Digital advertising guidance: special category data under the GDPR

IAB UK

June 2020

Contents

1. About this guidance

IAB UK has produced this guidance as part of our commitment 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 and technical approaches to achieving compliance with the GDPR and ePrivacy legislation (while recognising that individual companies remain accountable for deciding what approaches they should take in practice).

The purpose of this guidance is to help educate the digital advertising industry about what 'special category data' is, as defined in the GDPR (including how it may arise from the way in which other data is processed), and the legal provisions and requirements that apply if you need to process such data, to help companies understand their obligations, and how to comply with them in practice.

'Special category data' is a particular type of personal data as defined by the General Data Protection Regulation (GDPR) [1].The GDPR lists special categories of personal data that require substantially elevated levels of protection:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- data concerning health or data concerning a natural person's sex life or sexual orientation

This guidance is intended as a high-level overview for companies engaged in digital advertising in the UK, based on relevant UK law. It does not constitute legal advice. Companies remain responsible for their own compliance with applicable laws, and should take their own legal advice where necessary.

Note: IAB UK is carrying out a separate, complementary piece of work related to special category data to more fully explore how and where risks can arise of such data being inadvertently processed in the RTB supply chain, and to identify specific controls that can be used to minimise those risks. We will share further details later in 2020. Please check our website for updates: https://www.iabuk.com/GDPR-hub.

We recommend that you review your own data processing activities to identify whether you need to process special category data. If you do not, you should ensure you are not processing such data, directly or indirectly (including by making inferences from other data – see 'Special category data and digital advertising'). If you do, you must have in

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1

place a process to obtain explicit consent before doing so (as well as meeting all other relevant legal requirements for processing such data – see 'Requirements that apply to processing special category data'). Obtaining explicit consent may be difficult to do in practice, in the context of digital advertising, and you should be aware that the Transparency and Consent Framework (TCF) does not provide a means of establishing explicit consent (see page 13 for more details).

1.1 About the ICO

The Information Commissioner's Office (ICO) is the UK's data protection and privacy regulator. It is responsible for enforcing the GDPR and the Data Protection Act 2018 (DPA 2018) in the UK, along with most aspects of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), including regulation 6 that governs cookies and other similar technologies.

Specifically in relation to the GDPR, the ICO regulates any:

- UK-established data controllers and processors (subject to the one-stop-shop mechanism where that entity has a main establishment elsewhere in the EU)
- and entities outside the EU that process the data of individuals in the UK.

The ICO has a comprehensive set of guidance and resources for organisations on data protection and the GDPR, available at https://ico.org.uk/for-organisations/. For information about the impact of Brexit from a data protection perspective see the ICO's website: https://ico.org.uk/for-organisations/data-protection-and-brexit/.

1.2 The ICO Update report into ad tech and RTB

In June 2019, the ICO published its 'Update report into ad tech and RTB' (the 'Update report'), which summarised the findings of its review of the use of personal data and cookies (and other similar technologies) in the real-time bidding (RTB) process. In its report the ICO set out its observations about RTB with respect to the relevant provisions of the GDPR and the Data Protection Act 2018, and PECR.

One of the six key points in the ICO's Update report was the processing of special category data (without explicit consent being obtained) as a consequence of data that is (or may be) contained in RTB bid requests.

This guidance forms part of the actions set out in IAB UK's response to the Update report. In that response we set out our views on special category data and RTB, and committed to a number of actions relating to special category data, including to publish guidance to help educate the industry.[2]

[2] see section B of our action plan on page 24 of our response

2. Special category data

2.1 What you need to know

Background

'Special category data' is a particular type of personal data. In the UK, processing of personal data is regulated by the General Data Protection Regulation (GDPR) [3] and the Data Protection Act 2018 (DPA 2018).[4] The GDPR lists special categories of personal data that require substantially elevated levels of protection.

Details

The GDPR defines what constitutes 'personal data', 'processing', and 'special category data'. The GDPR sets out particular requirements that you must meet if you want to process special category data.

