisers often wish to avoid views on specific content categories, or DSPs may wish to avoid bidding (on behalf of their advertiser clients) on

requests referencing sensitive categories that could be inappropriate from a targeting perspective

The IAB Europe Transparency and Consent Framework

Following adoption of the GDPR in April 2016, IAB Europe and national IABs worked together to develop the Transparency and Consent Framework (TCF), in collaboration with IAB Tech Lab and companies across the digital advertising ecosystem.

The TCF facilitates digital advertising and content companies' compliance with the principles of the GDPR – including lawfulness, fairness and transparency, purpose limitation and data minimisation – and with the consent requirements of the ePD. It is the result of an unprecedented collaboration over nearly three years between buy-side, intermediary and sell-side actors (e.g. agencies, advertising technology companies and media owners and publishers) to achieve a common solution that works for all players. The long term goal is that this standard will be adopted widely by all players that process personal data used in the third-party digital advertising ecosystem.

The TCF is a protocol comprising a set of policies and technical specifications, and underpinned by terms and conditions for registered companies. It was conceived as an open-source, cross-industry standard to support organisations that process personal data in order to deliver advertising on their sites or to personalise content. The TCF provides a mechanism that enables first parties (digital media and other websites) and third parties (vendors acting as data controllers or processors) to establish a GDPR legal basis for that processing, and (in accordance with PECR requirements) to obtain prior consent to store information on a user device or access already stored information.

In the case of the consent legal basis, the TCF works by giving users the opportunity to provide prior approval to a limited set of third parties whom they are comfortable to have process their personal data or access information on their devices, for a limited set of defined, disclosed purposes and with all the rights and obligations that accrue to users under the GDPR. In the case of legitimate interests legal basis, the TCF provides a standardised means of making the required information disclosures and, as from version 2, integrates “right to object” functionality that is a condition for legality of the legitimate interests legal basis. It provides users with information and control over how their data may be used, and by whom. The information disclosures must be made using standardised wording. Similarly, the TCF provides a standardised means for recording the user's choices and communicating them to other parties in the delivery chain so that those parties understand their own prerogatives and can appropriately protect and process the user's personal data and

access user devices, as the case may be.

The purpose and benefits of the TCF are to:

- Enable vendors (i.e. data controllers) to establish an appropriate GDPR lawful basis to process personal data. No consent signal must be generated prior to an 'affirmative act'
- Implement GDPR-defined consent for ePD compliance
- Provide full transparency into which vendors are seeking to access devices and process personal data, and for what purposes
- Provide control to publishers over the vendors operating on their sites and apps, so that processing can be proportionate
- Create standardised signals to enable accountability
- Establish minimum criteria for the consent and transparency user interface, including disclosure of vendors and purposes, plus privacy policy links and information about legal bases relied on

The TCF is a world-leading initiative and the only advertising industry transparency and consent framework built to respond to GDPR. In less than two years it has become the industry standard, with over 500 registered 'vendors' and over 130 registered and verified Consent Management Providers. The TCF also represents a pan-European set of policies and technical protocols to help companies achieve key compliance objectives under the GDPR and national implementations of ePD.

The long term goal is that every relevant organisation is signed up to, and puts in place plans to implement, version 2.0 of the TCF.⁹ It is important for organisations to be aware that the TCF is a tool that can help them meet the consent and transparency requirements of the GDPR and the ePD (and as from v 2.0, will provide a complete accommodation of the legitimate interests legal basis). Companies remain individually accountable for ensuring that they are implementing TCF correctly, and that they are complying with all relevant provisions of the GDPR and the ePD in practice.

⁹ For further information see <https://www.iabuk.com/policy/transparency-consent-framework-20-launches> and to find out more, and register, visit <https://iabeuropa.eu/transparency-consent-framework/>

5. Commentary on specific topics

Context-related information and special category data

The 'Update report' refers to special category data that is being processed in RTB bid requests, based on the fact that the Content Taxonomy contains categories that relate to topics such as health, religion, etc. that are often used to populate the site object field 'site.pagecat' (as defined in the OpenRTB Protocol).