The GDPR defines 'personal data' as follows:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[5]

And it defines 'processing' of personal data as follows:

> 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;[6]

Special category data is personal data that meets one (or more) of the following criteria[7]:

- it reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership
- it concerns health, a person's sex life or a person's sexual orientation
- it is genetic data

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1

[4] Details of the data protection framework in the UK and how it operates are available on the ICO's website: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/

[5] GDPR Article 4(1)

[6] GDPR Article 4(2)

[7] GDPR Article 9(2)

- it is biometric data (where used for identification purposes)

Note: For the purpose of drafting this guidance, we have assumed that genetic data and biometric data used for unique identification is not processed for digital advertising purposes. There are additional requirements that apply to processing genetic data and biometric data and this guidance does not address those.

The GDPR provides higher protection for special category data, 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 prohibited unless one of the specific conditions in Article 9 of the GDPR is satisfied. Although there are a number of conditions available in Article 9, in the case of digital advertising generally, and RTB specifically, the only one available is 'explicit consent' (Article 9(2)(a)). The ICO's 'Update report' says: 'The only applicable condition is explicit consent. No other condition can be relied upon and none of the public interest conditions within the DPA 2018 can apply to RTB specifically or online advertising more generally'.

For more details about the conditions for processing special category data see the ICO's guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

2.2 Special category data and digital advertising

In the vast majority of cases (though not all[8]), UK data controllers, including IAB UK members, do not need to, and should not, process special category data for activities relating to digital advertising.

In other cases, if processing of special category data is necessary, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. There are also other requirements that apply to processing special category data, detailed later in this section and in section 3.

Data that may be considered to be special category data

Much of the data processed for digital advertising purposes does not constitute special category data, by itself, or in combination with other data. Some of it may not in itself be personal data. However, it is possible that information that is not personal data and/or special category data at the point of collection, or on its own, could potentially become special category data depending on how it is processed, particularly when it is associated with a user ID. For example, inferences of a special category nature could be drawn based on collating data from multiple sources associated with a user ID for the purpose of targeting ads to particular audiences.

[8] We recognise that there may be some digital advertising scenarios where processing special category data is necessary and justifiable. As part of our actions in response to the ICO's Update report, IAB UK plans to solicit use cases from members that are processing special category data and utilising explicit consent. We may use these to generate example case studies for such processing.

The ICO's special category data guidance[9] explains that whether or not an inference or guess constitutes processing special category data depends on:

> '…how certain that inference is, and whether you are deliberately drawing that inference.
>
> If you can infer relevant information with a reasonable degree of certainty then it's likely to be special category data even if it's not a cast-iron certainty. But if it is just a possible inference or an 'educated guess', it is not special category data (unless you are specifically processing to treat someone differently on the basis of that inference) - even if that guess turns out to be right.'

These considerations are most likely to be relevant for activities that support behavioural or interest-based targeting, such as audience segmentation.

If you:

- use data to infer or attribute special category details about or to a person (i.e. details revealing or concerning the special categories set out in the GDPR)
- otherwise use or treat data as special category data (i.e. as revealing or concerning the special categories of personal data set out in the GDPR)

then it is likely that this would be considered to be processing of special category data. You should not, therefore, use non-special category data to seek to reveal or establish (including in a probabilistic way) special category details about individuals as part of:

- real-time processing data of contained in bid requests
- building or using profiles and audience segments, or other targeting techniques
- generating inferences from other data
- obtaining and using data from third party sources

If you are intentionally making inferences of a special category nature (about things such as politics, health risks, or sexual orientation) for the purpose of profiling and targeting users, then the ICO's guidance says that 'you are processing special category data irrespective of the level of statistical confidence. The key question here is not whether the inferences are correct, but whether you are using an inference linked to one of the special categories to influence your activities in any way.'

We recommend that you read the ICO's GDPR guidance on special category data, which contains a section on inferences and educated guesses.