Special category data is data that falls within the scope of the GDPR, i.e. is personal data (information that relates to an identified or identifiable individual), and that either:

- Reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership
- Concerns health, a person's sex life or a persons' sexual orientation
- Is genetic data
- Is biometric data (where used for identification purposes)

GDPR provides that such data merits higher protection, not just due to its sensitive nature, but because the misuse of this data could create significant risks to the individual's fundamental rights and freedoms. Processing is only permitted if one of the specified conditions set out in Article 9 of the GDPR are met (the only one that is applicable to RTB is explicit consent).

We believe that context category fields such as those detailed in the Content Taxonomy, that may be included in a bid request, do not in themselves constitute special category data because, on their own, they do not reveal information about the individual user, or concern their health, sex life or sexual orientation. Rather, they are derived from categorising the nature of the environment (e.g. surrounding page content) where the ad impression has become available. The nature of the environment is independent from the user and cannot be attributed to the user by default.

Whether the content-based data in a bid request constitutes personal data on the basis that it can identify a person, directly or indirectly, will depend on what other data the company in question holds or has access to. It is for each organisation to then assess whether it is, or may be, processing special category data as a result of receiving content-based data.

However, we also recognise that there are risks that information that is not special category data at the point of collection could potentially become special category data depending on how and by whom it is processed (e.g. as a consequence of collating and/or drawing inferences from non-special category data). We believe that

there are ways in which to minimise such risks in RTB, for example by limiting or flagging certain data that is included in bid requests in order to help minimise those risks. See section 6 for more details.

We are aware that IAB Tech Lab is separately undertaking a global review of whether protocol implementers should provide additional metadata within the parts of the content taxonomy that could be considered sensitive. That signal could be used by SSPs and DSPs downstream to inform whether or not they choose to assign a behavioural attribute to an identifier, based on repeated viewing of certain types of content.

Additionally, we are committing to a workstream that will explore other factors that can contribute to the potential risk of special category data being processed without explicit consent. As part of this work we will need to explore when, and in what circumstances, 'factual' data becomes or could become personal data, and specifically special category data.

Data sharing

The 'Update report' concludes: "The profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bid request, all without the individuals' knowledge". It is important to clarify that, while bid requests are shared with companies who have been disclosed to individuals in advance, these are not profiles. A bid request is a set of information, only some of which may be personal data.

If a bid request uses the OpenRTB protocol then it can contain five broad types of information:

- **Regs:** contains any known legal, governmental, or industry regulations that are in effect
- **Site:** used to define an ad supported website, in contrast to a non-browser application, for example
- **User:** contains information known or derived about the human user of the device
- **Device:** provides information pertaining to the device through which the user is interacting
- **Geo:** encapsulates various methods for specifying a geographic location. Usually derived from IP address, though may come from native latitude/longitude when in-app

Much targeting of advertising via RTB is based on identifying those users whose user IDs have been placed into an audience 'segment', e.g. 'auto-intender' (which could be based on user IDs that have recently visited a site aimed at car-buyers, for example), that matches a buyer's target audience. However, these determinations

are typically proprietary and typically not shared as part of the OpenRTB process. As such, we maintain that to refer to detailed profiles being shared among hundreds of organisations for any one bid request is not an accurately reflection of what happens in practice.

Legitimate interests as a legal basis for processing personal data

In its 'Update report', the ICO questions whether data processing as part of RTB can be based on the legitimate interests legal basis, in part because such data processing is often facilitated by access to or storage of information that falls within the scope of PECR.

We see PECR and its scope (privacy of electronic communications) as separate to the GDPR's scope (personal data). PECR Regulation 6 (1) states that:

... a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met...

Paragraph (2) goes on to describe the consent mechanism, and the GDPR specifies what constitutes consent.

We are in no doubt as to consent being the required legal basis for access and storage under PECR. However, the prohibitions set out in PECR Regulation 6 (1) apply only to those instances in which information is actually stored or accessed on the user terminal itself. In our view, storage and access for the purpose of dropping cookies (or similar technologies) is separate from subsequent processing of personal data with reference to those cookies (and indeed, the two are regulated by two different legislative instruments at EU level and under UK law). Some data processing may also be carried out without reference to the cookie (or other similar technology).