[9] See the ICO's guidance on inferences and educated guesses: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7

Special category data could also arise inadvertently. The types of information or data that could potentially be used or combined in such a way that they create an inference about or attribute special category details to a user, include, for example:

- content preferences such as sites visited and articles read (see 'Content taxonomies and categories' below)
- location (e.g. a place of worship)
- basket contents or purchase history (e.g. a medical product)
- a user's interaction with an ad

This information or data could arise based on information in, or about (note: this list is not exhaustive):

- a bid request
- the page or app from which the bid request arises, including its URL (if it is descriptive of the content)
- the ad creative
- a product/product page
- a retail site
- a campaign landing page
- third party sources (e.g. CRM data; DMP/other onboarded data; proprietary data (e.g. from an ad tech service provider)

You should identify whether your data processing creates a risk of processing special category data. Your record of processing activities (ROPA) (see page 15) and any associated DPIAs should provide a basis for your risk assessment. As part of this process, you should consider any automated processing you use, such as the use of optimisation algorithms. Remember that 'processing' includes the entire lifecycle of the data, as set out in the ICO's guidance: 'Almost anything you do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it'.[10] If risks do arise, you should put in place appropriate controls to minimise them (for example, whether and how you store data and associate it with a user ID). See section 3 for further guidance.

Content taxonomies and categories

The IAB Tech Lab's[11] Content Taxonomy is designed to provide publishers with a standardised way to tag and organise their page content. This taxonomy is included in the

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/?q=processing

[11] 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

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 identify the type of environment (content/context) where an ad might appear, although many DSPs rely on external contextual targeting services that specialise in semantic analysis. While IAB Tech Lab ultimately provides the standard and establishes guidance on how to communicate this information in the Open RTB protocol, each party is responsible for how they use the standard and their compliance with applicable law.

IAB UK's view is that context/content category fields such as those detailed in the IAB Content Taxonomy, that may be included the relevant field in a bid request, do not in and of themselves constitute special category data. 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.

However, content categories that are associated with user IDs or other personal data could inadvertently become personal data and specifically, special category data if processed with intent to reveal special category information. For example, if information about users' content preferences is collated over time, and/or combined with other data from multiple sources for the purpose of targeting, then if inferences or educated guesses of a special category nature are made about the user based on that combined data, it could constitute special category data.

In March 2020 the IAB Tech Lab released its updated Content Taxonomy 2.1 for public comment. The update is designed to introduce additional privacy safeguards. Specifically, the Content Taxonomy 2.1 introduces a 'sensitive data' extension (indicator) to taxonomy nodes that could be used to generate sensitive or special category data, as described above, and provides a clear signal to supply chain participants regarding the privacy implications of storing it. Associated updates to the AdCOM (Advertising Common Object Model) / Open RTB guidance have been made that specify that all exchanges that use the protocol should account for all local legislation and not pass any content taxonomy node that has the 'sensitive data' indicator.

If you use the IAB Tech Lab Content Taxonomy and/or other content or context taxonomies or information (e.g. contextual analysis of URLs) for any of your RTB-related activities, you should assess whether your use of this information means you are, or may be, processing special category data and make any necessary changes to ensure that your activities comply with the GDPR. We recommend that, if you use the IAB Tech Lab Content Taxonomy, you put in place plans to implement version 2.1 and review/update your data storage and related practices accordingly. We expect version 2.1 to be released to the market at the start of Q3 2020.

on brand safety and ad fraud; consumer identity, data, and privacy; advertising experiences and measurement; and programmatic advertising.

Audience taxonomies

The IAB Tech Lab Audience Taxonomy provides a common nomenclature for audience segment naming conventions, and promotes comparability of data across different providers when different language is used to describe the same type of segment. It is a key element in IAB Tech Lab's Data Transparency Standard (datalabel.org), which promotes consistent labelling of audience data by first-party and third-party sources.

Audience segments could either in themselves, or in combination with other data, constitute special category data. Audience segments are more likely to pose such a risk, given their purpose (i.e. to describe a likely demographic, or interest, or to indicate purchase intent).

In March 2020, alongside the updated Content Taxonomy 2.1 the IAB Tech Lab released Audience Taxonomy 1.1. The update aligns much of the nomenclature with the new Content Taxonomy updates described above, and deprecates segment names that could be used to describe sensitive data types. We recommend that, if you use the Audience Taxonomy, you put in place plans to implement version 1.1. We expect version 1.1 to be released to the market at the start of Q3 2020.

If you use other audience taxonomies, or other approaches to naming audience segments, we recommend that you review these taxonomies to ensure that you are not using segment types or names that could constitute special category data.

2.3 Requirements that apply to processing special category data

Special category data is, by definition, personal data and therefore it is subject to all of the relevant provisions and requirements that apply to processing personal data in the GDPR, as well as some specific additional protections. This section highlights some of the main considerations that apply in particular.

If you need to process special category data, you should carefully review this processing and ensure it is both justified and compliant with the GDPR and you must carry out a DPIA. Further details are provided below.

You must also ensure that you have met all other relevant requirements for processing special category data including having a process for obtaining explicit consent (in addition to any consent you may need to obtain to process personal data under article 6 of the GDPR, and/or to meet the requirements in PECR) before doing so. You must not process any type of special category data (including inferred or attributed data) without this consent.

If you have made a deliberate decision to process special category data, we recommend that you also seek your own legal advice to ensure that your processing is compliant with the law.

DPIAs

Because of the sensitive nature of special category data, processing it may create high risks to individuals' interests. Article 35[12] of the GDPR requires you to undertake a Data Protection Impact Assessment (DPIA) for:

- any type of processing that is likely to be high risk
- any type of processing specified in article 35(3)
- any of the processing operations published on the ICO's list[13] (which it is required to publish under article (35(4))

This means that if you are processing special category data you will be required to carry out a DPIA[14] and as part of this, you need to consider both the necessity and proportionality of your processing, and document and justify your use of special category data. You must also identify any associated risks and implement appropriate measures to mitigate those risks.

For more details see the ICO's guidance on special category data.

Note: IAB UK is also developing guidance on data security, including risk management and DPIAs, and a template DPIA framework for digital advertising, which we expect to publish in summer 2020. In the meantime, you can refer to the ICO's guidance on DPIAs.

Explicit consent

The GDPR says that, while generally prohibited, special category data can be processed (subject to other relevant requirements for processing being met) if 'the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.'[15]

This means that in order to process special category data, in addition to the requirement to establish a legal basis for the processing of personal data under Article 6 of the GDPR, you must first also obtain explicit consent. This is in addition to any consent you may need to obtain if you are relying on consent as your legal basis under article 6 of the GDPR, and/or to meet the requirements in PECR. You must not process any type of special category data (including inferred or attributed data) without this consent.

The Transparency and Consent Framework (TCF) does not provide a means of establishing explicit consent under Article 9 of the GDPR for processing special category data. You can use the TCF to establish a lawful basis for processing personal data under Article 6, and/or complying with the consent requirements in PECR, as applicable to you. If you need to

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504#tocId49

[13] Assuming that you are regulated by the ICO – see 'About the ICO' in section 1 of this guidance. Otherwise, the list published by the relevant Data Protection Authority.

[14] n.b. this does not mean that you do not need to carry out a DPIA for other data processing, even if you are not processing special category data.

[15] Article 9(2)

process special category data, you need to put in place an additional means of obtaining explicit consent before you process it.

The GDPR does not define what constitutes ‘explicit consent’. The ICO’s guidance says that explicit consent needs:

- a very clear and specific statement of consent, and
- to be expressly confirmed in words (whether oral or written) (and if oral, ICO guidance says you need to keep a record of the script)

and that an ‘affirmative action’ would not in itself constitute explicit consent. The guidance goes on to say that explicit consent needs to ‘specifically refer to the element of the processing that requires explicit consent’ and ‘specify the nature of the special category data’, and that it should be separate from any other consent you are seeking.

For more details see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/.

Other requirements

There may also be other requirements that are engaged if you are processing special category data. The ICO’s guidance says:

> ‘If you process special category data you must keep records, including documenting the categories of data. You may also need to consider how the risks associated with special category data affect your other obligations – in particular, obligations around data minimisation, security, transparency, DPOs and rights related to automated decision-making.’

For more details on documentation requirements, see the ICO’s guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/should-we-document-anything-else

3. What this means in practice

3.1 Summary

In the vast majority of cases companies engaged in digital advertising, and related activities, do not need to, and should not, process special category data. This section focuses on giving guidance on that basis. It is not designed to provide comprehensive guidance to companies who have made a deliberate decision to process special category data, as the considerations will be different.