As such, our view is that this subsequent processing of personal data is subject to the legal basis provisions of the GDPR. Legitimate interest is therefore a possible legal basis for processing personal data in these circumstances (if the other conditions for its use set out in the GDPR are met). It is also important that each data processing purpose is considered separately, and an appropriate legal basis determined and established for each – which may be consent, but may also be legitimate interests (subject to the relevant conditions and requirements for using this legal basis). There are a number of different types of data processing associated with RTB, from targeting to analytics, and consent may not be the most appropriate legal basis for all of these activities.

We welcome the opportunity for further discussions with the ICO on this subject as we continue our dialogue.

6. IAB UK's response

IAB UK is proposing action on the six key issues from the 'Update report', which can be summarised as:

- A. Use of organisational/technical measures to secure data in transit and at rest, appropriate safeguards for international transfers and appropriate data minimisation and retention controls
- B. Processing of special category data
- C. Reliance on legitimate interests (LI) as a legal basis for storage / access (cookies and similar technologies)
- D. Legitimate interests legal basis
- E. Data Protection Impact Assessment (DPIA) requirements
- F. Transparency and fairness (information provided to consumers)

We have developed these proposals in discussion and consultation with relevant members, and early versions have been shared with the ICO to encourage discussion. Where this section refers to actions by the ICO, these are 'in principle' positions that have been agreed as part of our ongoing engagement but not necessarily yet endorsed by the ICO.

The actions can be broadly characterised as follows:

- TCF-related (subject to adoption under TCF governance processes):
 - Extensions of TCF v2.0 policies and/or adopting best-practice recommendations to respond to regulators' feedback, or to accommodate aspects of the GDPR that the TCF does not directly implement yet
 - Future TCF functionality and/or policies – whether obligatory, or for voluntary adoption on an interim basis
- Protocol-based solutions and associated policies (e.g. in the case of special category data)
- Education, via guidance and good practices, on meeting the requirements of the GDPR and ePD/implementing legislation, reflecting existing TCF functionality, policies and Ts&Cs, and any other agreed solutions identified as part of this work
- Guidance developed by IAB UK on the application in the EEA of Tech Lab-owned global protocols and taxonomies in a GDPR-compliant way, including anticipated changes (referred to in the following section)

Action taken

Since the 'Update report' was published, IAB UK and IAB Europe have taken action to help support change in the industry both in the short and longer term. This includes:

TCF:

- The launch of version 2.0 policies and technical specifications, for implementation in 2020 (see section 3)
- Adding a new requirement to the vendor registration for version 2.0, so that vendors declaring legitimate interest as a legal basis for processing personal data confirm that they have carried out a legitimate interest assessment in respect of that processing
- Execution of a CMP validation programme to check compliance of version 1.0-registered CMPs with the TCF policies and technical specifications
- IAB UK and IAB Europe have initiated a joint workstream (subject to TCF governance processes) to develop additional commitments in relation to data security for future integration into the TCF policies; extend the existing requirements; and support companies with template due diligence questionnaires and other tools to enable them to comply with those commitments
- IAB Europe and IAB UK are currently working to develop template legitimate interests assessments (LIAs) and data protection impact assessments (DPIAs) for digital advertising and digital media that could be enlisted as tools to standardise approaches and encourage good practices in these assessments
- IAB UK and IAB Europe are continuing to promote the TCF to the market and encourage all companies to whom it is applicable to implement the TCF
- IAB Europe has begun a workstream to seek European Data Protection Board (EDPB) endorsement for a GDPR trans-national Code of Conduct based on the TCF

Data contained in bid requests

We have carried out work in the short term related to minimising the potential risks that content categories can pose. Used in bid requests to describe the page context of an impression, content categories could be associated with user IDs or other personal information and inadvertently become special category data (for example, if combined with other data over time and used to draw inferences), which cannot be processed without the user's explicit consent.

To address this we are working to develop 'rules' for the UK market to minimise the inclusion of content category data in a bid request when it is generated (i.e. in the site object field 'site.pagecat', that draws on the IAB Tech Lab Content Taxonomy) and we will publish our proposals shortly.

Additionally, in response to the 'Update report', IAB Tech Lab, via the relevant Working Groups, has been carrying out work looking at the Content Taxonomy and Audience Taxonomy to see whether there are amendments that could be proposed, or guidance developed on the application of these products, that respond to market

needs related to privacy and data protection. Tech Lab will publish more information to the market about the conclusions of this work and next steps in the first quarter of 2020.

Guidance

IAB UK has also begun work on developing guidance for companies engaged in RTB on some of the core aspects of GDPR and PECR compliance, to help them understand and interpret these legislative requirements in the context of their own processing activities.

Detailed future action plan

This section sets out the actions that IAB UK is committing to, with reference to the six key areas in the 'Update report'. For each issue, we have identified some agreed **principles** that will underpin specific **actions**, which will themselves form a set of **'deliverables'**.

Within this plan are some actions that are intended to provide the basis for future discussion with the ICO, which may themselves generate further actions in the future.

A high-level Project Initiation Document (PID) will be drafted by IAB UK that underpins each workstream. The PID will include standard project planning components, including timelines and milestones. This PID will be shared with the ICO, and the ICO has agreed to liaise with IAB UK to provide feedback as required.

Note: The scope of these actions is companies within the ICO's jurisdiction. For companies that carry out cross-border processing, these actions relate only to UK-based data controllers whose lead supervisory authority is the ICO.



A: Use of organisational/technical measures to secure data in transit and at rest, appropriate safeguards for international transfers and appropriate data minimisation and retention controls

Principles

UK data controllers, including IAB UK members:

- Must have adequate technical and organisational measures in place to secure data in transit and at rest
- Must retain personal data for no longer than is necessary for the purposes for which the personal data are processed and for which a legal basis has been established
- Should carry out due diligence prior to contracting with third parties with whom they wish to share data, and ongoing monitoring of those third parties following contracting, considering the security and retention risks associated with the processing to be undertaken by the third party

UK data controllers, including IAB UK members, should take measures to ensure that third parties (including both data controllers and processors) with whom they wish to share data, have and maintain appropriate technical and organisational measures to secure data. Such measures could include, but are not limited to, direct due diligence processes (such as a written questionnaire or other assessment), or confirmation of the third party's participation in a standardised compliance mechanism (such as a third party audit against a standardised framework, or participation in an appropriate Code of Conduct).

UK data controllers may choose to share information with the ICO that demonstrates the measures they have taken in response to a relevant request from the ICO, even when not legally required to supply such information.*
(*where the controller is within the jurisdiction of the ICO and the request is made pursuant to the ICO's regulatory powers).

Actions

IAB UK will identify good practices that will support its members to undertake a risk-based approach to assessing the risks of sharing personal data with third parties, addressing both security and retention.

It will incorporate these good practices into new material for its members, including:

- Guidance* on security and retention

- Guidance* on appropriate storage and retention policies/practices (including determining retention periods)
- Supporting material, for instance risk-based assessment methodologies, triage criteria, template questionnaires and retention schedules

The ICO will liaise with IAB UK to discuss its understanding of good practices regarding security and retention, and provide feedback as required.

*Note: In some cases, IAB UK may identify existing guidance which addresses the areas in scope, and make reference to that instead.

Deliverables

IAB UK will initiate a workstream to deliver the agreed actions regarding security, data minimisation and retention.

As part of this workstream, and in conjunction with IAB Europe, IAB UK will initiate a workstream within the TCF to propose possible new/additional requirements for integration into the TCF policies* to enhance the existing requirements for due diligence by data controllers intending to share users' personal data with other data controllers or processors, and the expectations on members to regularly monitor adherence to contracts.

*Note: TCF policies changes are subject to the relevant TCF governance processes.