Note: IAB UK is carrying out a separate, complementary piece of work related to special category data to more fully explore how and where risks can arise of such data being inadvertently processed in the RTB supply chain, and to identify specific controls that can be used to minimise those risks. We will share further details later in 2020. Please check our website for updates: https://www.iabuk.com/GDPR-hub. In the meantime, the following sections provide guidance to digital advertising companies to help you with the process of identifying and minimising risks.

Avoid processing any special category data (unless you can demonstrate that it is necessary and justified - see section 2.3)

This includes avoiding processing non-special category data in a way that could mean that it falls within the definition of special category data (e.g. by using it with the intention of inferring special category attributes to support targeting). You should review your processing activities and ensure that they do not involve such processing.

Understanding the risk

As outlined in the preceding section, there are risks that information that is used for digital advertising and related purposes, that is not special category data (or perhaps not even personal data) at its origin – such as content categories, ad creatives and retail-related information – could potentially become, or be used to infer special category data, depending on how and for what purpose it is processed, particularly if it is linked to a user ID and is combined with other data. For example, if you hold information about a user's content preferences (e.g. regular browsing of information about symptoms of a specific medical condition) and you hold other information about the user's purchases (e.g. of a particular over-the-counter medication), these data points, if combined with the intent to reveal information about the user's health (that they are suffering from that medical condition) in order to target advertising to them, could therefore constitute special category data. See Data that may be considered to be special category data in section 2.

What constitutes special category data can be obvious if the data explicitly reveals information (racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership) about the individual user, or clearly concerns their health, sex life or sexual orientation. Some, however, can be less obvious and will vary on a case-by-case basis. You therefore need to review the risk based on the specifics of the data that you process, and your processing activities, such as how you segment audiences and target ads.

You should identify if risks arise, as part of your data processing, in relation to special category data and, if so, put in place controls to minimise them. You should consider all aspects of your use of data, from ingesting it to using, storing and sharing it. You should also consider whether risks arises indirectly, for example, if as a buyer you set up campaigns and select targeting criteria, and/or onboard data for this purpose.

Article 30 of GDPR obliges you to produce a Record of Processing Activities (ROPA), which describes in detail all of the personal data that you receive, store, process and share. This document will allow you to understand the type of data that you process and will form the basis of your risk assessments.

Data minimisation

Data minimisation is one of the central principles of the GDPR. Your ROPA will enable you to assess exactly what data is needed for your processing activities, and you should ensure that no further data is processed outside of these requirements. You should minimise the data you process, including special category data, at all stages of the data processing lifecycle. As explained in section 2.2, you should be aware that special category data can be inferred or may otherwise arise from processing non-special category data.

Purpose limitation

A further important principle of the GDPR is purpose limitation. You should identify the specific and explicit purposes for which you are processing personal data and you should not process data that is incompatible with this purpose. You should document your processing purposes in your ROPA, as described above. If you have no explicit and specific purpose for processing special category data, then you (or your partners on your behalf) cannot process data in such a way as to infer special category data without first gaining explicit consent to do so. This is because of both the purpose limitation principle and the specific requirements relating to special category data as set out in Article 9 of the GDPR, described in section 2.3 of this guidance.

Implementing appropriate safeguards

There are safeguards that you can put in place to reduce the risk of special category data arising from your processing activities. As the risk is likely to be primarily related to what data you have, and in what combination you store or use it, then you should consider what data you need to create, ingest, use, retain and share and identify ways to reduce or remove data you do not need, and whether you can store data in a way that reduces the risk of processing special category data, such as by dropping certain data points, safeguarding them (e.g. using pseudonymisation or anonymisation techniques) or decoupling them from user IDs.

You should also consider what data is used for targeting purposes and what controls you can put in place around that to avoid processing special category data, whether as a buyer, an intermediary or a seller.

Content and audience taxonomies

If you use the IAB Tech Lab Content Taxonomy and/or other content or context taxonomies, you should assess whether your use of this data means you are, or may be, processing special category data and make any necessary changes to ensure that your activities comply with the GDPR. We recommend that, if you use the IAB Tech Lab Content Taxonomy, you put in place plans to implement version 2.1 and review/update your data storage and related practices accordingly. We expect version 2.1 to be released to the market at the start of Q3 2020.