B: Processing of special category data (SCD)

Principles

In the vast majority of cases (though not all), UK data controllers, including IAB UK members, do not need to, and should not, process SCD during the ad serving process, either:

- Directly as part of bid requests
- Through obtaining data from third party sources
- Through the generation of inferences from non-SCD data

Where SCD does not need to be processed, and where content category labels are used to populate bid request fields, these should not include labels that are obviously 'sensitive' and at risk of becoming SCD when associated with a user.

Where processing of SCD is envisaged, (for instance, in the context of delivering advertising on an online health publication) members will identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

UK data controllers, including IAB UK members, should not be using non-SCD to make inferences about individuals, including through building profiles and audience segments, that effectively create SCD about these individuals.

Actions

IAB UK will identify categories or tiers within the Content Taxonomy version 2.0 that would clearly become SCD when associated with a user and provide UK-focused guidance (as described earlier in this section of the response).

IAB UK will educate its members on the restrictions on processing SCD and enhanced requirements associated with choosing to seek to process this data.

IAB UK will work with other relevant trade bodies to provide specific guidance that targets advertisers/buyers, articulating the position that their members must not target segments that could constitute SCD unless explicit consent has been obtained.

IAB UK will solicit use cases from members that are processing SCD and utilising explicit consent. IAB will seek to generate (possibly anonymised) case studies from these use cases, outlining how this can be done. The ICO will liaise with IAB UK and provide feedback as required. If no such cases are forthcoming, IAB UK and the ICO will consider if and how to communicate the absence of such volunteered cases.

Deliverables

IAB UK will initiate a workstream to deliver the agreed actions regarding SCD. This workstream will include (but not be limited to) the following activities:

- Work with IAB UK members, specifically publishers, to obtain agreement on the principle of limiting risk of creating SCD from URLs
- Identification of controls to minimise the risk of creation and sharing of SCD via referred URLs, including engagement with brands/agencies (buyers) and 'brand safety' and 'anti-fraud' service providers, to minimise potential impact of changes to how URLs are processed on effective implementation of brand safety/ad placement and anti-fraud controls
- Work to pilot these controls with publishers, buyers and other stakeholders
- Work to address the risk of SCD being inferred from non-SCD, including the development of education and guidance as well as design and roll out of controls

C: Reliance on legitimate interests (LI) for storage/access (cookies and similar technologies)

Principles

Data controllers must obtain PECR- and GDPR-standard consent for storage of information on a device, or access to information stored on a device (e.g. cookies and other similar technologies) unless an exemption applies.

Legitimate interest is not an available legal basis for such storage/access (without prejudice to establishing a legal basis for subsequent data processing).

Note: Consent is the only available legal basis for 'storage and access' under TCF v 2.0

UK data controllers, including IAB UK members, that use cookies and similar technologies must provide clear and comprehensive information about the purposes of any cookie/similar technology; and obtain consent for storage/access that is not strictly necessary unless an exemption applies.

Actions

IAB UK will educate its members on the requirements of PECR, utilising the ICO's recently released 'Guidance on the use of cookies and similar technologies', and promote the use of the TCF, where appropriate, for obtaining consent in accordance with PECR/GDPR requirements.

D: Legitimate interests legal basis

Principles

All UK data controllers, including IAB UK members, that wish to rely on legitimate interests as a lawful basis for any processing that they undertake must first fully carry out and document a legitimate interests assessment, including assessing and implementing safeguards that could reduce the harms on the individual.

Actions

IAB Europe will support discussion on legitimate interests as a lawful basis for advertising related activity by sharing completed and anonymised LIAs with the ICO.*

IAB Europe, IAB UK and the ICO will review the provided LIAs with a view to identifying use cases where the application of legitimate interests fulfils all the required criteria. IAB UK may supplement this discussion with other UK-specific examples as it sees fit.

*Note: with regards to legitimate interests as a lawful basis for advertising-related activity, this principle does not constitute, and should not be read as, anything more than the ICO wanting further input into its deliberations on this matter.

IAB UK will use the results of the IAB Europe / IAB UK / ICO discussions to educate its members on the requirements when seeking to rely on legitimate interests as a lawful basis for processing. IAB Europe have begun developing a template LIA as part of this work.