In March 2020, alongside the updated Content Taxonomy 2.1 the IAB Tech Lab released Audience Taxonomy 1.1. The update aligns much of the nomenclature with the new Content Taxonomy updates described above, and deprecates segment names that could be used to describe sensitive data types. We recommend that, if you use the Audience Taxonomy, you put in place plans to implement version 1.1. We expect version 1.1 to be released to the market at the start of Q3 2020.

If you use other audience taxonomies, or other approaches to naming audience segments, we recommend that you review these taxonomies to ensure that you are not using segment types or names that could constitute special category data.

3.2 What this means for media properties

- Safeguard your user data, especially data that is either special category data or could be used to infer or attribute special category details. Be aware that some kinds of information or data (e.g. raw URLs, page content and purchase history) are particularly vulnerable to being used, including by those with whom you share data, to infer or attribute special category details.[16]
- Review how you store or share such data in conjunction with other personal data, particularly user IDs, and whether this creates a risk of special category data arising.
- Take specific precautions to ensure that you do not, and your downstream partners do not, make special category inferences from such data. For example:
  - apply data minimisation principles and consider techniques such as anonymisation/pseudonymisation of data[17] to reduce the risks of inferences being drawn
  - specifically address this in your data sharing agreements and/or contracts with your partners and clients, and identify your respective responsibilities in the event of an issue arising
- Avoid creating, providing or enabling the use of audience segments or other targeting functionality that are explicitly or obviously of a special category nature on your media properties unless you have an extremely robust compliance approach that goes beyond the TCF.
- Avoid inferring special category details from non-special category data (see the illustrative lists on pages 8-9 of this guidance).

3.3 What this means for third party technology/intermediary companies

- Safeguard your user data, especially data that is either special category data or could be used to infer or attribute special category details. Be aware that some kinds of information or data (e.g. raw URLs, page content) are particularly vulnerable to

[16] See pages 7-8 for more details on whether or not an inference or guess constitutes processing special category data.

[17] As noted on page 12, IAB UK will also be publishing guidance on data security, including risk management, and DPIAs, in summer 2020. In the meantime, links to the ICO's guidance are provided throughout this document and summarised in section 4.

being used, including by those with whom you share data, to infer or attribute special category details.[16]
- Review how you store and share non-personal data in conjunction with personal data, such as user IDs, and whether this creates a risk of special category data arising.
- Take specific precautions to ensure that you do not, and your downstream partners do not, make special category inferences from such data. For example:
    - apply data minimisation principles and consider techniques such as anonymisation/pseudonymisation of data[17] to reduce the risks of inferences being drawn
    - specifically address this in your data sharing agreements and/or contracts with your partners and clients, and identify your respective responsibilities in the event of an issue arising

- Avoid inferring special category details in creating or adding to profiles or segments
- Avoid inferring special category details from non-special category data (see the illustrative lists on pages 8-9 of this guidance)
- Avoid creating, using or enabling the use of targeting (including retargeting) criteria of a special category nature, unless you have an extremely robust compliance approach that goes beyond the TCF
- Do not allow onboarding of special category data unless you have an extremely robust compliance approach that goes beyond the TCF

3.4 What this means for advertisers

- Avoid using, creating or seeking to buy against segments, audiences, 'lookalikes' or other targeting (or retargeting) that is of an explicitly or obviously special category nature, at all costs, unless you have an extremely robust compliance approach that goes beyond the TCF. This includes asking your advertising partners to create or identify segments, profiles, etc. of a special category nature.
- Avoid inferring special category data details[18] from non-special category data (see the illustrative lists on pages 8-9 of this guidance)
- Do not obtain third party data of a special category nature, and do not onboard data of a special category nature to your or your advertising partners' systems for targeting purposes, unless you have an extremely robust compliance approach that goes beyond the TCF.

4. Further reading and resources

Legislation

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)

[18] See pages 7-8 for more details on whether or not an inference or guess constitutes processing special category data.

- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Regulation 6 covers cookies.

ICO guidance

- GDPR and consent
- Special category data (lawful basis for processing)
- Special category data
- Special category data – inferences and educated guesses
- DPIAs
- Guide to PECR – Cookies and similar technologies
- The use of cookies and similar technologies
- Data protection and Brexit