Note: TCF v 2.0 vendor registration process has been amended to include a requirement for vendors declaring LI as a legal basis to also confirm they have completed an LIA.

Deliverables

IAB UK will initiate a workstream to deliver the agreed actions regarding legitimate interests.

E: Data Protection Impact Assessment (DPIA) requirements

Principles

All UK data controllers, including IAB UK members, should undertake DPIAs where processing is likely to result in high risk, in order to assess the impact of the envisaged processing activity on the protection of personal data.

Given the nature of personal data processing within RTB, a DPIA is likely to be required for, at a minimum, participation in the RTB process.

Other aspects of the ad serving process should be assessed against existing ICO guidance on DPIAs.

Actions

IAB UK should educate and encourage its members to review their processing operations in light of the ICO's guidance on activities likely to result in high risk.

IAB UK will engage with its members and ascertain if additional guidance is required to 'bridge the gap' between current ICO guidance and industry awareness of this requirement.

IAB UK will develop additional guidance if required. This could include a DPIA framework for IAB UK members, providing some of the tools required to undertake assessments while reiterating that the responsibility lies with data controllers (IAB Europe has begun developing a template DPIA as part of this work). Where possible, and in order to ensure consistency in approach and communication, IAB UK will seek to work with relevant trade bodies as they develop their own DPIA framework approaches and guidance.

The ICO will liaise with IAB UK to confirm its understanding of good practices regarding DPIAs.

Deliverables

To be determined, depending on the outcome of the actions described above.

F: Transparency and fairness (information provided to consumers)

Principles

All data controllers operating within the TCF/OpenRTB must recognise their transparency obligations under GDPR Article 13/14 and PECR Regulation 6.

The complex nature of processing within RTB does not provide data controllers with an exemption from meeting their transparency obligations under GDPR and PECR. If adequate transparency cannot be provided, processing activities must be reviewed and, where necessary, amended.

Actions

IAB UK will engage with IAB Europe on the outcomes of discussions on changes to TCF policies with respect to CMP UIs.

Deliverables

In the absence of agreement on changes to TCF policies with respect to CMP UIs, IAB UK will initiate a workstream to deliver the actions including:

- Identify the good practices that IAB UK can communicate to its members on CMP UIs
- Based on the above, educating its members on good practices around CMP UIs

Further areas to explore

In developing this response, IAB UK has acted quickly in a tight time frame to provide assurance to the ICO that the industry can and will implement changes to address its concerns. Our work has identified some issues where further discussion and exploration is needed before the most appropriate responses and actions can be identified.

Additionally, some further topics arose during discussions with the ICO that are not specified in their 'Update report' and which we will continue to explore with the ICO in 2020. These include:

- Cookie walls and conditionality of access to content
- Legitimate interests as a legal basis for data processing under GDPR (i.e. after PECR requirements have been satisfied)

Next steps

IAB UK will develop a project plan that includes the actions and deliverables described above, and sets out the timescales within which we will deliver this work. We will liaise with the ICO to agree appropriate prioritisation, timings and milestones. We will share our plans with members, including details of the processes we will follow in taking forward this work (for example, how we will involve and consult members). We will publish further details early in 2020.

We will also look at other ways in which we can support members, such as through running training and workshops on specific topics, linked to the areas and actions described in our action plan above.

We will continue to work closely with the IAB UK Working Group, IAB Europe and its Working Groups, and the IAB Tech Lab as we take forward this work.

7. Conclusion

In June the ICO's message was clear: the digital advertising industry needs to improve its GDPR and ePrivacy compliance. All those involved in RTB, including advertisers, intermediaries and media owners, need to understand and meet their GDPR and PECR compliance obligations in practice.

Our response to the ICO sets out how IAB UK and its members, along with IAB Europe and IAB Tech Lab (where appropriate), will work together and with other parts of the industry to deliver realistic, meaningful and collective change, and to demonstrate responsibility as an industry.

Maintaining a successful and sustainable industry that operates compliantly requires everyone to be willing to take action and to invest in making changes where necessary, within their own organisations and as part of the IAB. We are committed to playing our role in helping this to happen, and the industry needs to be too.

